An Introduction to Quantum Computing

Lecture 08

Grover's Quantum Search Algorithm

Paolo Zuliani

zuliani@di.uniroma1.it

SAPIENZA
UNIVERSITÀ DI ROMA

Outline

- The Search Problem
- Grover’s algorithm

The Problem: Finding a Needle in a Haystack

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
78	655	***9797***	3249	6	13	877	56	8789	10	999	1548	***354***	75	1875	9

- Array of length $N = 2^n$ with $1 \leq M \leq N$ "solution" elements
- **Problem**: Find the index of a solution element

- Classical (random): $O(\frac{N}{M})$ array accesses in the worst case
- Quantum: Grover's algorithm returns a correct index ***with high probability***, with only $O(\sqrt{\frac{N}{M}})$ array accesses!

[$f(x) = O\big(g(x)\big)$ for $x \to \infty$ if $|f(x)| \leq K|g(x)|$ for some constant K and large x]

Towards the Quantum Algorithm

- Let A be our array of size $N = 2^n$
- Array indices can then be encoded with n bits

- We "encode" the solutions via the Boolean function

$$f:\{0,\dots,N-1\} \to \{0,1\}$$

$$f(i) = \begin{cases} 0 & \text{if } A[i] \text{ is } \textbf{not} \text{ a solution} \\ 1 & \text{if } A[i] \text{ is a solution} \end{cases}$$

Towards the Quantum Algorithm

For our $f: \{0, \dots, N-1\} \rightarrow \{0,1\}$ we build the unitary U_f

$$U_f: |x \otimes y\rangle \rightarrow |x \otimes (y \oplus f(x))\rangle$$

where x is a quantum register of length n and y is a qubit. Also, recall that:

$$U_f|x \otimes 0\rangle = |x \otimes f(x)\rangle \qquad U_f|x \otimes 1\rangle = |x \otimes \neg f(x)\rangle$$

Let's see what happens when $y = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ …

Towards the Quantum Algorithm

$$U_f\,|x\otimes\tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\rangle =$$

$$|x\otimes\tfrac{1}{\sqrt{2}}(|f(x)\rangle - |\neg f(x)\rangle)\rangle = \begin{cases} |x\otimes\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\rangle & \text{if } f(x) = 0 \\ |x\otimes\frac{1}{\sqrt{2}}(|1\rangle - |0\rangle)\rangle & \text{if } f(x) = 1 \end{cases}$$

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

Note that the (right-hand side) qubit is returned unaltered.

Towards the Quantum Algorithm

We can conveniently drop the RHS qubit and obtain the "**oracle**"

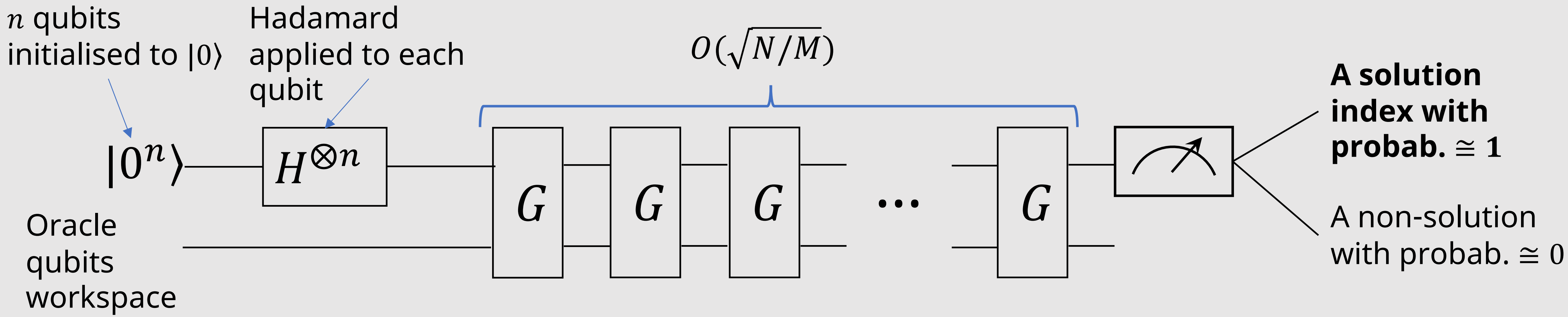
$$O_f|x\rangle = (-1)^{f(x)}|x\rangle$$

that 'flips' the amplitude of the solution elements!

Grover's algorithm is an example of **oracle** (or **black-box**) quantum algorithms.

The Deutsch-Jozsa algorithm is another one.

Grover's Quantum Circuit

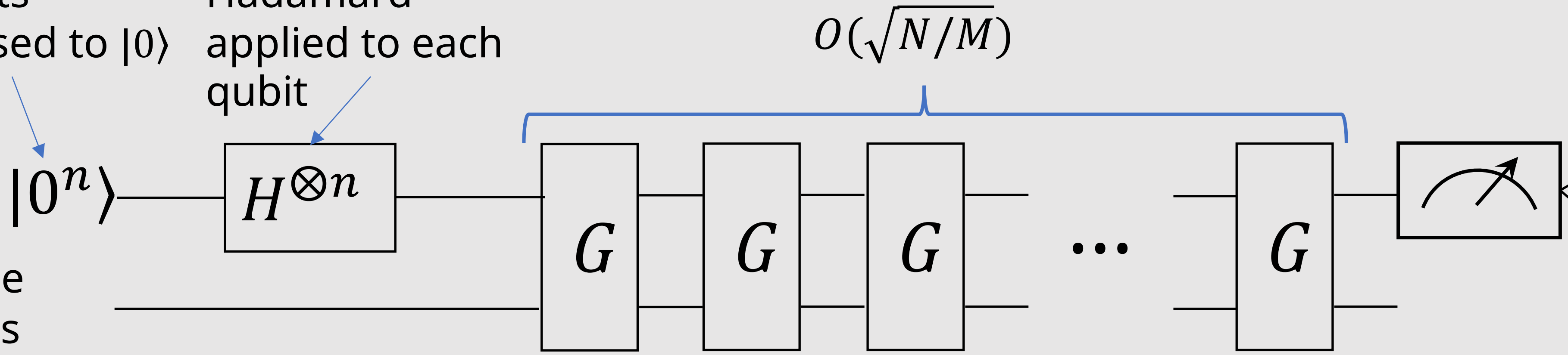


What is G? (And let's forget the oracle workspace.)

Grover's Quantum Circuit

n qubits initialised to $|0\rangle$

Hadamard applied to each qubit



A solution index with probab. $\cong 1$

A non-solution with probab. $\cong 0$

Oracle qubits workspace

In general, the state of the n qubits is

$$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \qquad \text{(with } \sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1\text{)}$$

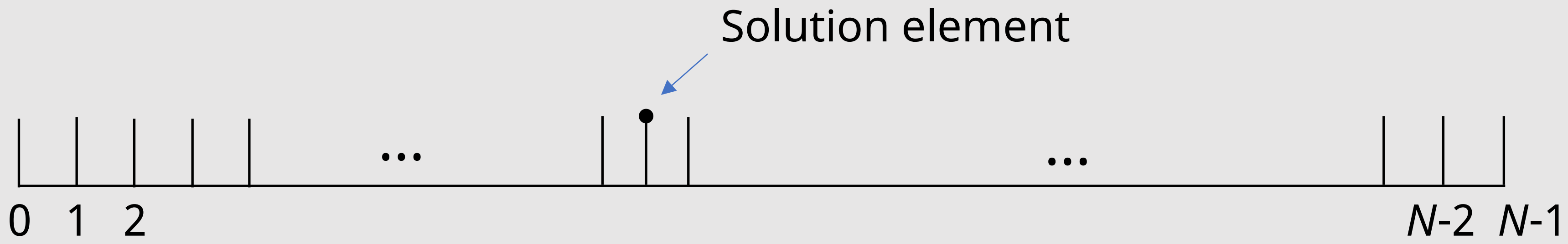
$$G = W \cdot O_f \quad \text{where} \quad W|x\rangle = (-\alpha_x + 2\langle\alpha\rangle)|x\rangle \qquad \langle\alpha\rangle = \frac{1}{N} \sum_{x \in \{0,1\}^n} \alpha_x$$

inversion about the mean
(a unitary transform!)

