

# Grover's algorithm

## Problem

Unsorted states:  $S = \{S_1, S_2, \dots, S_N\}$

Condition function:  $C(|S_i\rangle) = d_{iu}$

Mission: find  $S_v$  from  $S$

## Algorithm

(i) Initialization:  $|y\rangle = \frac{1}{\sqrt{N}}(|S_1\rangle + |S_2\rangle + \dots + |S_N\rangle)$

(ii) Repeat the following operations  $O(\sqrt{N})$  times:

(a) Let the system be in any state  $S_i$ :

If  $C(|S_i\rangle) = 1$ , rotate the phase of by  $\pi$  radians;

If  $C(|S_i\rangle) = 0$ , leave the system unaltered.

(b) Apply the diffusion transform  $D = -I + 2P$

where  $P_{ij} = \frac{1}{N}$  is the amplitude average operator.

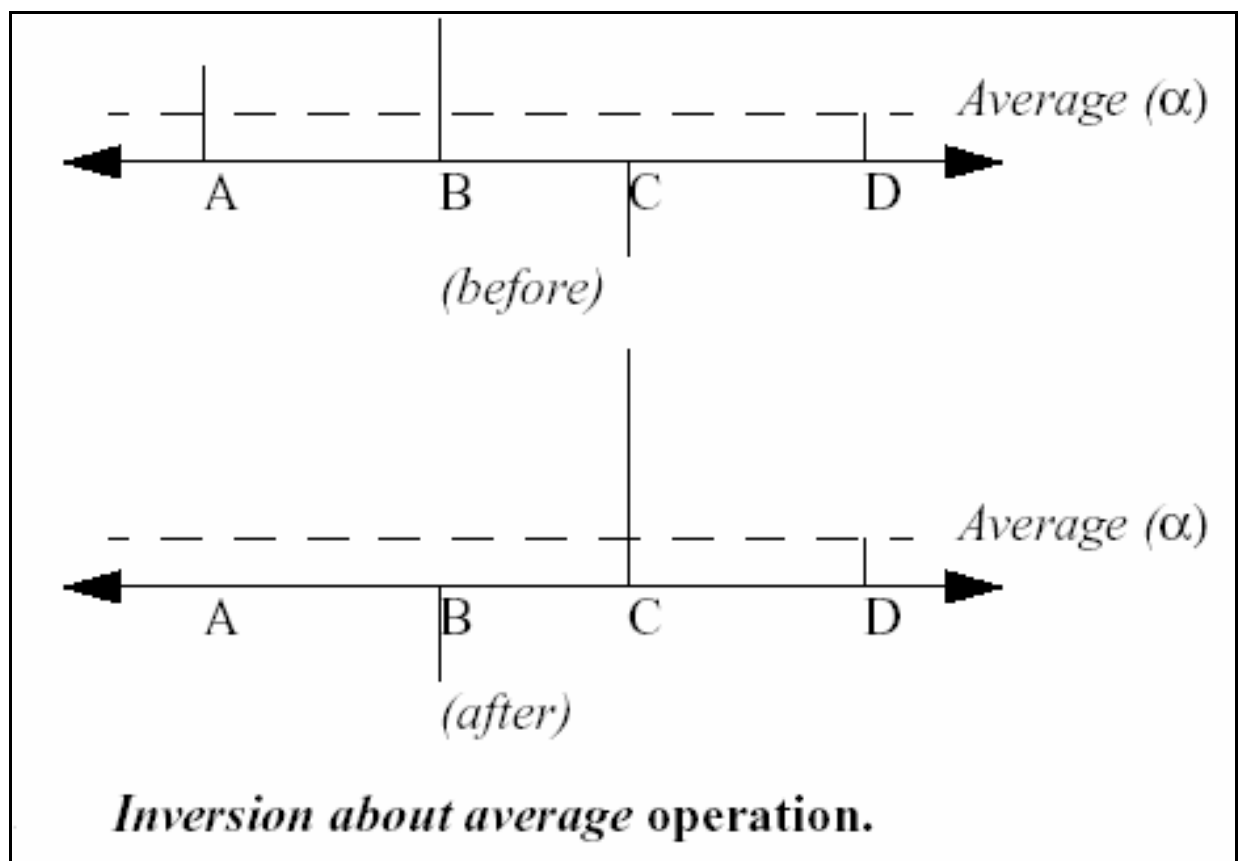
(iii) Measure the resulting state.  $S_v$

appears with a probability of at least 0.5

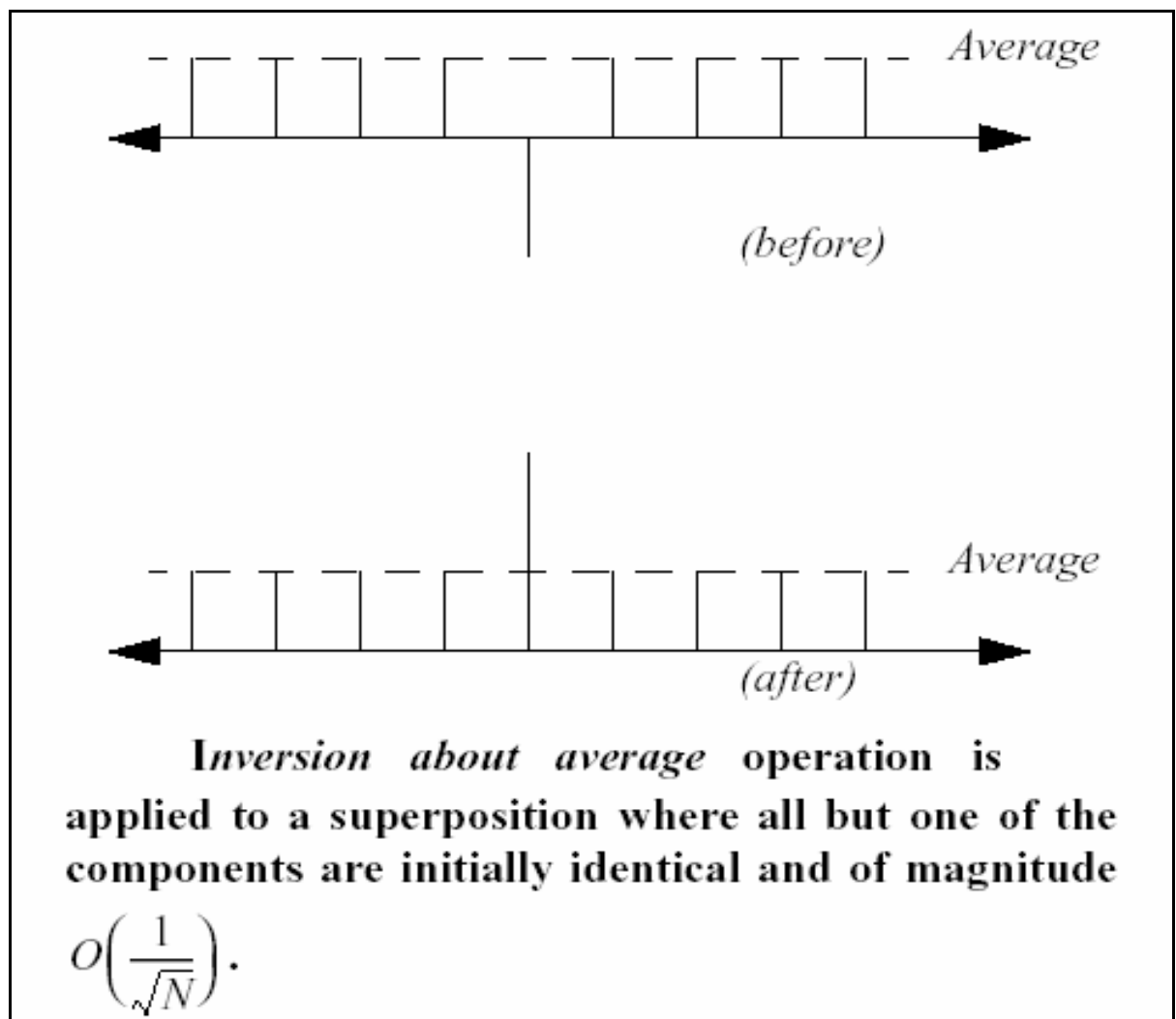
## Mechanism

$$D\bar{n} = (-I + 2P)\bar{n} = -\bar{n} + 2P\bar{n}$$

$\Rightarrow$  D is the inversion operation about average:



For the case one component with  
amplitude  $= -\sqrt{1-C^2}$  / others with amplitude  $= C / \sqrt{N}$ ,  
step (ii) results in the magnitude increase  $2C / \sqrt{N}$   
(=distance from average +average-original value  
 $= (\sqrt{1-C^2} + C / \sqrt{N}) + C / \sqrt{N} - \sqrt{1-C^2}$  )  
to this special component:



Once its magnitude  $\sqrt{1-C^2} < 1/\sqrt{2}$ , the increase

$$\frac{2C}{\sqrt{N}} > \frac{1}{\sqrt{2N}}. \text{ Hence there exists a } M < \sqrt{N}$$

such that perform step (ii)  $M$  times, the desired

state appears with a probability greater than 0.5.