Grover algorithm

Grover algorithm

- Known as quantum search algorithm
- Quantum algorithm for unstructured search that finds the unique input to a **black box** function that produces a particular output value.

$$x : represents\ a\ possible\ input.\ x \in \{0,\ 1\}^n$$

$$There\ are\ 2^n\ inputs$$

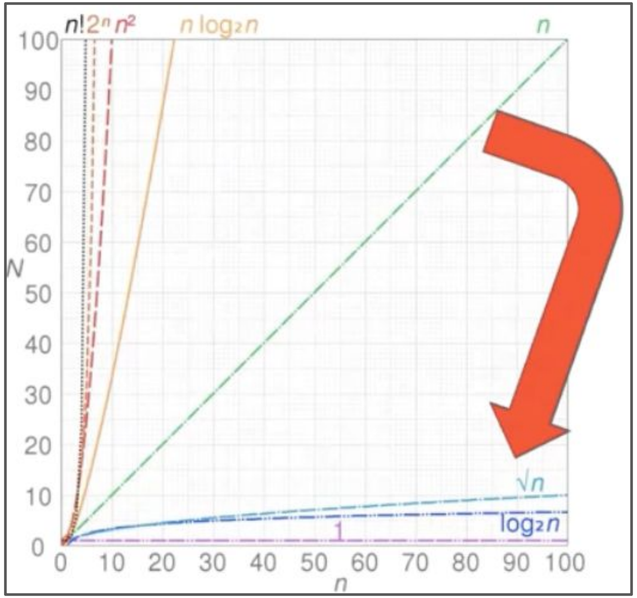
$$f(x) \in \{0,\ 1\}$$

$$\exists\ only\ one\ \omega\ such\ that\ f(\omega) = 1,\ all\ other\ x \neq \omega,\ f(x) = 0$$

Grover algorithm: The black box function

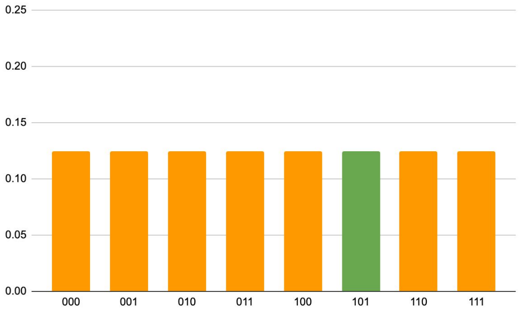
- The *f* function encodes the problem
- Grover works for problems where:
  - Solution is hard to find (computationaly difficult to generate)
  - But easy to verify: calculate f(x)
- Complexity
  - Classical computing: $O(2^n)$
  - Quantum computing: $O(2^{n/2})$

Example: n = 40
- Classical: $n^{40} \sim 10^{12}$
- Grover: $n^{20} \sim 10^{6}$



https://www.youtube.com/watch?v=YEI5vYdcoQ4

000	0.125
001	0.125
010	0.125
011	0.125
100	0.125
101	0.125
110	0.125
111	0.125



ω

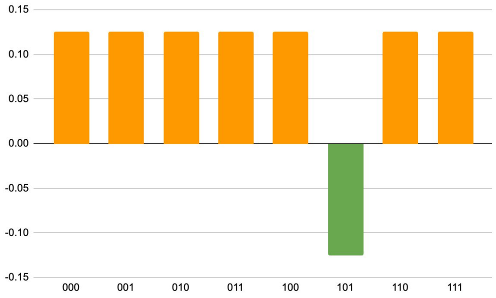
- ω is unknown (hard to find), but …
- If we calculate f(ω), the result will be 1: f(ω) = 1

a_i = 2*average - a_i

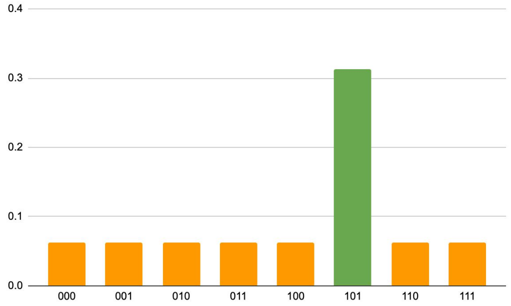
000	0.0625
001	0.0625
010	0.0625
011	0.0625
100	0.0625
101	0.3125
110	0.0625
111	0.0625

Marking the solution

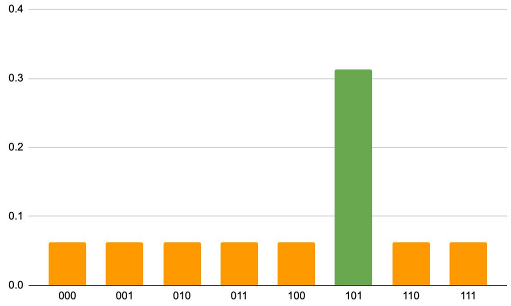
000	0.125
001	0.125
010	0.125
011	0.125
100	0.125
101	-0.125
110	0.125
111	0.125



Amplifying the solution (Diffusion)

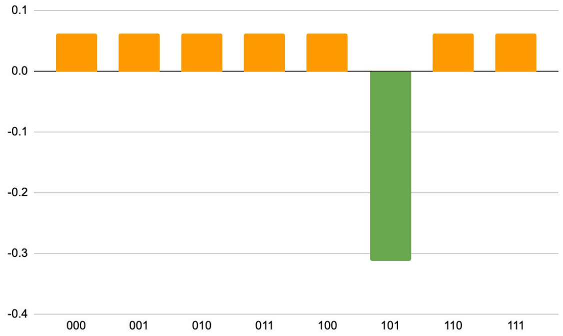


000	0.0625
001	0.0625
010	0.0625
011	0.0625
100	0.0625
101	0.3125
110	0.0625
111	0.0625