mean amplitude

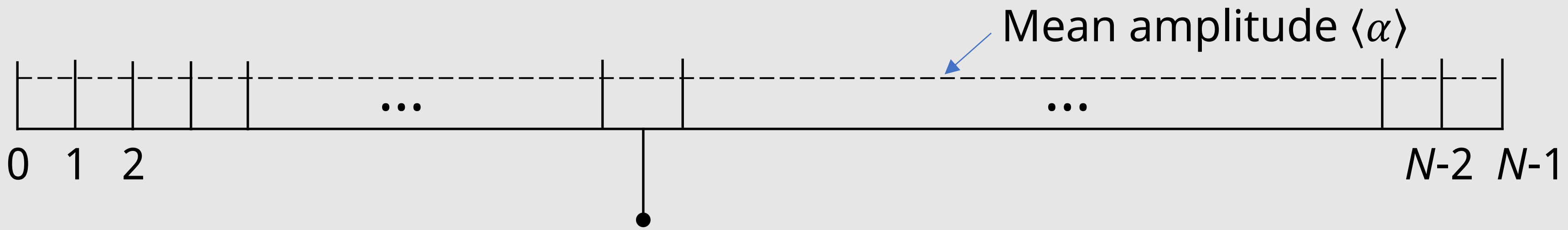
Grover's Iteration G

After the Hadamard, all amplitudes are (real) and equal to $\frac{1}{\sqrt{N}}$



Apply oracle
$O_f|x\rangle = (-1)^{f(x)}|x\rangle$

Apply inversion about mean
$W|x\rangle = (-\alpha_x + 2\langle\alpha\rangle)|x\rangle$



We have (unitarily) increased the amplitude of a solution!!

Apply oracle
$O_f|x\rangle = (-1)^{f(x)}|x\rangle$

Understanding G

Let $S = \{\text{solution indices}\}$ (in our example $S = \{2, 12\}$)
Define the vectors

Superposition of ***non-solution*** indices

$$|a\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \in \bar{S}} |x\rangle \qquad |b\rangle = \frac{1}{\sqrt{M}} \sum_{x \in S} |x\rangle$$

Superposition of ***solution*** indices

Note $\{0,1\}^n = \bar{S} \cup S$. Recall that after $H^{\otimes n}$ the state is

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$$

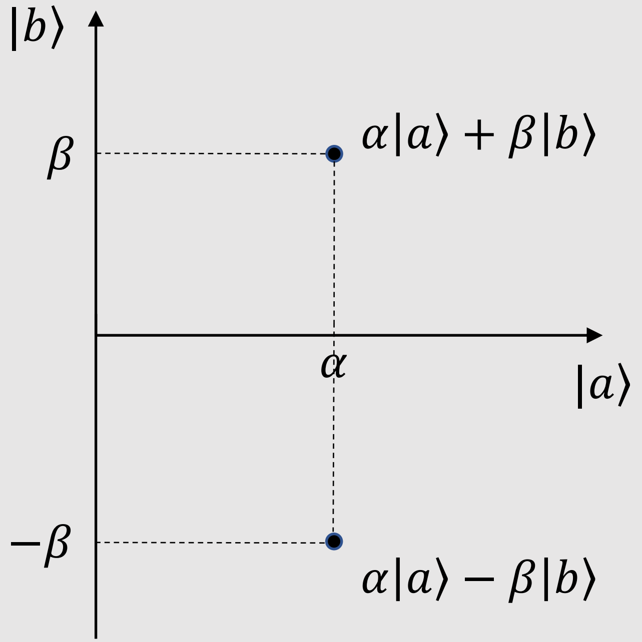
hence

$$|\psi\rangle = \sqrt{\frac{N-M}{N}} |a\rangle + \sqrt{\frac{M}{N}} |b\rangle$$

Understanding G

Recall that O_f inverts the sign of the <u>solution amplitudes</u>:

$$O_f|\psi\rangle = O_f(\alpha|a\rangle + \beta|b\rangle) = \alpha|a\rangle - \beta|b\rangle$$



O_f performs a *reflection* about $|a\rangle$!

