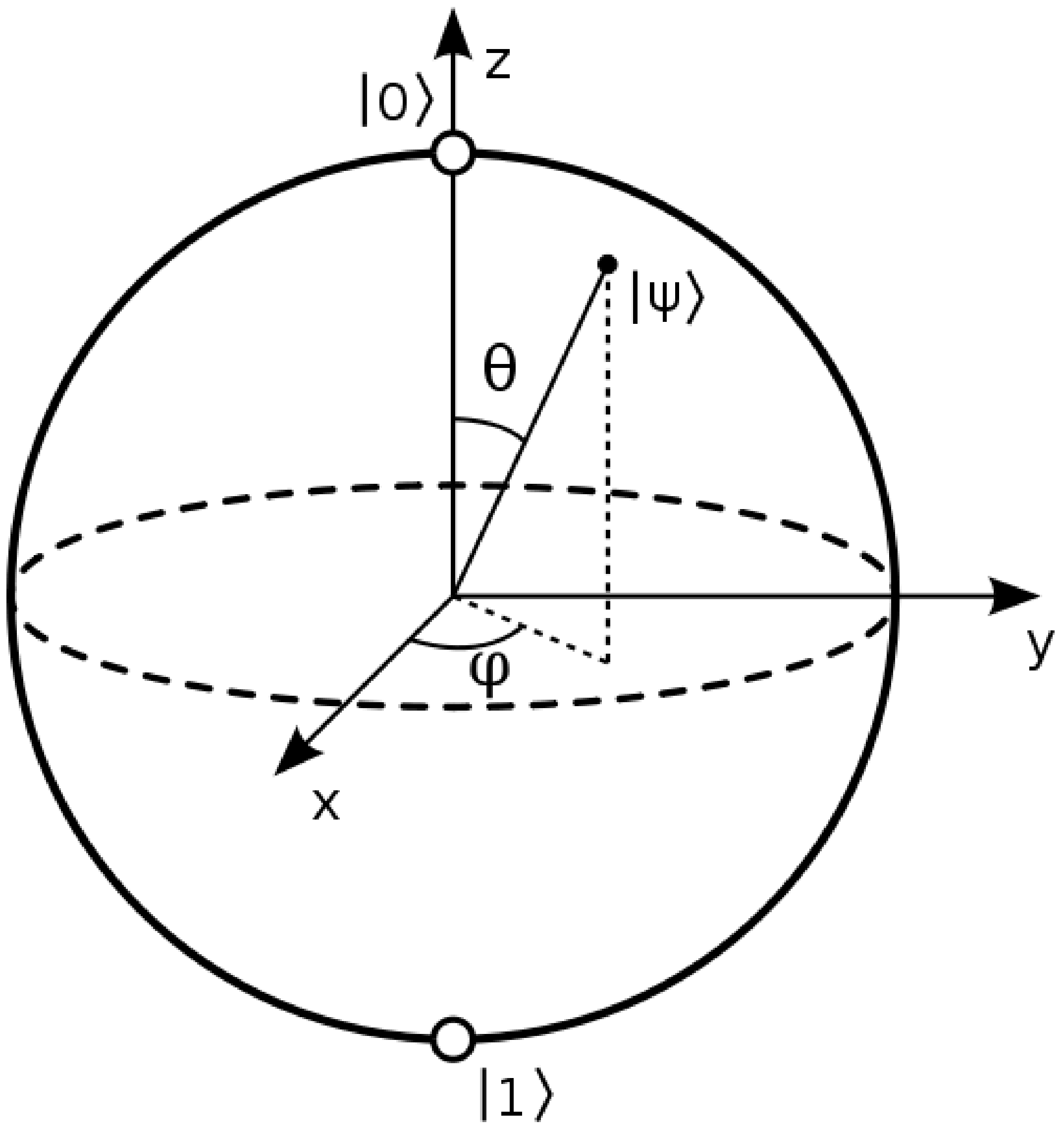
Grover's Algorithm (1996)



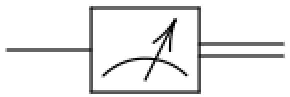
By Jean-Philippe Carlens and Antoine Cousson

WHAT IS
QUANTUM COMPUTING ?

What is Quantum Computing ?

Simple definition :
Computation of information based on quantum properties of particles such as : Superposition , interference and entanglement.

