Grover. Part 2

Anuj Dawar

Components of Grover Loop

- The Oracle -- O
- The Hadamard Transforms -- H
- The Zero State Phase Shift -- Z

The Quantum Oracle

Inputs oracle

$$|x\rangle|q\rangle|w\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle|w\rangle$$

This is action of quantum oracle

- The work qubits are returned to their initial state, so we will ignore them

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle$$

- Suppose the oracle qubit is initially in the state

$$|q\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

We need to initialize in a superposed state

The Quantum Oracle

This is a typical way how oracle operates

- If x is not a solution, the oracle does nothing

$$|x\rangle(\tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle) \xrightarrow{O} |x\rangle(\tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle)$$

- If x is a solution, the oracle qubit is flipped

$$|x\rangle(\tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle) \xrightarrow{O} -|x\rangle(\tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle)$$

- We can write both of these as

$$|x\rangle(\tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle) \xrightarrow{O} (-1)^{f(x)}|x\rangle(\tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle)$$

- Or simply as

$$|x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle$$

Encodes input combination with changed sign in a superposition of all

This is a typical way how oracle operation is described

Role of Oracle

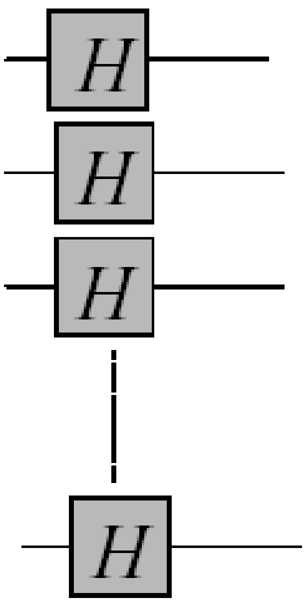
- We want to encode input combination with changed sign in a superposition of all states.
- This is done by Oracle together with Hadamards.
- We need a circuit to distinguish somehow globally good and bad states.

Hadamard gate

- Remembering the Hadamard gate,

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

- In a slight abuse of notation,



$$= H^{\otimes n}$$

Vector of Hadamards

Will be written simply as H

$$|\psi\rangle \equiv H|0\rangle = \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle$$

Zero state phase shift

All information of oracle is in the phase but how to read it?

$$|x\rangle \xrightarrow{Z} (-1)^{\partial_{x0}}|x\rangle$$

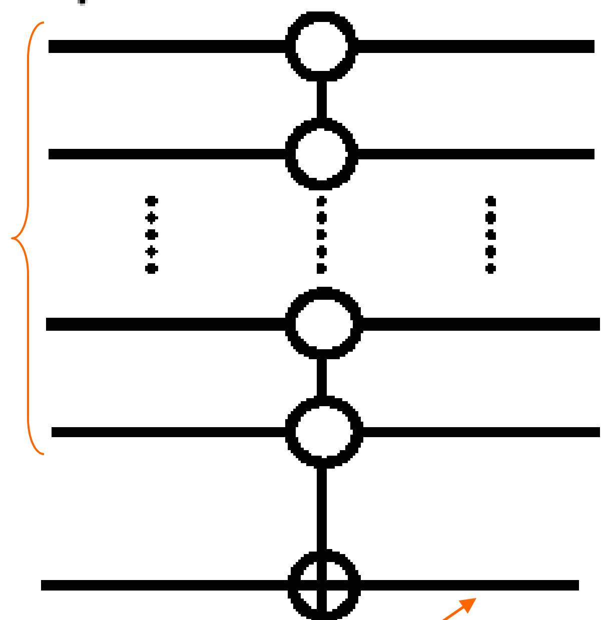
Flips the data phase

This is value of oracle bit

- One way to implement Z:

This is just an example of a single minterm, but can be any function

$|x\rangle$



$(-1)^{\partial_{x0}}|x\rangle$

$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ $\quad$ $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

- Flips the oracle qubit iff $|x\rangle = |0\rangle$

Zero state phase shift

- The matrix representation of Z

Flips the oracle bit when all bits are zero

$$Z = \begin{bmatrix} -1 & 0 & 0 & & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ & \vdots & & \ddots & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

This is state of all zeros

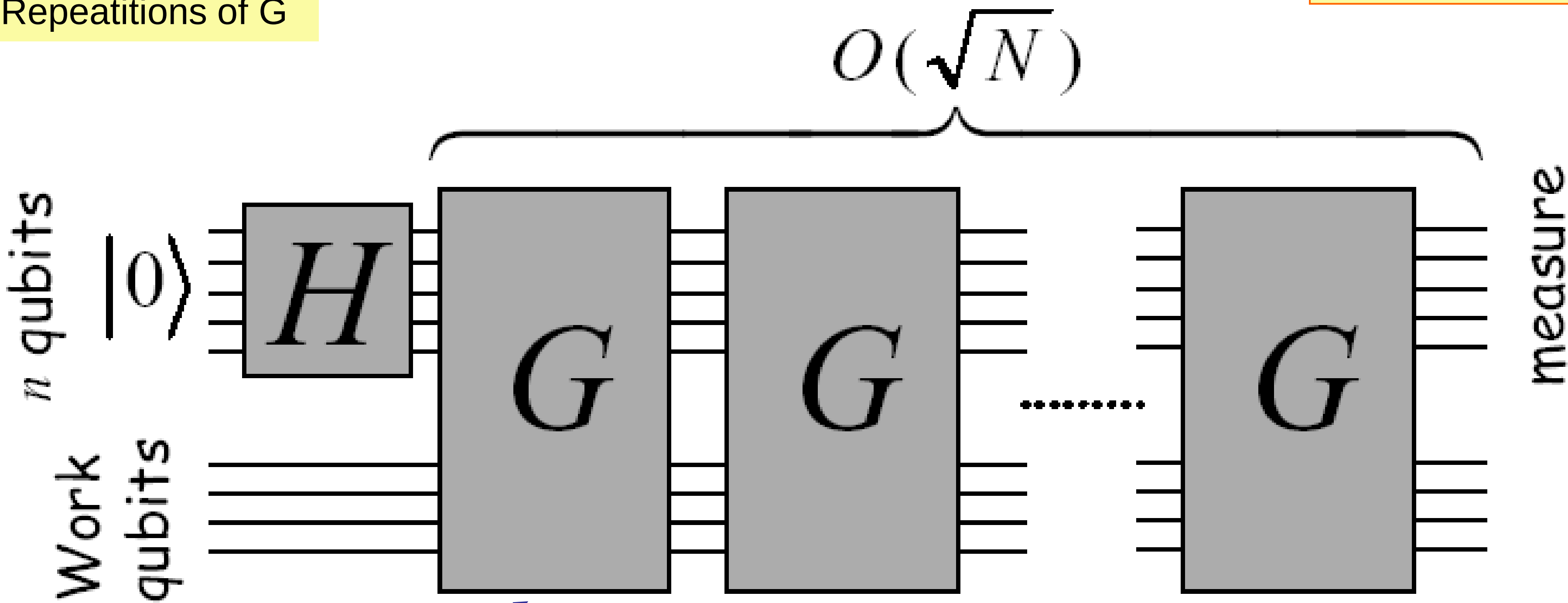
$$Z = 2|0\rangle\langle 0| - I$$

Rewriting matrix Z to Dirac notation, you can change phase globally

This is a global view of Grover. Repeatitions of G

Grover's Algorithm

Here you have all components of Grover's loop



$$G = HZHO$$

In each G

(1) Apply the oracle

(2) Apply the Hadamards

(3) Apply the zero state phase shift

(4) Apply the Hadamards

Generality

- Observe that a problem is described only by Oracle.
- So by changing the Oracle you can have your own quantum algorithm.
- You can still improve the Grover loop for particular special cases

Here we explain in detail what happens inside G. This can be generalized to G-like circuits

Grover Iterate

$$G = HZHO$$

Grover iterate has two tasks: (1) invert the solution states and (2) invert all states about the mean

- O: inverts the solution states
- HZH: invert all states about the mean

proof

$$\begin{aligned} &HZH \\ &H(2|0\rangle\langle 0| - I)H \\ &2H|0\rangle\langle 0|H - HIH \\ &2|\psi\rangle\langle\psi| - HIH \\ &2|\psi\rangle\langle\psi| - I \end{aligned}$$

Grover Iterate

$$HZH = 2|\psi\rangle\langle\psi| - I$$

$$(|\psi\rangle\langle\psi|)|\alpha\rangle = \frac{1}{N}\begin{bmatrix} 1 & 1 & 1 & & 1 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1 & & 1 \\ & \vdots & & \ddots & \\ 1 & 1 & 1 & & 1 \end{bmatrix}\begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_N \end{bmatrix} = \begin{bmatrix} \frac{\sum \alpha_n}{N} \\ \frac{\sum \alpha_n}{N} \\ \frac{\sum \alpha_n}{N} \\ \vdots \\ \frac{\sum \alpha_n}{N} \end{bmatrix}$$

$\bar{a}$

Here we prove that $|\psi\rangle\langle\psi|$ used inside HZH calculates the mean

Grover Iterate

$$HZH = 2|\psi\rangle\langle\psi| - I$$

From previous slide

$$HZH|\alpha\rangle = (2|\psi\rangle\langle\psi| - I)\sum_n \alpha_n |n\rangle$$

$$= \sum_n (2\overline{\alpha} - \alpha_n |n\rangle)$$

HZH: invert all states about the mean

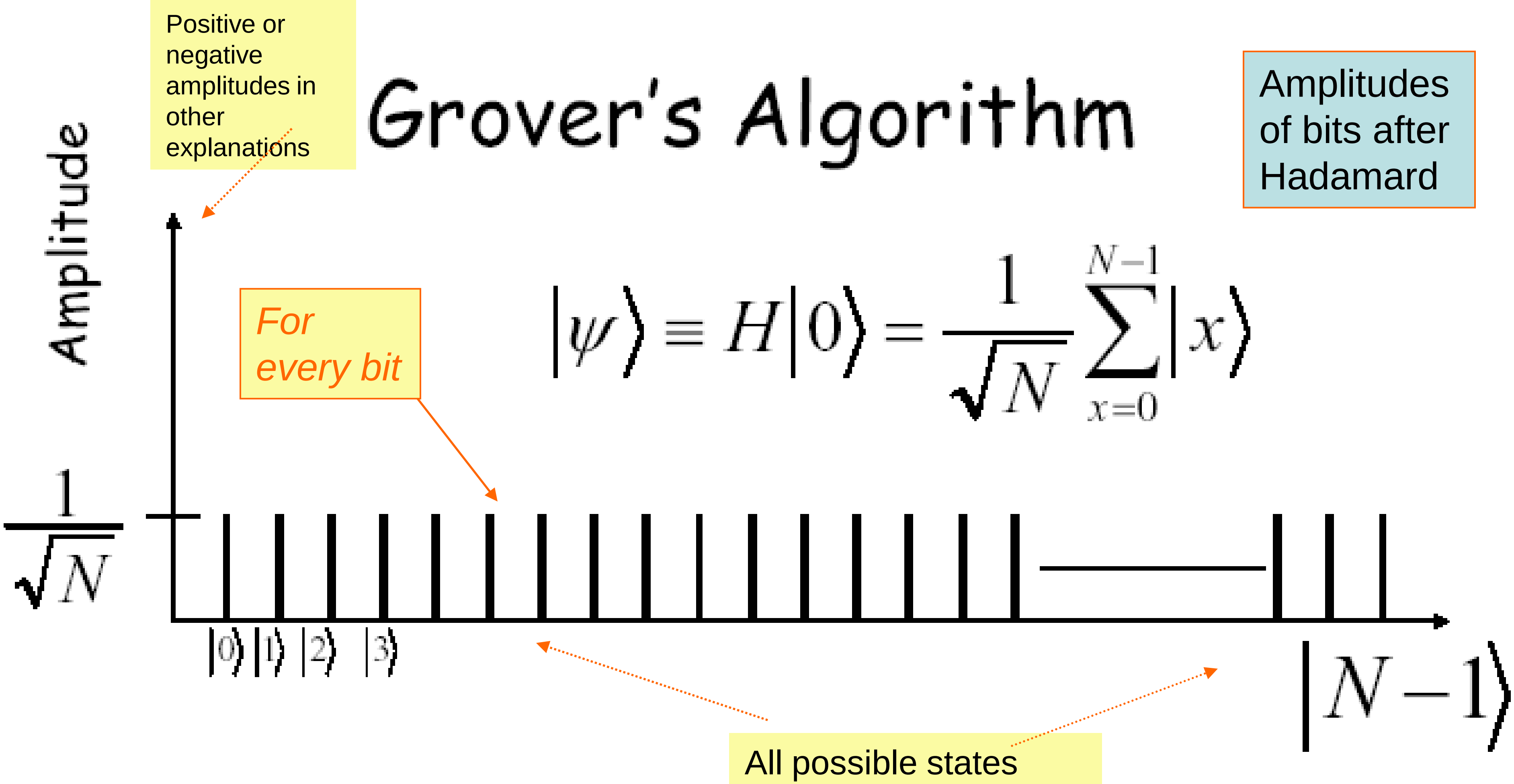
This proof is easy and it only uses formalisms that we already know.

What does it mean invert all states about the mean?

Grover's Algorithm

Amplitudes of bits after Hadamard

$$|\psi\rangle \equiv H|0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$



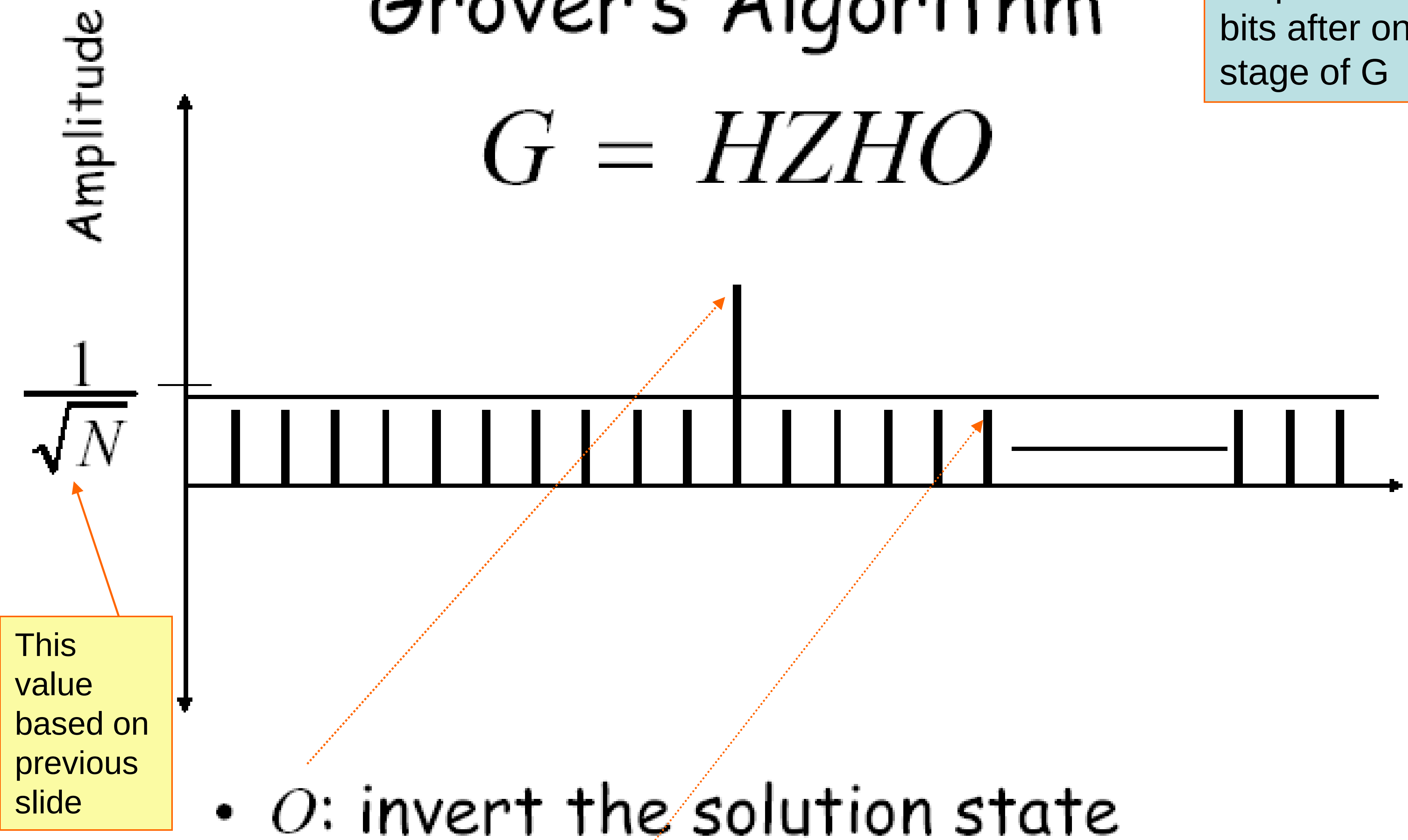
- The probability of measuring the marked state,

$$P(m) = \frac{1}{N} = \frac{1}{2^n}$$

Grover's Algorithm

Amplitudes of bits after one stage of G

$$G = HZHO$$

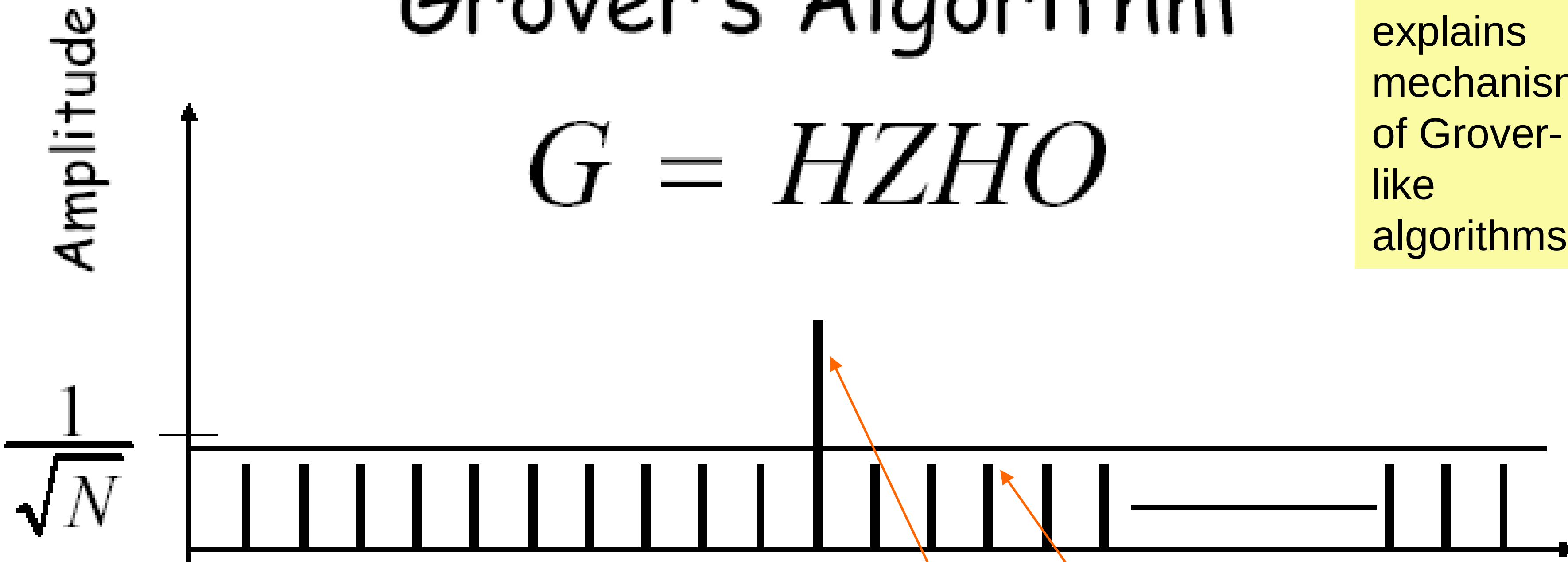


- O: invert the solution state
- HZH: invert all states about the mean

Grover's Algorithm

This slides explains mechanism of Grover-like algorithms

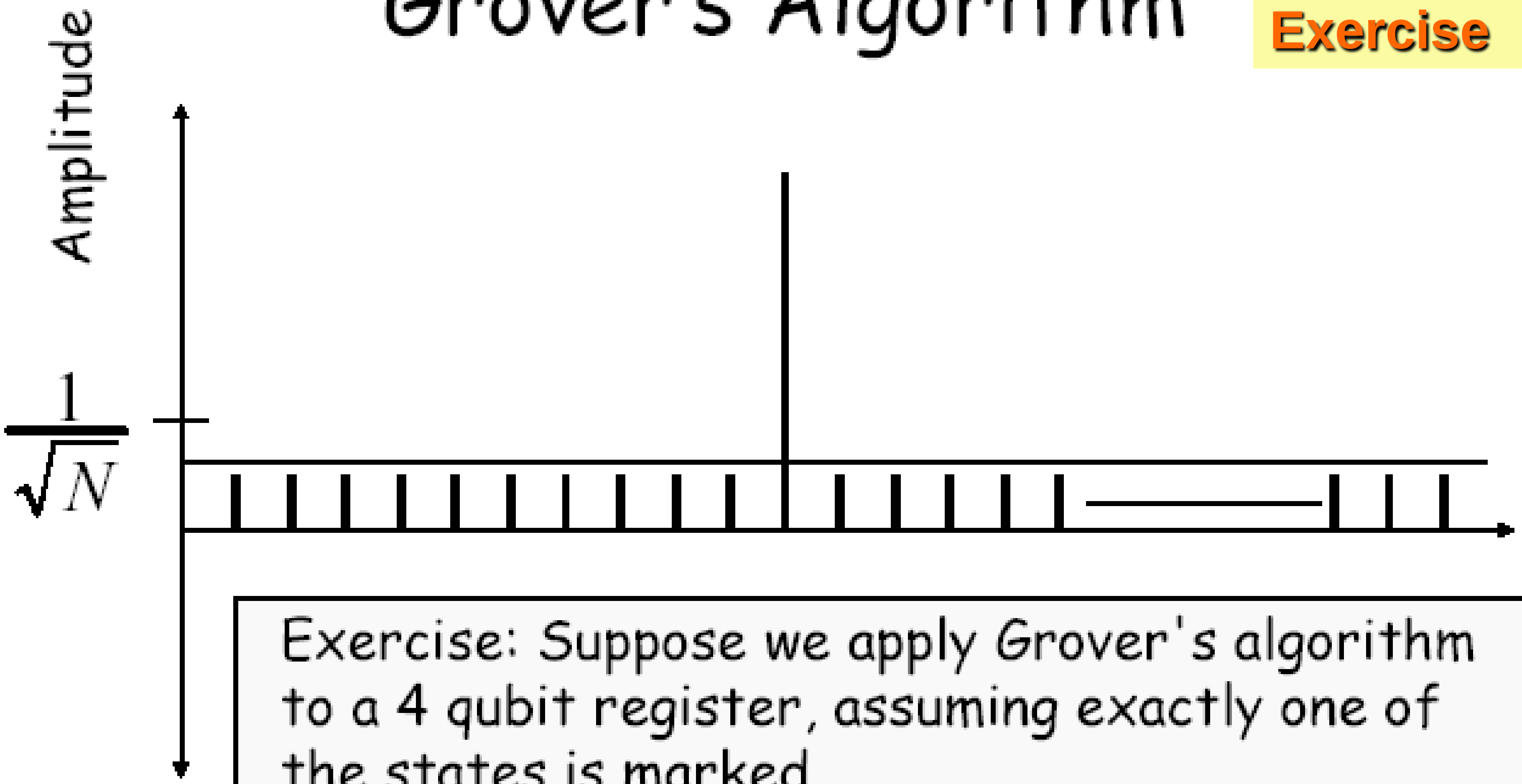
$$G = HZHO$$



- The unmarked states decreased by a very small amount
- The marked state increased by $O(\frac{1}{\sqrt{N}})$
- To get P(m) = O(1), we need to apply the Grover iterate $O(\sqrt{N})$ times.

Grover's Algorithm

Additional Exercise



Exercise: Suppose we apply Grover's algorithm to a 4 qubit register, assuming exactly one of the states is marked.

What is the probability of measuring the marked state after applying the Grover iterate 0,1,2,3 times?

You can verify it also in simulation

How many Grover iterates do we need?

- Initial amplitudes of the marked and unmarked states:

$$m_0 = \frac{1}{\sqrt{N}} \qquad u_0 = \frac{1}{\sqrt{N}}$$

Here we calculate analytically when to stop

- After inverting the marked state, the average amplitude is

$$a_i = \frac{(N-1)u_{i-1} - m_{i-1}}{N}$$

- Completing the Grover iterate

For marked state

$$m_i = 2a_i + m_{i-1}$$

For unmarked state

$$u_i = 2a_i - u_{i-1}$$

The equations taken from the previous slides "Grover Iterate"

How many Grover iterates do we need?

- Substituting a_i in gives

recursion

$$m_i = 2(1-\tfrac{1}{N})u_{i-1} + (1-\tfrac{2}{N})m_{i-1}$$

$$u_i = 2(1-\tfrac{2}{N})u_{i-1} - \tfrac{2}{N}m_{i-1}$$

We want to find how many times to iterate

- We would like to find k, such that

$$|m_k| \geq \frac{1}{\sqrt{2}} \quad \text{so that} \quad P(m_k) \geq \frac{1}{2}$$

We found k from these equations

- Note that

$$\begin{bmatrix} m_k \\ u_k \end{bmatrix} = \begin{bmatrix} 1-\frac{2}{N} & 2-\frac{2}{N} \\ -\frac{2}{N} & 1-\frac{2}{N} \end{bmatrix}^k \begin{bmatrix} \frac{1}{\sqrt{N}} \\ \frac{1}{\sqrt{N}} \end{bmatrix}$$

$$k = \left\lceil \frac{\pi\sqrt{N}}{4} \right\rceil$$

Generalizations of Grover's Algorithm

- What if we have more than one marked state?

$$k = \left\lceil \frac{4}{\pi} \sqrt{\frac{N}{M}} \right\rceil$$

  - M: Number of solutions
  - M < N/2

- What if we use a different initial state?
  - The algorithm still works

- What if we alter the Grover iterate?
  - The algorithm still works

Optimality of search algorithm

- Classically, if all you can do is ask questions of the oracle
  - The best you can do is $O(N)$

- Quantumly, if all you can do is ask questions of the oracle
  - The best you can do is $O(\sqrt{N})$

Summary

- Used to solve a problem that you don't know much about:
  - Unsorted databases
  - NP-complete problems
- Problems remain intractable
- Square-root speed-up