Marking the solution

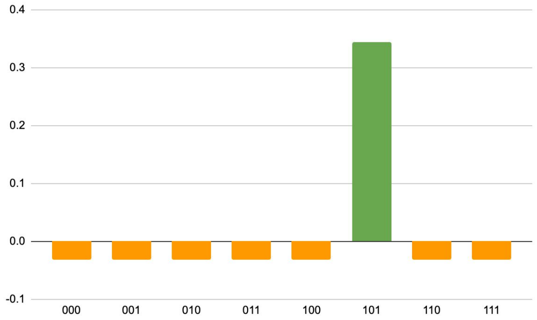
000	0.0625
001	0.0625
010	0.0625
011	0.0625
100	0.0625
101	-0.3125
110	0.0625
111	0.0625



a_i = 2*average - a_i

Amplifying the solution (Diffusion)

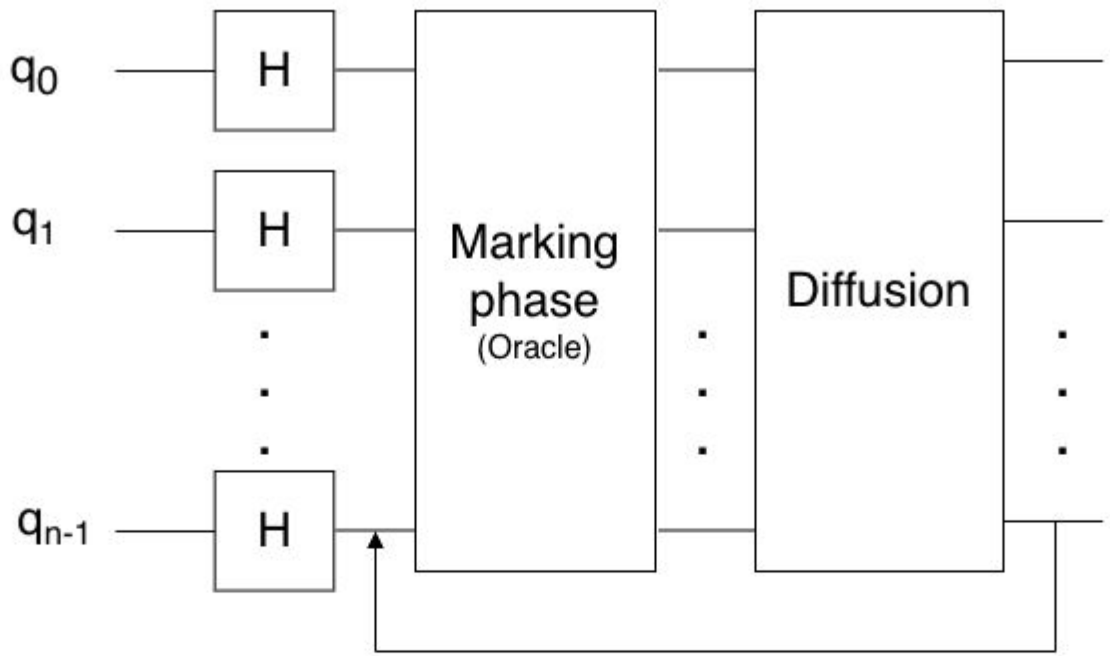
000	-0.03125
001	-0.03125
010	-0.03125
011	-0.03125
100	-0.03125
101	0.34375
110	-0.03125
111	-0.03125



Open questions

1. Which quantum circuit should be used for the marking phase?
2. Which quantum circuit should be used for the amplifying phase?
3. When to stop the loop ?
4. Why using a_i = 2*average - a_i as “amplifier”

Grover algorithm



Initialisation

- Start by a register of *n* qubits: |00000 ..00>.
- $N = 2^n$
- Apply Hadamard : $H^{\otimes n}$ on |00000 ..00> = $|\psi_0>$
- $|\psi_0> =$ $$\frac{1}{\sqrt{N}} \sum |i> \; with \; |i> \; \in \; \{|0000 \ldots 00>, \; \ldots \; |11111 \ldots 11>\}$$

Marking phase (Oracle)

$$O = I - 2\,|\omega><\omega|$$

$$O|x> = \begin{cases} |x> \; for\ all\ x \neq |\omega> \\ -|x> \; for\ x = |\omega> \end{cases}$$

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

Quantum circuit:

1. Apply X to all qubits with state 0 in ω
2. Apply MCZ (phase flip only if all qubits are 111.. 11)
3. Undo the X gates (Apply X to all the qubits to which we applied an X in step 1)

The oracle **marks the solution (ω)** by flipping its sign (phase)

Diffusion phase

$$D = 2|\psi_0><\psi_0| - I$$

D is the quantum implementation of:

$a_i \leftarrow 2*average - a_i$

$$|\psi_0> = \frac{1}{\sqrt{N}}\sum |i>$$

$$with\ |i> \in \{|0000\ldots 00>, \ldots |11111 \ldots 11>\}$$

The diffusion phase mirrors each amplitude around the average.

Diffusion phase: Quantum circuit

$$D = H^{\otimes n} \underbrace{X^{\otimes n} MCZ X^{\otimes n}}_{} H^{\otimes n}$$

- The component along $|\psi_0>$ becomes aligned with $|0>$
- This is essentially a change of basis (coordinates)

Apply the phase flip on |0>

(I - 2 |0><0|)

Returns to the original basis

Hes·so

Diffusion phase: To summarise …

- The first Hadamard transform the basis so that $|\psi_0>$ corresponds to |0>
- Middle block: apply the phase flip on |0>
- Second Hadamard return to the original basis