Measuring a qubit is a projection on a certain basis a qubit on a superposition state collapse in on state and all the others are lost

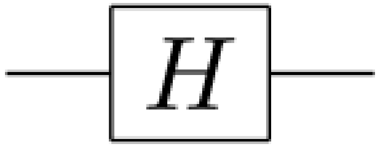


What is a Qubit ?

- $|0>$
- $|1>$
- $\frac{1}{\sqrt{2}}|0> + \frac{1}{\sqrt{2}}|1>$

What is
Quantum Computing ?

<u>Quantum Gate:</u>
A quantum gate is a unitary operator, it can be described as a unitary matrix relative to some basis.
A quantum gate is reversible.



$$HH^* = I$$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

CLASSICAL COMPUTING DATA STRUCTURES

DATA STRUCTURES

Unsorted data structures :
- Just storing data in the first location available without pre-computing

- The fastest way to search is simply to iterate on each element.

- N element, so the worst case is N iterations, best case 1 iteration.
Average : N/2

Sorted data structures :
- Storing data smartly in locations according to their value

- Allow other way to search than the exhaustive one

- Drastically improve the search complexity

DATA STRUCTURES

Unsorted data structure	Sorted data structure
Julia	Alex
David	David
Peter	Julia
Steve	Marie
Victor	Peter
Marie	Steve
Alex	Victor

In this case, we made a pre-computing by storing data in alphabetical order.
The structure is sorted.

Grover's algorithm usage

- Search in database
- SAT problems (e.g. Sudoku)
- Graph coloration
- Search of Hamiltonian path

Used with **unsorted** data / no specific data **structures**.

0	3	4	2	9	1	7	5
					w		N

Ex : *find x, s.t f(x)=1*

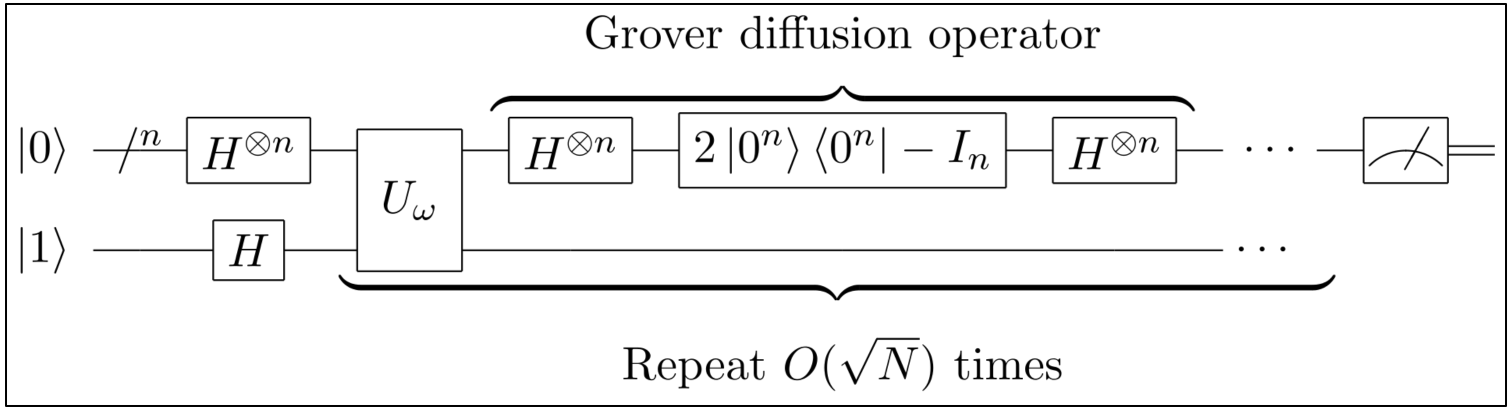
N = 8

Benefits over a regular Algorithm :

- the search among N elements in a time proportional to $\sqrt{N}$ with a storage space proportional to log(N).

