

## II. Grover's algorithm

- algorithm "searching an unsorted database" with  $N=2^n$  elements in  $\Theta(\sqrt{N})$  time rather: find  $x$  s.t.  $f(x)=1$

→ classical alg. needs on average  $\frac{N}{2} = \Theta(N)$  time

- goal: find  $\omega$ , given an oracle  $U_f$  with  $f: \{0,1\}^n \rightarrow \{0,1\}$ ,  $f(x) = \begin{cases} 1, & \text{if } x=\omega \\ 0, & \text{else} \end{cases}$ ,  $f_0(x) = \begin{cases} 0, & \text{if } x=0..0 \\ 1, & \text{else} \end{cases}$

$$\text{phase oracle: } U_f(x) = (-1)^{f(x)} = |x\rangle \Rightarrow U_f: |\omega\rangle \rightarrow -|\omega\rangle$$

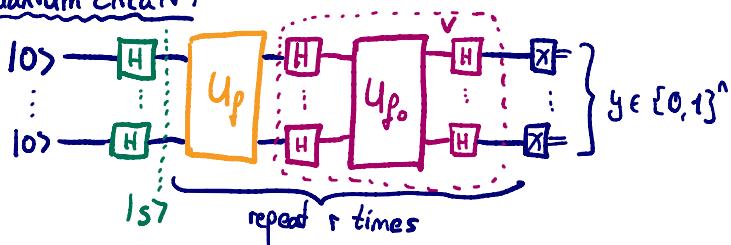
$$|x\rangle \rightarrow |x\rangle \oplus x \omega \quad \Rightarrow U_f: |0\rangle^{\otimes n} \rightarrow |0\rangle^{\otimes n}$$

$$|x\rangle \rightarrow -|x\rangle \quad \text{if } x \neq 0..0$$

$$\hookrightarrow U_f = 1 - 2|\omega\rangle\langle\omega|$$

$$\hookrightarrow U_{f_0} = 2|0\rangle\langle 0|^{\otimes n} - 1I$$

quantum circuit:



Claim:  $y = \omega$  (with high prob.)

Proof: Let us define the uniform superposition state  $|s\rangle := H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$

$$\text{and } V := H^{\otimes n} \cdot U_{f_0} \cdot H^{\otimes n} = H^{\otimes n} \cdot 2|0\rangle\langle 0|^{\otimes n} \cdot H^{\otimes n} - H^{\otimes n} \cdot H^{\otimes n} = 2|s\rangle\langle s| - 1I$$

⇒ Grover's algorithm carries out the operation  $(V \cdot U_f)^r$  on the state  $|s\rangle$ .

Let  $\Sigma$  be the plane spanned by  $|s\rangle$  and  $|\omega\rangle$  and let  $|\omega^\perp\rangle$  be the state

$$\text{orthogonal to } |\omega\rangle \text{ in } \Sigma: \quad |\omega^\perp\rangle := \frac{1}{\sqrt{2^n-1}} \sum_{x \neq \omega} |x\rangle$$

$$\Rightarrow |s\rangle = \sqrt{\frac{2^n-1}{2^n}} |\omega^\perp\rangle + \frac{1}{\sqrt{2^n}} |\omega\rangle = \cos \frac{\theta}{2} |\omega^\perp\rangle + \sin \frac{\theta}{2} |\omega\rangle$$

$$\begin{aligned} \text{define } \theta \text{ s.t. } \sin \frac{\theta}{2} &= \frac{1}{\sqrt{2^n}} \\ \Rightarrow \theta &= 2 \cdot \arcsin \frac{1}{\sqrt{2^n}} \end{aligned}$$

protocol:

1.) Prepare  $|s\rangle$

2.) Apply  $U_f = 1 - 2|\omega\rangle\langle\omega|$  → reflection at  $|\omega^\perp\rangle$

3.) Apply  $V = 2|s\rangle\langle s| - 1I$  → reflection at  $|s\rangle$

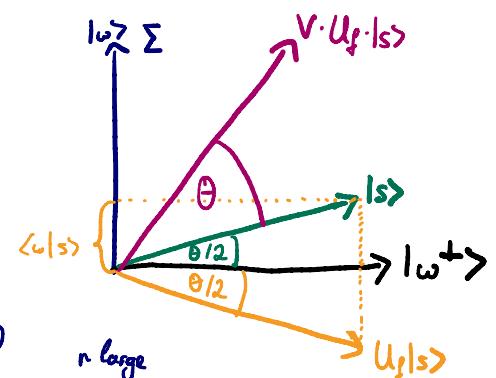
⇒  $V \cdot U_f$  corresponds to a rotation by an angle  $\theta$

⇒ after  $r$  applications of 2) & 3), the state is rotated by  $r \cdot \theta$

$$\hookrightarrow \text{choose } r, \text{ s.t. } r \cdot \theta + \frac{\theta}{2} \approx \frac{\pi}{2} \Rightarrow r = \frac{\pi}{2\theta} - \frac{1}{2} = \frac{\pi}{4 \cdot \arcsin \frac{1}{\sqrt{2^n}}} - \frac{1}{2} \approx \frac{\pi}{4} \sqrt{2^n} = O(\sqrt{N})$$

