Grover Algorithm

Problem: Search some solutions in an unstructured database

Classical: Essential problem

N entries → in average N/2 tests

Quantum Grover algorithm: $O(N^{1/2})$

Very general since can speed up all classical algorithms using a search heuristic

Formulation of the problem:

N elements indexed from 0 to N-1, $N=2^n$

$\{|x\rangle\}_x$ search register, elements repertoried via their index

The search problem admits M solutions

Stolze & Suter 8.4

Grover Algorithm: the Oracle

Key element: the Oracle

$$f(x) = \begin{cases} 1 & \text{if x is a solution} \\ 0 & \text{otherwise} \end{cases}$$

Naively: „black box“ *recognizing* a solution

More precisely: unitary operator acting on a tensor product

$$O|x\rangle_{\text{Register}}|q\rangle_{\text{Oracle}} \quad = \quad |x\rangle|q \oplus f(x)\rangle$$

flips the oracle qbit if x is a solution

Grover Algorithm: the Oracle

Key element: the Oracle

$$f(x) = \begin{cases} 1 & \text{if x is a solution} \\ 0 & \text{otherwise} \end{cases}$$

Naively: „black box“ *recognizing* a solution

More precisely: unitary operator acting on a tensor product

$$O|x\rangle_{\text{Register}}|q\rangle_{\text{Oracle}} = |x\rangle|q \oplus f(x)\rangle$$

flips the oracle qbit if x is a solution

Role of the oracle qbit:

$$\begin{aligned} |q_0\rangle &= (|0\rangle - |1\rangle)\,1/\sqrt{2} \\ |q_0 \oplus 1\rangle &= -|q_0\rangle \\ O|x\rangle|q_0\rangle &= (-1)^{f(x)}|x\rangle|q_0\rangle \end{aligned}$$

The oracle qbit is unchanged → will be omitted
The oracle marks the solutions to the search problem

Grover Algorithm: principle

Step 1. Initialization of the register: $|0\rangle^{\otimes n}$

Step 2. Hadamard gate $|\psi_2\rangle = H^{\otimes n}\,|0\rangle^{\otimes n} = 1/\sqrt{N}\ \Sigma_{x=0}^{N-1}\,|x\rangle$

Iteration step: (1) Apply the Oracle O

(2) Apply the Hadamard transformation $H^{\otimes n}$

(3) Perform a conditional phase shift with all computational basis states except $|0\rangle^{\otimes n}$ C_π

(4) Apply the Hadamard transformation $H^{\otimes n}$

$$
\begin{aligned}
G &= H^{\otimes n} C_\pi H^{\otimes n}\, O \quad \text{mit } C_\pi = -\mathbf{1} + 2|0\rangle\langle 0| \\
&= (\underbrace{-H^{\otimes n}\mathbf{1}H^{\otimes n}}_{-\mathbf{1}} + 2\, \underbrace{H^{\otimes n}|0\rangle}_{|\psi\rangle_2} \underbrace{\langle 0|H^{\otimes n}}_{\langle\psi|_2})\, O \\
&= (2|\psi_2\rangle\langle\psi_2| - \mathbf{1})\, O
\end{aligned}
$$

Grover Algorithm: geometrical interpretation

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}}\sum_x (1-f(x))|x\rangle$$ Superposition of the non-solutions

$$|\beta\rangle = \frac{1}{\sqrt{M}}\sum_x f(x)|x\rangle$$ Superposition of the M solutions

$$\Rightarrow |\psi_2\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle = \cos\left(\frac{\theta}{2}\right)|\alpha\rangle + \sin\left(\frac{\theta}{2}\right)|\beta\rangle$$

Grover Algorithm: geometrical interpretation

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}}\sum_x (1-f(x))|x\rangle$$ Superposition of the non-solutions

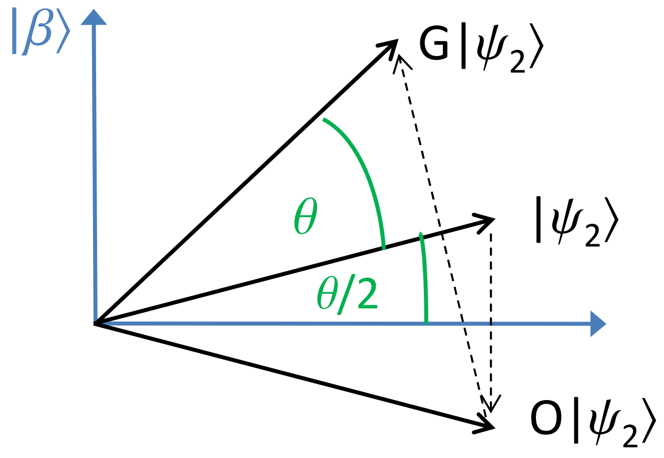
$$|\beta\rangle = \frac{1}{\sqrt{M}}\sum_x f(x)|x\rangle$$ Superposition of the M solutions

$$\Rightarrow |\psi_2\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle = \cos\left(\frac{\theta}{2}\right)|\alpha\rangle + \sin\left(\frac{\theta}{2}\right)|\beta\rangle$$

$$O|\psi_2\rangle = \cos\left(\frac{\theta}{2}\right)|\alpha\rangle - \sin\left(\frac{\theta}{2}\right)|\beta\rangle$$ Relection about the $|\alpha\rangle$ axis

$$H^{\otimes n}C_\pi H^{\otimes N} = (2|\psi_2\rangle\langle\psi_2| - \mathbf{1}) = \underbrace{|\psi_2\rangle\langle\psi_2|}_{\text{Projection onto } |\psi_2\rangle} - \underbrace{(\mathbf{1} - |\psi_2\rangle\langle\psi_2|)}_{\text{Projection orthogonal to } |\psi_2\rangle}$$

Reflection about the $|\psi_2\rangle$ - axis



Grover Algorithm: convergence

- The iteration of G corresponds to a rotation of θ.

  After k steps:

  $$G^k|\psi_2\rangle = \cos((2k+1)\,\theta/2)\,|\alpha\rangle + \sin((2k+1)\theta/2)\,|\beta\rangle$$

- How many iterations are required?

Idea: the obtained state should be almost along $|\beta\rangle$, since a measurement would project the state onto a solution

k_{ideal} is such that $(2k_{ideal}+1)\theta/2 = \pi/2$

For M/N << 1: $k_{ideal} \propto \sqrt{\frac{N}{M}}$

- What happens if one realizes more iterations?

Grover Algorithm: what did we gain?

- **Better scalability:** low computational costs

- **Two essential questions left**
  - ✓ How to technical implement an Oracle operator, without actually solving the search problem?
  - ✓ How to know the number of solutions to a search problem M without actually solving it?

Grover Algorithm: what did we gain?

- **Better scalability:** low computational costs

- **Two essential questions left**

  ✓ How to technical implement an Oracle operator, without actually solving the search problem?

  Example: Think about the oracle of the factoring problem.

  Does it help alone?

  ✓ How to know the number of solutions to a search problem M without actually solving it?

  Yes ! Quantum Fourier transform. Reformulation of the problem in terms of the determination of a phase factor.