- N elements .
- Log(N) qubits for the algorithm

Quantum circuit of the algorithm



Quantum circuit of Grover's algorithm

source : https://fr.wikipedia.org/wiki/Algorithme_de_Grover

The Two main element of The Algorithm

- The Oracle :

Principle of black box

$$\begin{cases} U_\omega|x\rangle = -|x\rangle & \text{for } x = \omega, \text{ that is, } f(x) = 1, \\ U_\omega|x\rangle = |x\rangle & \text{for } x \neq \omega, \text{ that is, } f(x) = 0. \end{cases}$$

O|x> = $(-1)^{f(x)}$ |x>

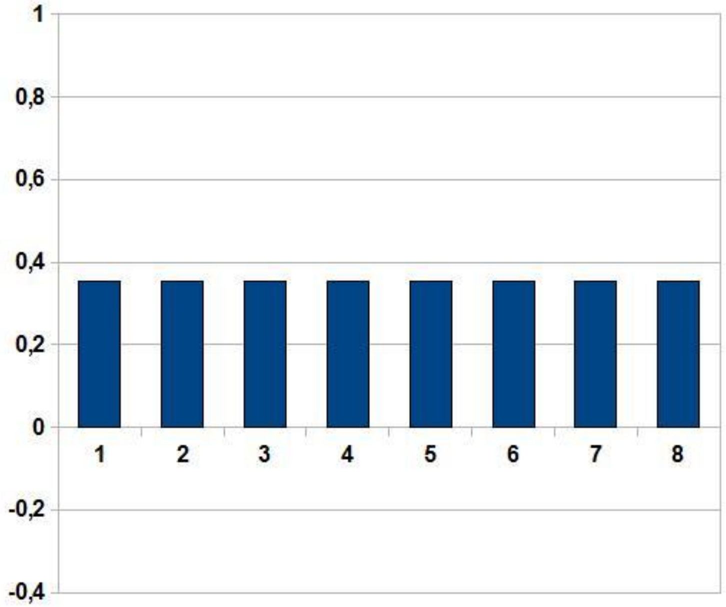
- The Amplitude amplification algorithm :

$$\begin{aligned} \hat{H}\hat{Z}\hat{H} &= \hat{H}\left(2\,|0\rangle\,\langle 0| - \hat{I}\right)\hat{H} \\ &= 2\hat{H}\,|0\rangle\,\langle 0|\,\hat{H} - \hat{H}\hat{I}\,\hat{H} \\ &= 2\,|\Psi_0\rangle\,\langle \Psi_0| - \hat{H}\hat{I}\,\hat{H} \\ &= 2\,|\Psi_0\rangle\,\langle \Psi_0| - \hat{I} \\ &= \frac{2}{2^N}\sum_{i,j}|i\rangle\,\langle j| - \hat{I} \end{aligned}$$

The first step is to construct a superposition state of every elements in the database

- Initial state for the algorithm :

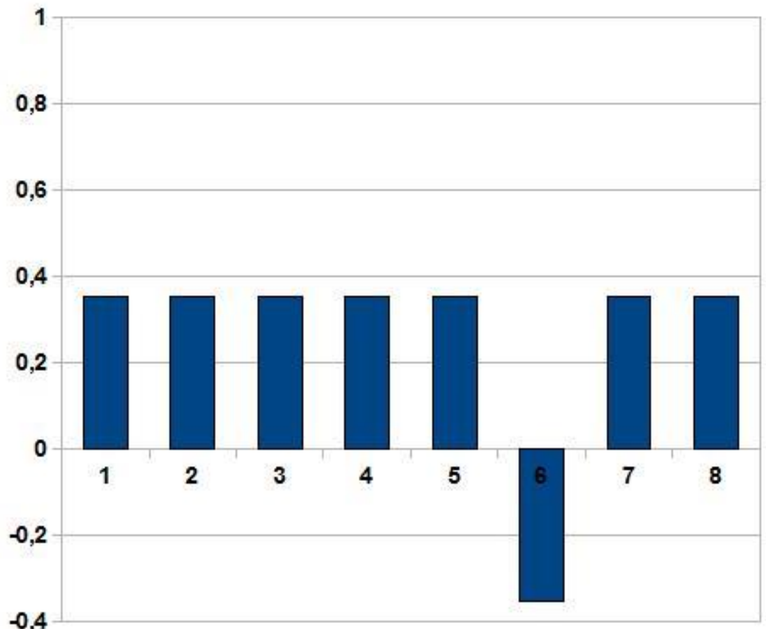
$$|\Psi_0\rangle = \frac{1}{\sqrt{2^N}} \sum_{x=0}^{2^N-1} |x\rangle$$



Source : https://fr.wikipedia.org/wiki/Algorithme_de_Grover#/media/Fichier:Grover-EtatInitial.jpg

The second step is to apply the Oracle to our qubit's states.

- Inverse the phase of the target state by applying the oracle.



Source : https://fr.wikipedia.org/wiki/Algorithme_de_Grover#/media/Fichier:Grover-PassageParBoiteNoire.jpg

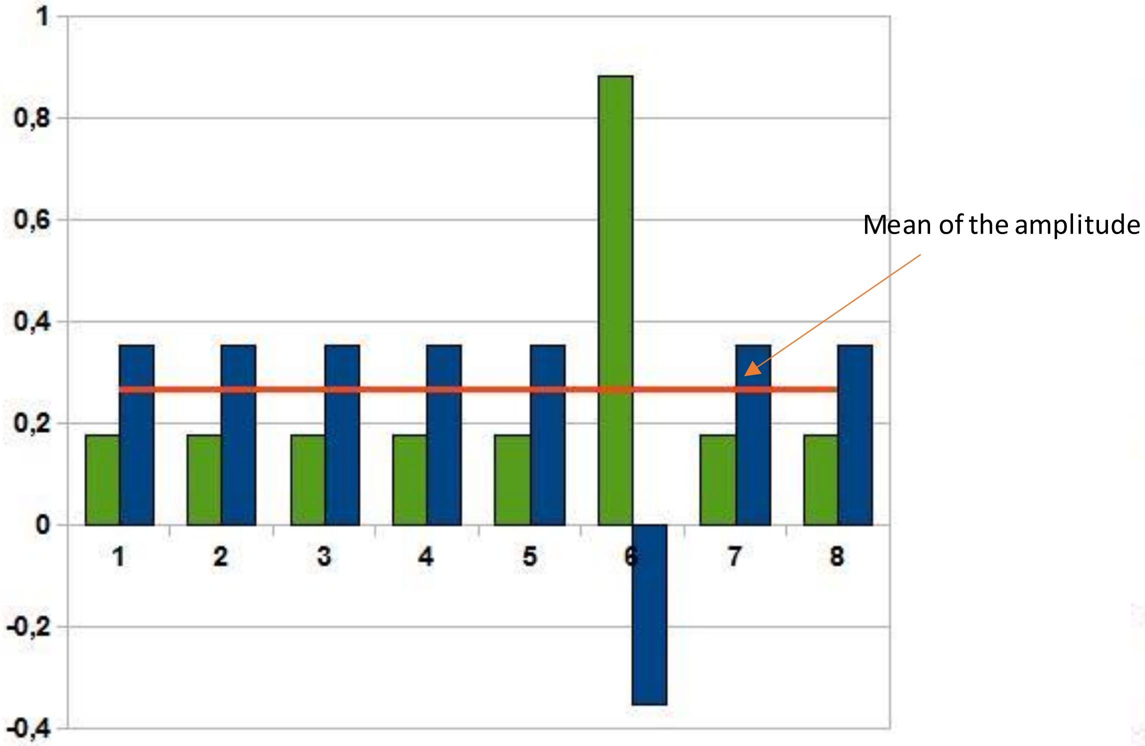
What is the diffusion operator ?

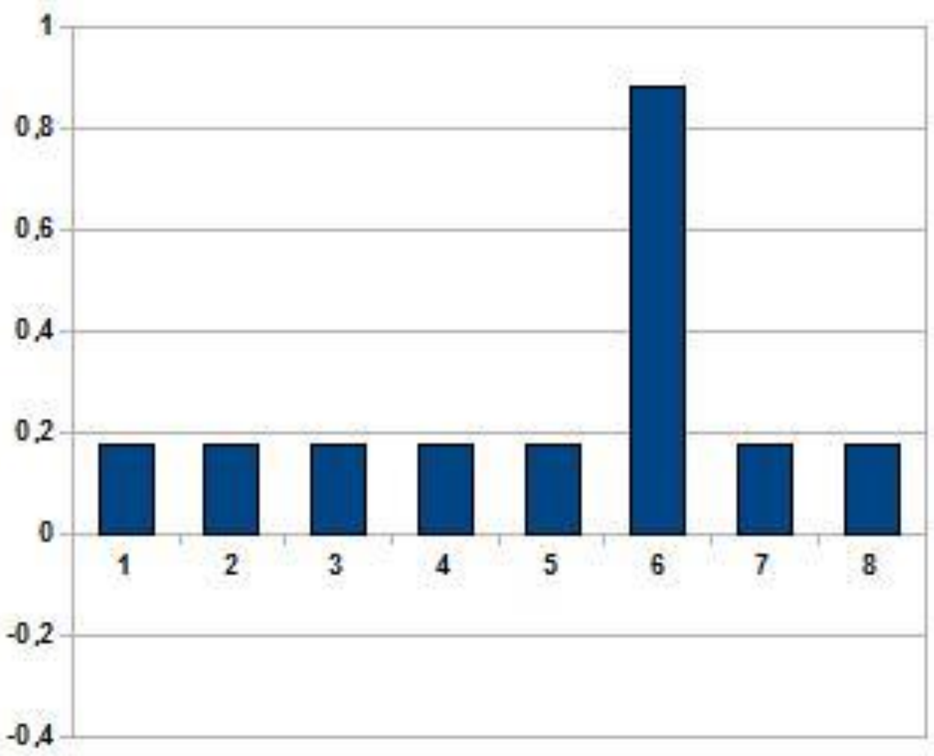
- Enhance the probability to measure the target state.
- Amplify the target state amplitude and minimize others.
- Inverse states amplitudes around the mean.

$$\begin{aligned}\hat{H}\hat{Z}\hat{H} &= \hat{H}\left(2\left|0\right\rangle\left\langle 0\right| - \hat{I}\right)\hat{H} \\ &= 2\hat{H}\left|0\right\rangle\left\langle 0\right|\hat{H} - \hat{H}\hat{I}\hat{H} \\ &= 2\left|\Psi_0\right\rangle\left\langle\Psi_0\right| - \hat{H}\hat{I}\hat{H} \\ &= 2\left|\Psi_0\right\rangle\left\langle\Psi_0\right| - \hat{I} \\ &= \frac{2}{2^N}\sum_{i,j}\left|i\right\rangle\left\langle j\right| - \hat{I}\end{aligned}$$

$$\hat{Z} = 2\left|0\right\rangle\left\langle 0\right| - \hat{I}$$

The third step is the amplitude amplification





Source : https://fr.wikipedia.org/wiki/Algorithme_de_Grover#/media/Fichier:Grover-MiroirMoyenne.jpg

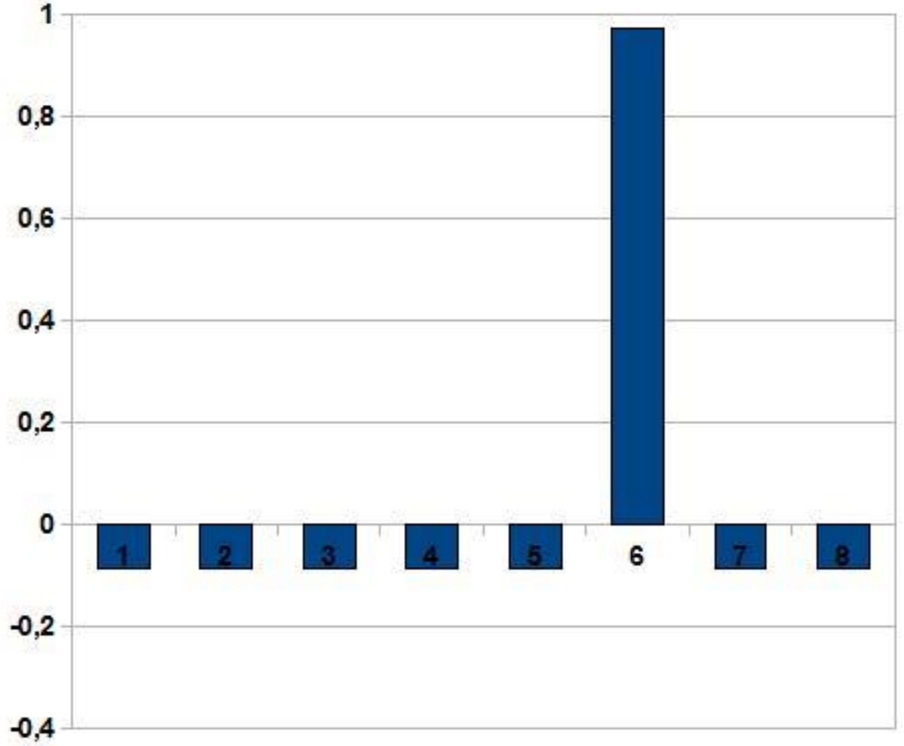
Grover's Operator

Grover operator ➡ $$\hat{G} = \Big(\overbrace{\hat{H}\hat{Z}\hat{H}}^{\text{Grover diffusion operator}}\Big)\,\hat{O}$$