⇒ after  $r$  calls to the oracle, the final meas. will result in state  $|\omega\rangle$  with min. probability

$$p(\omega) \geq 1 - \sin^2 \frac{\theta}{2} = 1 - \frac{1}{2^n} \quad (\text{if } \xrightarrow{\text{Up}} |\omega^\perp\rangle)$$

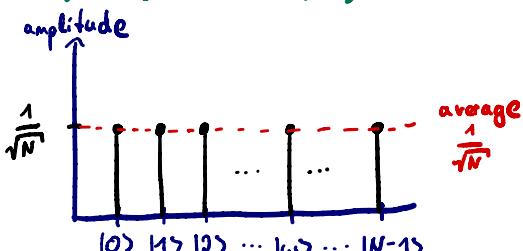


□

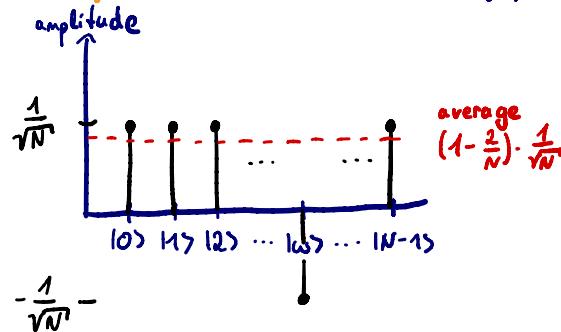
## Amplitude amplification

The general idea behind Grover's algorithm is amplitude amplification. Let us have a look at the amplitudes at each step in Grover's algorithm:

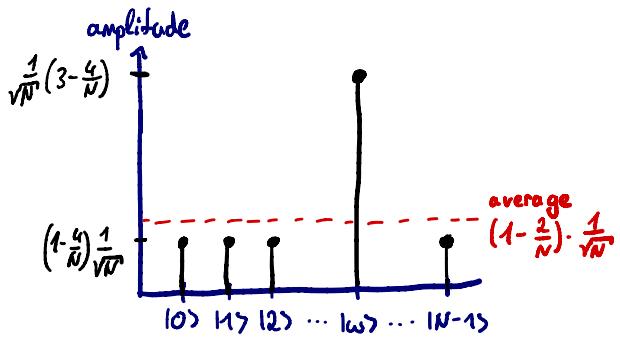
$$1.) |s\rangle := H^{\otimes n} |0\rangle^{\otimes n}$$



$$2.) U_f |s\rangle = (1 - 2|\alpha_x\rangle\langle\alpha_x|) |s\rangle \rightarrow \text{flip amplitude of } |\alpha_x\rangle$$



$$3.) V \cdot U_f \cdot |s\rangle = (2|s\rangle\langle s| - 1) \cdot U_f \cdot |s\rangle \rightarrow \text{reflect amplitude about the average amplitude}$$



As for  $|q\rangle := \sum_i \alpha_i |i\rangle \quad V|q\rangle$  gets:

$$(2|s\rangle\langle s| - 1)|q\rangle = 2 \cdot \frac{1}{N} \cdot \sum_j |j\rangle \cdot \sum_k \langle k| \cdot \sum_i \alpha_i |i\rangle - \sum_i \alpha_i |i\rangle$$

$$= 2 \cdot \frac{\sum_k \alpha_k}{N} \cdot \sum_j |j\rangle - \sum_j \alpha_j |j\rangle$$

$$= \sum_j (2 \cdot \langle \alpha \rangle - \alpha_j) |j\rangle$$

Reflection of  $\alpha_j$  about average  $\langle \alpha \rangle$  ( $\rightarrow$  if  $\alpha_j = \langle \alpha \rangle + \Delta$  then  $\alpha_j' = 2\langle \alpha \rangle - \alpha_j - \langle \alpha \rangle - \Delta$ )

$\Rightarrow$  by repeating step 2) & 3), the amplitude of  $|\alpha_x\rangle$  will increase further  $\Rightarrow$  amplitude amplification!

## Multiple marked elements

When we have  $M$  marked elements  $\omega_i$ , we define the winning state as

$$|\omega\rangle := \frac{1}{\sqrt{M}} \sum_{i=1}^M |\omega_i\rangle \quad \rightarrow \quad |\omega^\perp\rangle = \frac{1}{\sqrt{N-M}} \cdot \sum_{x \notin \{\omega_1, \dots, \omega_M\}} |x\rangle$$

$$\Rightarrow |s\rangle = \frac{\sqrt{N-M}}{\sqrt{N}} \cdot |\omega^\perp\rangle + \sqrt{\frac{M}{N}} \cdot |\omega\rangle =: \cos \frac{\theta}{2} |\omega^\perp\rangle + \sin \frac{\theta}{2} |\omega\rangle$$

$$\hookrightarrow \sin \frac{\theta}{2} = \sqrt{\frac{M}{N}} \quad \rightarrow \text{angle becomes larger!}$$

$$\Rightarrow r = \frac{\pi}{4 \cdot \arcsin(\sqrt{\frac{M}{N}})} - \frac{1}{2} = O(\sqrt{\frac{N}{M}})$$

→ we can see this speedup also when looking at the amplitudes:

