Quantum Computation
(Lecture 3)

Luís Soares Barbosa

Universidade do Minho

HASLab
HIGH-ASSURANCE SOFTWARE LABORATORY

INL
INTERNATIONAL IBERIAN NANOTECHNOLOGY LABORATORY

UNITED NATIONS UNIVERSITY
UNU-EGOV

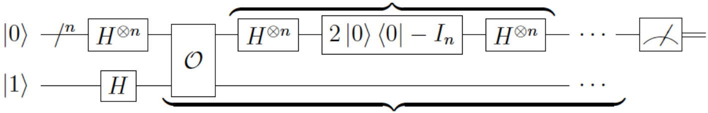
MSc Physics Engineering

Universidade do Minho, 2021-22

Grover's algorithm

Recall Grover's algorithm:

- Prepare the initial state: $|0\rangle^{\otimes n}|1\rangle$
- Apply $H^{\otimes n} \otimes H$ to yield $\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|-\rangle$
- Apply the Grover iterator G to $\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|-\rangle$ a suitable number of times to obtain state $|a\rangle|-\rangle$ with high probability
- Measure the first n qubits to retrieve $|a\rangle$



A geometric perspective on G

Initial state: $|\psi\rangle \;=\; \frac{1}{\sqrt{N}}|a\rangle \;+\; \sqrt{\frac{N-1}{N}}|r\rangle$
The repeated application of G leaves the system in the 2-dimensional subspace of the original N-dimensional space, spanned by $|a\rangle$ and $|r\rangle$.

Another basis is given by $|\psi\rangle$ and the state orthogonal to $|\psi\rangle$:

$$|\overline{\psi}\rangle \;=\; \sqrt{\frac{N-1}{N}}|a\rangle \;-\; \frac{1}{\sqrt{N}}|r\rangle$$

Define an angle θ st $\sin\theta = \frac{1}{\sqrt{N}}$ (and, of course, $\cos\theta = \sqrt{\frac{N-1}{N}}$), and express both bases as

$$\begin{array}{rclrcl} |\psi\rangle &=& \sin\theta|a\rangle + \cos\theta|r\rangle & |\overline{\psi}\rangle &=& \cos\theta|a\rangle - \sin\theta|r\rangle \\ |a\rangle &=& \sin\theta|\psi\rangle + \cos\theta|\overline{\psi}\rangle & |r\rangle &=& \cos\theta|\psi\rangle - \sin\theta|\overline{\psi}\rangle \end{array}$$

A geometric perspective on G

G has two components:

- V which applies a phase shift to $|a\rangle$: reflection over $|r\rangle$.
- W which applies a phase shift to all vectors in the subspace orthogonal to $|\psi\rangle$: reflection over $|\psi\rangle$.

Let's express the action of V in the basis $|\psi\rangle, |\overline{\psi}\rangle$ to perform afterwards the second reflection:

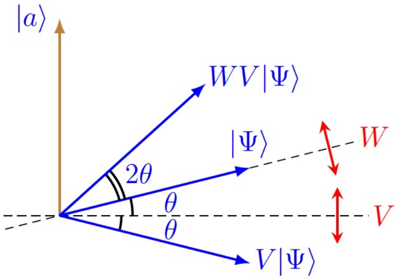
$$
\begin{aligned}
V|\psi\rangle &= -\sin\theta|a\rangle + \cos\theta|r\rangle \\
&= -\sin\theta(\sin\theta|\psi\rangle + \cos\theta|\overline{\psi}\rangle) + \cos\theta(\cos\theta|\psi\rangle - \sin\theta|\overline{\psi}\rangle) \\
&= -\sin^2\theta|\psi\rangle - \sin\theta\cos\theta|\overline{\psi}\rangle + \cos^2\theta|\psi\rangle - \cos\theta\sin\theta|\overline{\psi}\rangle \\
&= (-\sin^2\theta + \cos^2\theta)|\psi\rangle - 2\sin\theta\cos\theta|\overline{\psi}\rangle \\
&= \cos 2\theta|\psi\rangle - \sin 2\theta|\overline{\psi}\rangle
\end{aligned}
$$

