Quantum Systems

(Lecture 6: Search problems and the Grover algorithm)

Luís Soares Barbosa

Universidade do Minho

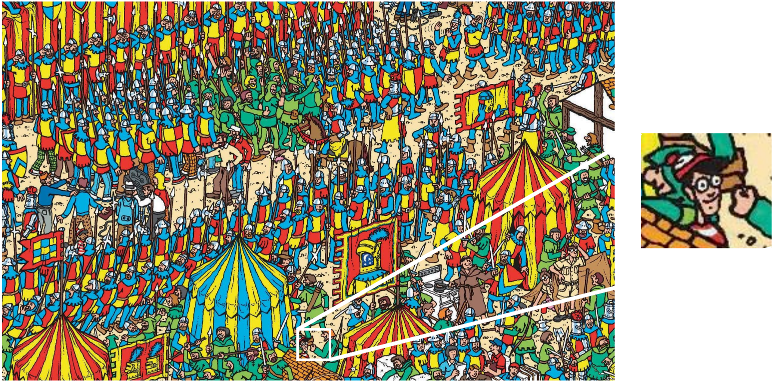
HASLab HIGH-ASSURANCE SOFTWARE LABORATORY

INL INTERNATIONAL IBERIAN NANOTECHNOLOGY LABORATORY

UNITED NATIONS UNIVERSITY UNU-EGOV

Universidade do Minho

Search problems



Search problems

Search problem

- **Search space**: unstructured / unsorted
- **Asset**: a tool to efficiently recognise a solution

Example: Searching in a sorted vs unsorted database

- find a name in a telephone directory
- find a phone number in a telephone directory

Search problems

Note that that a procedure to recognise a solution does not need to rely on a previous knowledge of it.

Example: password recognition

- $f(x) = 1$ iff $x = 123456789$ (f knows the password)
- $f(x) = 1$ iff $hash(x) = \text{c9b93f3f0682250b6cf8331b7ee68fd8}$ (f recognises a correct password, but does not know it as inverting a hash function is, in general, very hard.)

Search problems

A typical formulation

Given a function $f : 2^n (= N) \longrightarrow 2$ such that there exists a unique number, encoded by a binary string a, st

$$f(x) = \begin{cases} 1 & \Leftarrow x = a \\ 0 & \Leftarrow x \neq a, \end{cases}$$

determine a.

A classical solution

- 0 evaluations of f: probability of success: $\frac{1}{2^n}$
- 1 evaluation of f: probability of success: $\frac{2}{2^n}$
  (choose a solution at random; if test fails choose another.
- 2 evaluations of f: probability of success: $\frac{3}{2^n}$.
- k evaluations of f: probability of success: $\frac{k+1}{2^n}$.

Search problems

Grover's algorithm (1996): A quadratic speed up

- Worst case for a classic algorithm: 2^n evaluations of f
- Worst case for Grover's algorithm: $\sqrt{2^n}$ evaluations of f

An oracle for f

... provides a means to recognize a solution for an input $|v\rangle$:

$$U_f \;=\; |v\rangle|t\rangle \mapsto |v\rangle|t \oplus f(v)\rangle$$

Thus, preparing the target register with $|0\rangle$,

$$U_f \;=\; |v\rangle|0\rangle \mapsto |v\rangle|f(v)\rangle$$

Measuring the target after U_f will return its answer to the given input, as (classically) expected.

Superposition will make the difference to take advantage of a quantum machine.

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

An oracle for f

$|\psi\rangle$ can be expressed in terms of two states separating the solution states and the rest:

$$|a\rangle \text{ and } |r\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \in N \setminus \{a\}} |x\rangle$$

which form a basis for a 2-dimensional subspace of the original N-dimensional space.

Thus,

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

An oracle for f

If the target qubit is set to $|-\rangle$, the effect of U_f is just

$$U_f \;=\; |x\rangle|-\rangle \mapsto (-1)^{f(x)}|x\rangle|-\rangle$$

Since $|-\rangle (= \frac{|0\rangle - |1\rangle}{\sqrt{2}})$ is an eigenvector of X, this corresponds to a single qubit oracle which encodes the answer of U_f as a phase shift:

$$V \;=\; |x\rangle \mapsto (-1)^{f(x)}|x\rangle$$

$$\left(\text{i.e. } V|a\rangle = -|a\rangle \;\text{ and }\; V|x\rangle = |x\rangle \;(\text{for } x \neq a)\;\right)$$

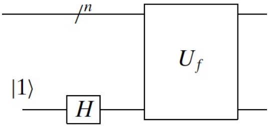
which can be expressed as

$$V \;=\; \sum_{x \neq a} |x\rangle\langle x| - |a\rangle\langle a| \;=\; I - 2|a\rangle\langle a|$$

An oracle for f

$$V = \sum_{x \neq a} |x\rangle\langle x| - |a\rangle\langle a| = I - 2|a\rangle\langle a|$$

The circuit



V identifies the solution but does not allow for an observer to retrieve it because the square of the amplitudes for any value is always $\frac{1}{N}$.