Understanding G

Recall that $W|x\rangle = (2\langle\alpha\rangle - \alpha_x)|x\rangle$, where $|x\rangle$ is a basis vector

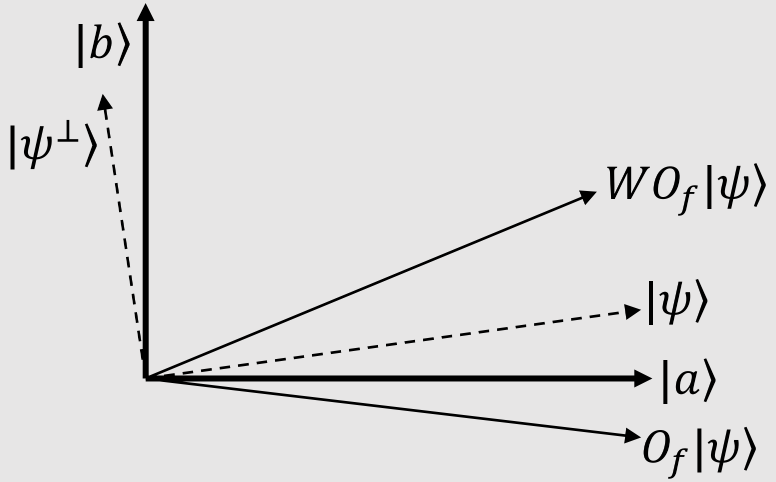
Equivalently $\quad W = 2P_\psi - I$

where P_ψ is the *projection* operator over $|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x\in\{0,1\}^n}|x\rangle$

Now, $W = 2P_\psi - I = 2P_\psi - \left(P_\psi + P_{\psi^\perp}\right) = P_\psi - P_{\psi^\perp}$

W performs a *reflection* about $|\psi\rangle$!

$G = WO_f$ is thus a *rotation* in the plane defined by $|a\rangle$ and $|b\rangle$!!



Understanding G

Let $\theta/_2$ be the angle between $|a\rangle$ and $|\psi\rangle$

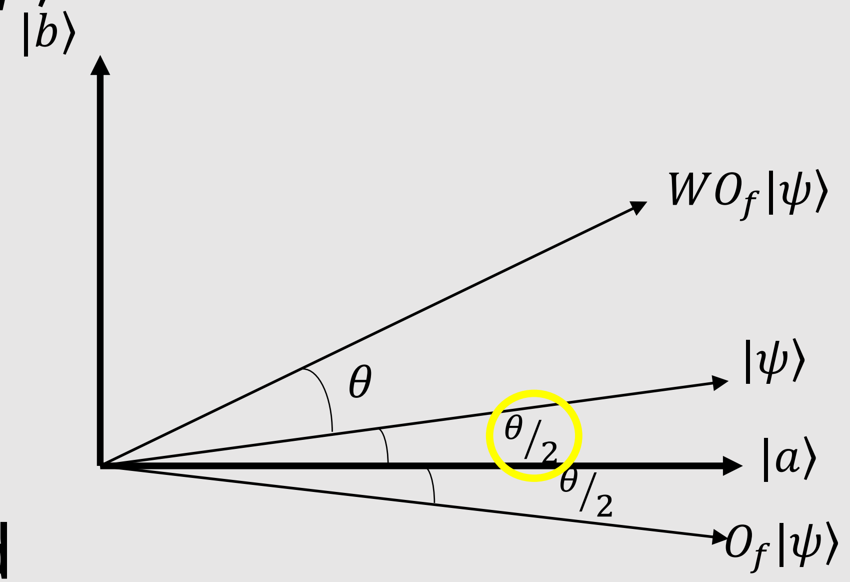
Since $|\psi\rangle = \sqrt{\frac{N-M}{N}}|a\rangle + \sqrt{\frac{M}{N}}|b\rangle$ we have

$\cos\theta/_2 = \sqrt{\frac{N-M}{N}}$ and $\sin\theta/_2 = \sqrt{\frac{M}{N}}$

Hence $|\psi\rangle = \cos\theta/_2\,|a\rangle + \sin\theta/_2\,|b\rangle$ and

$G|\psi\rangle = WO_f|\psi\rangle = \cos{}^{3\theta}/_2\,|a\rangle + \sin{}^{3\theta}/_2\,|b\rangle$ (rotation by θ)

$$\boxed{G^k|\psi\rangle = \cos\frac{(2k+1)\theta}{2}|a\rangle + \sin\frac{(2k+1)\theta}{2}|b\rangle \qquad (k = 0, 1, 2, 3, \dots)}$$

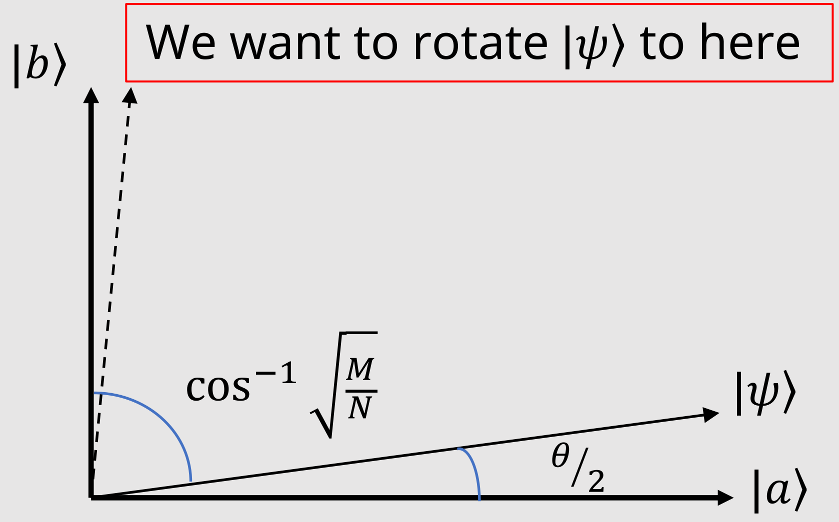


How Many Iterations of G?

Superposition of ***non-solution*** indices

Superposition of ***solution*** indices

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}|a\rangle + \sqrt{\frac{M}{N}}|b\rangle$$



To increase the probability of success, *i.e.*, finding a solution, we need to ***rotate*** $|\psi\rangle$ ***towards*** $|b\rangle$.

Now, each application of G is a rotation by θ. Thus, applying G

$k = \left\lfloor \left(\frac{\cos^{-1}\sqrt{\frac{M}{N}}}{\theta} \right) \right\rfloor$ times gets us to *within an angle* $\frac{\pi}{4}$ of $|b\rangle$!

A measurement will return a solution with probability *at least* 50%!

How Many Iterations of G?

Assuming $M \leq \frac{N}{2}$ ensures that $\theta \leq \frac{\pi}{2}$.

Now, note that $k = \left\lfloor \left(\frac{\cos^{-1} \sqrt{\frac{M}{N}}}{\theta} \right) \right\rfloor \leq \left\lceil \frac{\pi}{2\theta} \right\rceil$, since $\cos^{-1} \leq \frac{\pi}{2}$. Thus

$\sqrt{\frac{M}{N}} = \sin \frac{\theta}{2} \leq \frac{\theta}{2}$ and therefore $\frac{1}{\theta} \leq \frac{1}{2} \sqrt{\frac{N}{M}}$

and thus

$$\boxed{k = \left\lfloor \left(\frac{\cos^{-1} \sqrt{\frac{M}{N}}}{\theta} \right) \right\rfloor \leq \left\lceil \frac{\pi}{2\theta} \right\rceil \leq \left\lceil \frac{\pi}{4} \sqrt{\frac{N}{M}} \right\rceil}$$

How to remove the $M \leq \frac{N}{2}$ requirement?