A geometric perspective on G

Then, the second reflection over $|\psi\rangle$ yields the effect of the Grover iterator:

$$G|\psi\rangle \;=\; \cos 2\theta|\psi\rangle + \sin 2\theta|\overline{\psi}\rangle$$

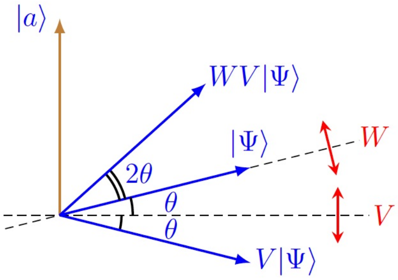
which boils down to a 2θ rotation:



What's behind the scenes?

- The key is the selective shifting of the phase of one state of a quantum system, one that satisfies some condition, at each iteration.
- Performing a phase shift of π is equivalent to multiplying the amplitude of that state by -1: the amplitude for that state changes, but the probability of being in that state remains the same
- Subsequent transformations take advantage of that difference in amplitude to single out that state and increase the associated probability.
- This would not be possible if the amplitudes were probabilities, not holding extra information regarding the phase of the state in addition to the probability — it's a quantum feature.

How many times should G be applied?



From this picture, we may also conclude that the angular distance to cover towards an amplitude maximizing the probability of finding the correct solution is

$$\frac{\pi}{2} - \theta = \frac{\pi}{2} - \arcsin\left(\frac{1}{\sqrt{N}}\right)$$

How many times should G be applied?

Thus, the ideal number of iterations is

$$t = \left\lfloor \frac{\frac{\pi}{2} - \arcsin \frac{1}{\sqrt{N}}}{2\theta} \right\rfloor$$

A lower bound for θ gives an upper bound for t
— for N large $\theta \approx \sin\theta = \frac{1}{\sqrt{N}}$. Thus,

$$t = \frac{\frac{\pi\sqrt{N}-2}{2\sqrt{N}}}{\frac{2}{\sqrt{N}}} \approx \frac{\pi}{4}\sqrt{N}$$

So, G applied t times leaves the system within an angle θ of $|a\rangle$. Then, a measurement in the computational basis yields the correct solution with probability

$$\| \langle a|G^t|\psi\rangle \| \geq \cos^2\theta = 1 - \sin^2\theta = \frac{N-1}{N}$$

which, for large N, is very close to 1.

How many times should G be applied?

For an alternative computation, recall

$$G|\psi\rangle \;=\; \cos 2\theta|\psi\rangle + \sin 2\theta|\overline{\psi}\rangle$$

By induction (prove it!), after k iterations,

$$\begin{aligned} G^k|\psi\rangle \;&=\; \cos(2k\theta)|\psi\rangle + \sin(2k\theta)|\overline{\psi}\rangle \\ &=\; \sin(2k+1)\theta|a\rangle + \cos(2k+1)\theta|r\rangle \end{aligned}$$

Thus, to maximize the probability of obtaining $|a\rangle$, k is selected st

$$\sin((2k+1)\theta) \;\approx\; 1 \quad \text{i.e.} \quad (2k+1)\theta \approx \frac{\pi}{2}$$

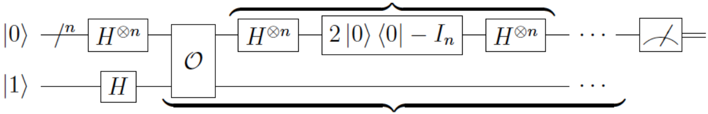
which leads to

$$k \;\approx\; \frac{\pi}{4\theta} - \frac{1}{2} \;\approx\; \frac{\pi}{4}\sqrt{N} \;\approx\; t$$

Grover's algorithm ($\mathcal{O}(\sqrt{N})$)

Revisit our first slide:

- Prepare the initial state: $|0\rangle^{\otimes n}|1\rangle$
- Apply $H^{\otimes n} \otimes H$ to yield $\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|-\rangle$
- Apply the Grover iterator G to $\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|-\rangle$, $t \approx \frac{\pi}{4}\sqrt{N}$ times, leading approximately to state $|a\rangle|-\rangle$
- Measure the first n qubits to retrieve $|a\rangle$



Execution time wrt (classical) exhaustive search:

from $\mathcal{O}(N)$ to $\mathcal{O}(\sqrt{N})$

Multiple solutions

Assume there are M (out of $2^n = N$) input strings evaluating to 0 by f

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = \underbrace{\sqrt{\frac{M}{N}}|s\rangle}_{\text{solution}} + \underbrace{\sqrt{\frac{N-M}{N}}|r\rangle}_{\text{the rest}}$$

where

$$|s\rangle = \frac{1}{\sqrt{M}} \sum_{x \text{ solution}} |x\rangle \quad \text{and} \quad |r\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \text{ no solution}} |x\rangle$$

Multiple solutions

$$t = \left\lfloor \frac{\frac{\pi}{2} - \arcsin\sqrt{\frac{M}{N}}}{2\theta} \right\rfloor$$

which, for N large, $M \ll N$ (thus $\theta \approx \sin\theta$), yields

$$t \approx \frac{\pi}{4}\sqrt{\frac{N}{M}}$$

The probability to retrieve a correct solution is

$$\| \langle s|G^t|\psi\rangle \| \geq \cos^2\theta = 1 - \sin^2\theta = \frac{N-M}{N}$$

which, for $M = \frac{N}{2}$ yields $\frac{1}{2}$, but for $M \ll N$, is again close to 1.

Multiple solutions

Computing the effect of G: 2θ

$$\sin 2\theta = 2\sqrt{\frac{N-M}{N}} = 2\frac{\sqrt{M(N-M)}}{N}$$

$$2\theta = \arcsin\left(2\frac{\sqrt{M(N-M)}}{N}\right)$$

M (out of 100)	$\arcsin\theta$
0	0
1	0.198
20	0.8
40	0.979
50	1
60	0.979
80	0.8
99	0.198
M	0

Multiple solutions

Surprisingly, the rotation in each iteration decreases from $M = \frac{N}{2}$ to N, and the number of iterations consequently increases, although one would expect to be easier to find a correct solution if their number increases!

Solution: resort to draft paper!

To double the number of elements in the search space, by adding N extra elements, none of which being a solution.

The technique: Amplitude amplification

Grover's algorithm made use of

$$H^{\otimes n}|00\cdots 0\rangle$$

to prepare a uniform superposition of potential solutions.

In general, one may resort to any program K to map the solution space to any superposition of guesses, plus some extra qubits to be used as draft paper:

$$K|00\cdots 0\rangle \;=\; \sum_x \alpha_x|x\rangle\,|\mathrm{draft}(x)\rangle$$

The technique: Amplitude amplification

$$|\psi\rangle = \sum_{x \text{ solution}} \alpha_x |x\rangle \, |\text{draft}(x)\rangle + \sum_{x \text{ no solution}} \alpha_x |x\rangle \, |\text{draft}(x)\rangle$$

yielding the following probabilities:

$$p_s = \sum_{x \text{ solution}} \| \alpha_x \|^2 \quad \text{and} \quad p_{ns} = \sum_{x \text{ no solution}} \| \alpha_x \|^2 = 1 - p_s$$

Of course, amplification has no use if $p_s \in \{0, 1\}$.