An amplifier

This entails the need for a mechanism to boost the probability of retrieving the solution.

$$\begin{aligned} P &= |x\rangle \mapsto (-1)^{\delta_{x,0}}|x\rangle \\ &= |0\rangle\langle 0| + (-1)\sum_{x\neq 0}|x\rangle\langle x| \\ &= |0\rangle\langle 0| + (-1)(I - |0\rangle\langle 0|) \\ &= 2|0\rangle\langle 0| - I \end{aligned}$$

P applies a phase shift to all vectors in the subspace spanned by all the basis states $|x\rangle$, for $x \neq 0$, i.e. all states orthogonal to $|00\cdots 0\rangle$.

An amplifier

Prepare a state in uniform superposition:

$$|\psi\rangle = H^{\otimes n}|00\cdots 0\rangle = |+\rangle^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

and define an operator $W = H^{\otimes n}\, P\, H^{\otimes n}$, which

- $W|\psi\rangle = |\psi\rangle$,
- $W|\phi\rangle = -|\phi\rangle$, for any vector $|\phi\rangle$ in the subspace orthogonal to $|\psi\rangle$ (i.e. spanned by the basis vectors $H|x\rangle$ for $x \neq 0$).

W applies a phase shift of -1 to all vectors in the subspace orthogonal to $|\psi\rangle$.

An amplifier

Then,

$$\begin{aligned} W &= H^{\otimes n}\, P\, H^{\otimes n} \\ &= H^{\otimes n}\,(2|0\rangle\langle 0| - I)\, H^{\otimes n} \\ &= 2(H^{\otimes n}|0\rangle\langle 0|H^{\otimes n}) - H^{\otimes n}\, I\, H^{\otimes n} \\ &= 2|\psi\rangle\langle\psi| - I \end{aligned}$$

The effect of W: to *invert about the average*

$$
\begin{aligned}
W\left(\sum_k \alpha_k|k\rangle\right) &= \left(2\left(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}\langle y|\right) - I\right)\sum_k \alpha_k|k\rangle \\
&= \left(2\left(\frac{1}{N}\sum_{x=0}^{N-1}|x\rangle\sum_{y=0}^{N-1}\langle y|\right) - I\right)\sum_k \alpha_k|k\rangle \\
&= 2\left(\frac{1}{N}\sum_{x,y,k}\alpha_k|x\rangle\langle y|k\rangle\right) - \sum_k \alpha_k|k\rangle \\
&= 2\left(\underbrace{\frac{1}{N}\sum_k \alpha_k}_{\alpha\text{ - mean}}\sum_x |x\rangle\right) - \sum_k \alpha_k|k\rangle \\
&= 2\,\alpha\sum_k |k\rangle - \sum_k \alpha_k|k\rangle \\
&= \sum_k (2\,\alpha - \alpha_k)|k\rangle
\end{aligned}
$$

The effect of W: to *invert about the average*

The effect of W is to transform the amplitude of each state so that it is as far above the average as it was below the average prior to its application, and vice-versa:

$$\alpha_k \;\mapsto\; 2\alpha - \alpha_k$$

$\boxed{W \text{ inverts and boosts the “right” amplitude; slightly reduces the others.}}$

Invert about the average: Example

Let $N = 2^2$ and suppose the solution a is encoded as the bit string 01. The algorithm starts with a uniform superposition

$$H^{\otimes 3}|0\rangle \;=\; \frac{1}{2}\sum_{k=0}^{3}|k\rangle$$

which the oracle turns into

$$\frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$$

The effect of inversion about the average is

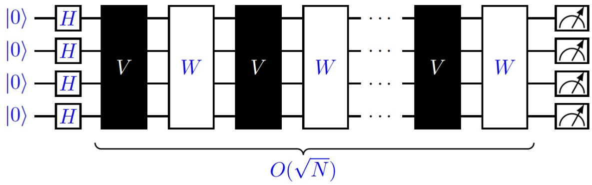
$$2\overbrace{\begin{bmatrix}\frac{1}{4}\\ \frac{1}{4}\\ \frac{1}{4}\\ \frac{1}{4}\end{bmatrix}}^{\alpha\sum_k |k\rangle} - \overbrace{\begin{bmatrix}\frac{1}{2}\\ -\frac{1}{2}\\ \frac{1}{2}\\ \frac{1}{2}\end{bmatrix}}^{\sum_k \alpha_k|k\rangle} = \begin{bmatrix}\frac{2}{4}-\frac{1}{2}\\ \frac{2}{4}+\frac{1}{2}\\ \frac{2}{4}-\frac{1}{2}\\ \frac{2}{4}-\frac{1}{2}\end{bmatrix} = \begin{bmatrix}0\\ 1\\ 0\\ 0\end{bmatrix}$$

$$\boxed{\text{Measuring returns the solution with probability 1!}}$$

The Grover iterator

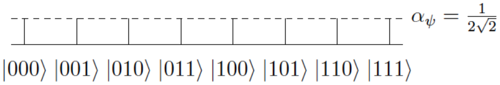
$$\begin{aligned} G &= W V \\ &= H^{\otimes n} P H^{\otimes n} V \\ &= (2|\psi\rangle\langle\psi| - I)\,(I - 2|a\rangle\langle a|) \end{aligned}$$