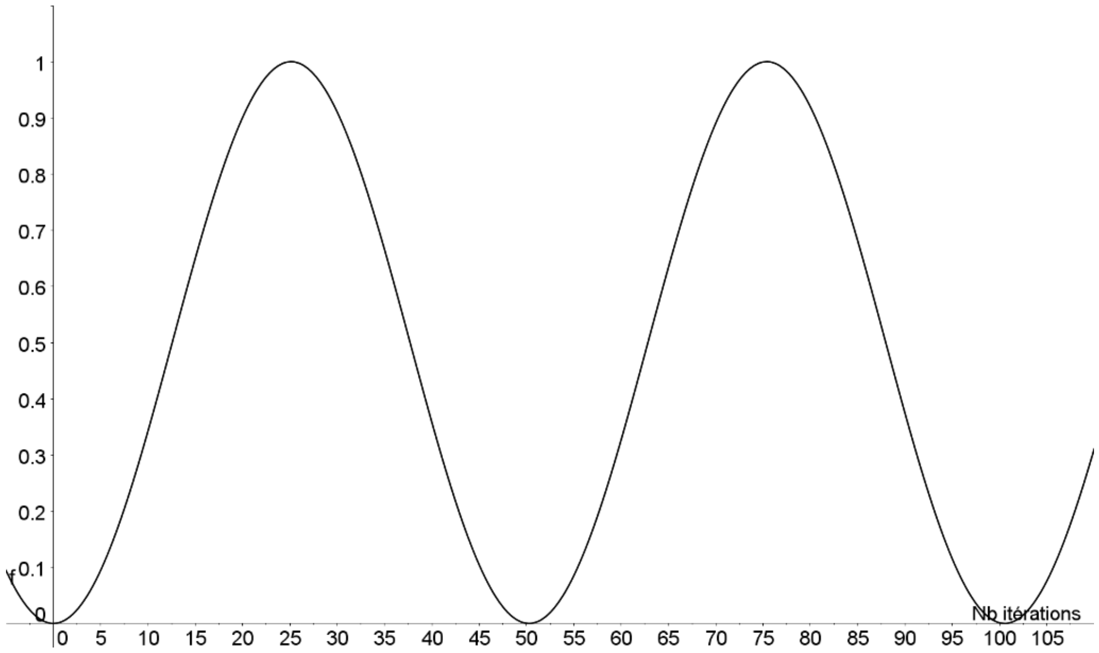
Hadamar operator ➡
$$\hat{H} = \frac{1}{\sqrt{2}}\left(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|\right) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$
$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Zero phase shift ➡ $$\hat{Z} = 2\,|0\rangle\langle 0| - \hat{I}$$

Then we iterate until the probability is the closest as possible to the solution



Closest probability



Probability of detection based on the number of iterations, for 10 qubits = search among 1024 elements.

A Sudoku solver with Grover in Qiskit

Is there a better algorithm than Grover for Quantum unstructured search ?

Grover's quantum searching algorithm is optimal

Christof Zalka

Phys. Rev. A **60**, 2746 – Published 1 October 1999

"I show that for any number of oracle lookups up to about π/4√N, Grover's quantum searching algorithm gives the maximal possible probability of finding the desired element. I explain why this is also true for quantum algorithms which use measurements during the computation. I also show that unfortunately quantum searching cannot be parallelized better than by assigning different parts of the search space to independent quantum computers."

• Received 20 February 1998

DOI: https://doi.org/10.1103/PhysRevA.60.2746

Article : https://arxiv.org/pdf/quant-ph/9711070.pdf

Bibliography:

- https://quantum-computing.ibm.com/composer/docs/iqx/guide/grovers-algorithm
- https://docs.microsoft.com/en-us/azure/quantum/concepts-grovers
- https://qiskit.org/textbook/ch-algorithms/grover.html
- https://fr.wikipedia.org/wiki/Probl%C3%A8me_SAT
- https://en.wikipedia.org/wiki/Hamiltonian_path
- https://fr.wikipedia.org/wiki/Coloration_de_graphe
- https://fr.wikipedia.org/wiki/Porte_quantique#Porte_Hadamard_(H)
- https://fr.wikipedia.org/wiki/Algorithme_de_Grover
- https://github.com/qiskit-community/qiskit-textbook/blob/main/content/ch-algorithms/grover.ipynb
- https://arxiv.org/pdf/quant-ph/9711070.pdf
- https://www.youtube.com/watch?v=EoH3JeqA55A
- https://www.researchgate.net/publication/23421235_Strength_and_Weakness_in_Grover's_Quantum_Search_Algorithm