The technique: Amplitude amplification

Otherwise ($0 < p_s < 1$), the amplitudes of solution inputs should be amplified.
First, express

$$|\psi\rangle \;=\; \sqrt{p_s}|\psi_s\rangle \;+\; \sqrt{p_{ns}}|\psi_{ns}\rangle$$

for the normalised components

$$\begin{aligned} |\psi_s\rangle \;&=\; \sum_{x \text{ solution}} \frac{\alpha_x}{\sqrt{p_s}}|x\rangle\,|\mathrm{draft}(x)\rangle \\ |\psi_{ns}\rangle \;&=\; \sum_{x \text{ solution}} \frac{\alpha_x}{\sqrt{p_{ns}}}|x\rangle\,|\mathrm{draft}(x)\rangle \end{aligned}$$

which rewrites to

$$|\psi\rangle \;=\; \sin\theta|\psi_s\rangle \;+\; \cos\theta|\psi_{ns}\rangle$$

for $\theta \in [0, \frac{\pi}{2}]$ such that $\sin^2\theta = p_s$.

The technique: Amplitude amplification

A generic search iterator is built as

$$S = KPK^{-1}V = W_K V$$

where

$$\begin{aligned} W_K|\psi\rangle &= |\psi\rangle \\ W_K|\phi\rangle &= -|\phi\rangle \quad \text{for all states orthogonal to } |\psi\rangle \end{aligned}$$

The sets $\{|\psi_s\rangle, |\psi_{ns}\rangle\}$ and $\{|\psi\rangle, |\overline{\psi}\rangle\}$ are bases for the relevant 2-dimensional subspace.

The technique: Amplitude amplification

As expected, starting in $|\psi\rangle$, the oracle produces

$$-\sin\theta|\psi_s\rangle \;+\; \cos\theta|\psi_{ns}\rangle \;=\; \cos(2\theta)|\psi\rangle - \sin(2\theta)|\overline{\psi}\rangle$$

which, followed by the amplifier, yields

$$\cos(2\theta)|\psi\rangle + \sin(2\theta)|\overline{\psi}\rangle$$

i.e. the effect of iterator S is

$$S|\psi\rangle \;=\; \cos(2\theta)|\psi\rangle + \sin(2\theta)|\overline{\psi}\rangle$$

which can be expressed in the basis $\{|\psi_s\rangle, |\psi_{ns}\rangle\}$ as

$$S|\psi\rangle \;=\; \sin(3\theta)|\psi_s\rangle + \cos(3\theta)|\psi_{ns}\rangle$$

The technique: Amplitude amplification

The repeated application of S a total of k times rotates the initial state $|\psi\rangle$ to

$$S^k|\psi\rangle = \sin((2k+1)\theta)|\psi_s\rangle + \cos((2k+1)\theta)|\psi_{ns}\rangle$$

For the correct number of iterations, this procedure reaches a state such that a measurement will return an element of the subspace spanned by $|\psi_s\rangle$ with a probability close to 1.

The technique: Amplitude amplification

As before, to get that high probability, the smallest value for k one can choose is such that

$$(2k+1)\theta \;\approx\; \frac{\pi}{2}$$

For a small θ, as

$$\sin\theta \;=\; \sqrt{p_s} \;\approx\; \theta$$

the magnitude of the right number of iterations is

$$\mathcal{O}\left(\sqrt{\frac{1}{\theta}}\right)$$

because

$$(2k+1)\sqrt{p_s} \;=\; \theta \;\Leftrightarrow\; k \;=\; \frac{\pi}{4\sqrt{p_s}} - \frac{1}{2}$$

To follow

The algorithm requires that one knows in advance how many times iterator S is to be applied:

- For $K = H$ (uniform sampling the input) this boils down to know the number of solutions of the search problem.
- For a generic K this amounts to know the probability with which K guesses a solution to the problem, i.e. $\sin(\theta)$.

To see ...

- blind search
- estimate the amplitude with which K maps $|00\cdots0\rangle$ to the subspace of solutions