Grover search algorithm

Quantum Computing Minicourse ICTP-SAIFR

Stefano Carrazza[‡] and Matteo Robbiati[†]

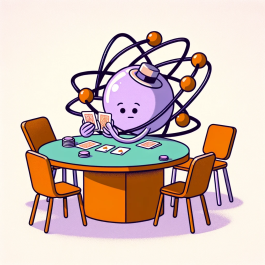
8 April 2024

[‡] Associate Professor & Researcher, University of Milan and INFN Milan, Italy.
[†] PhD candidate, University of Milan, Italy and CERN, Switzerland.

Motivation

The Grover algorithm is powerful when searching an item among an unordered set of candidates.

Extract the jack of clubs from a Poker deck



Find a passcode composed of 10 numbers

Find an antidote to the Cobra poison, exploring 10^{20} molecules

? How many attempts could you need, in the worst scenario, to explore all the possibilities?

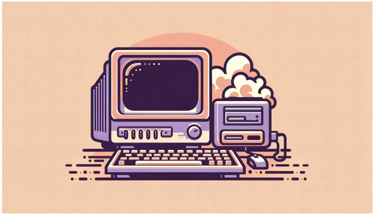
⚠ In the worst scenario, you will need to check 52 **cards**, 10^{10} **passcodes** and 10^{20} **molecules**.

Quadratic speedup

If we consider a time cost of $\delta = 10^{-8}$ seconds for any algorithmic call (quantum or classical) we would wait:

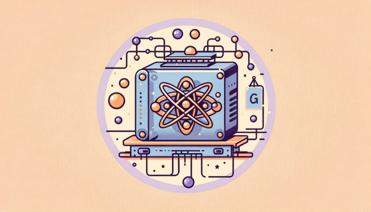
On a classical computer

- 0.52 μs to find the jack of clubs;
- 100 seconds to find the passcode;
- $\sim$ 31688 years to find the Cobra antidote.



On a quantum computer

- 0.0721 μs to find the jack of clubs;
- 0.001 seconds to find the passcode;
- 100 seconds to find the Cobra antidote.



The Grover algorithm solves this kind of search with a number of algorithmic calls proportional to $\sqrt{N}$, where N is the dimension of the search space.

The Grover algorithm

The key steps of the Grover algorithm:

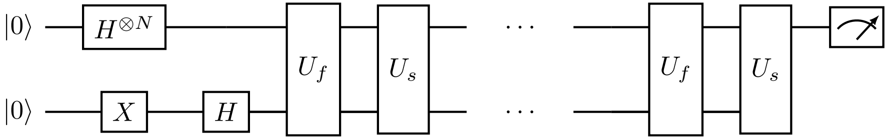
1. prepare a system of N qubits into a maximally superposed state;
2. prepare an ancilla qubit into the $|-\rangle$ state;
3. apply an oracle operator U_f which can mark the correct solution;
4. apply a diffusion operator U_s which amplifies the correct solution;
5. repeat 3. and 4. for the optimal number of times.

The Grover algorithm

The key steps of the Grover algorithm:

1. prepare a system of N qubits into a maximally superposed state;
2. prepare an ancilla qubit into the $|-\rangle$ state;
3. apply an oracle operator U_f which can mark the correct solution;
4. apply a diffusion operator U_s which amplifies the correct solution;
5. repeat 3. and 4. for the optimal number of times.

In terms of quantum circuit:



step 1 and 2: the state preparation

Lets consider 2^N elements composing our search space.

step 1 and 2: the state preparation

Lets consider 2^N elements composing our search space.

We can encode them into the amplitudes of a quantum state of N qubits:

$$\begin{bmatrix} \text{item}_1 \\ \text{item}_2 \\ \dots \\ \text{item}_{2^N} \end{bmatrix} \quad \rightarrow \quad \begin{bmatrix} \psi_{00\dots0} \\ \psi_{00\dots1} \\ \dots \\ \psi_{11\dots1} \end{bmatrix}$$

step 1 and 2: the state preparation

Lets consider 2^N elements composing our search space.

We can encode them into the amplitudes of a quantum state of N qubits:

$$\begin{bmatrix} \text{item}_1 \\ \text{item}_2 \\ \dots \\ \text{item}_{2^N} \end{bmatrix} \quad \rightarrow \quad \begin{bmatrix} \psi_{00\dots0} \\ \psi_{00\dots1} \\ \dots \\ \psi_{11\dots1} \end{bmatrix}$$

Let us use an **ancilla**, which will help us in manipulating the system's qubits through a kickback-like procedure.

In the complete framework, we are going to use $N+1$ qubits, whose state is $|\psi\rangle\,|a\rangle$.

The first step of the algorithm is the state preparation into one maximally superposed state:

$$H^{\otimes N+1}\,|00\dots0\rangle\,|1\rangle = |+ + \dots +\rangle\,|-\rangle\,.$$

Step 3: the oracle U_f

Step 4: the diffusion operator U_s