The Grover circuit

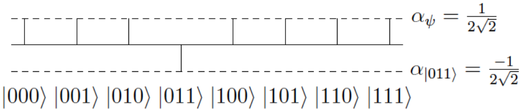


Example: $N = 8,\ a = 3$

Starting point:



After the oracle



Example: $N = 8,\ a = 3$

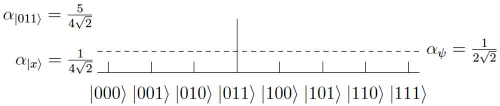
Inversion about the average

$$
\begin{aligned}
&(2|\psi\rangle\langle\psi| - I)\left(|\psi\rangle - \frac{2}{2\sqrt{2}}|011\rangle\right) \\
&= 2|\psi\rangle\langle\psi|\psi\rangle - |\psi\rangle - \frac{2}{\sqrt{2}}|\phi\rangle\langle\psi|011\rangle + \frac{1}{\sqrt{2}}|011\rangle \\
&= 2|\psi\rangle\langle\psi|\psi\rangle - |\psi\rangle - \frac{2}{\sqrt{2}}\frac{1}{2\sqrt{2}}|\phi\rangle + \frac{1}{\sqrt{2}}|011\rangle \\
&= |\psi\rangle - \frac{1}{2}|\psi\rangle + \frac{1}{\sqrt{2}}|011\rangle \\
&= \frac{1}{2}|\psi\rangle + \frac{1}{\sqrt{2}}|011\rangle
\end{aligned}
$$

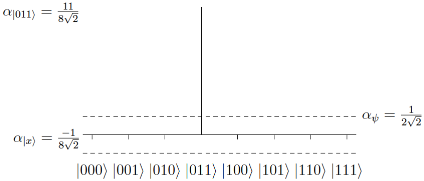
As $|\psi\rangle = \frac{1}{2\sqrt{2}}\sum_{k=0}^{7}|k\rangle$. we end up with

$$
\frac{1}{2}\left(\frac{1}{2\sqrt{2}}\sum_{k=0}^{7}|k\rangle\right) + \frac{1}{\sqrt{2}}|011\rangle \ = \ \frac{1}{4\sqrt{2}}\sum_{k=0,k\neq 3}^{7}|k\rangle + \frac{5}{4\sqrt{2}}|011\rangle
$$

Example: $N = 8,\ a = 3$



Making a second iteration yields



and the probability of measuring the state corresponding to the solution is

$$\left|\frac{11}{8\sqrt{2}}\right|^2 = \frac{121}{128} \approx 94,5\%$$

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 $|\psi\rangle$:

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

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

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

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 $|\psi\rangle$.

Thus, one should express the action of V in the basis $|\psi\rangle, |\overline{\psi}\rangle$ to perform afterwards the second reflection:

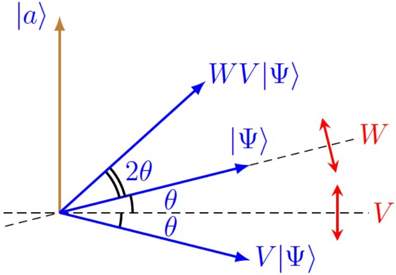
$$
\begin{aligned}
V|\psi\rangle &= -\sin\theta|a\rangle + \cos\theta|r\rangle \\
&= -\sin\theta(\sin\theta|\psi\rangle + \cos\theta|\overline{\psi}\rangle) + \cos\theta(\cos\theta|\psi\rangle - \sin\theta|\overline{\psi}\rangle) \\
&= -\sin^2\theta|\psi\rangle - \sin\theta\cos\theta|\overline{\psi}\rangle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

A geometric perspective on G

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

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

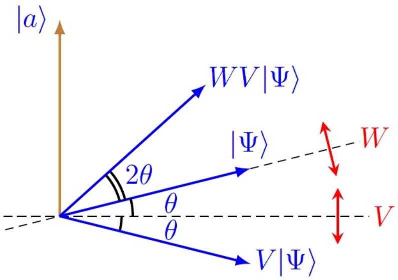
which boils down to 2θ rotation:



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 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,

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

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, 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

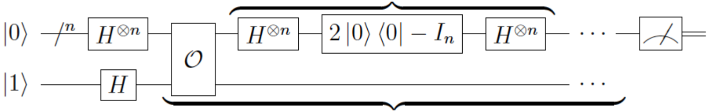
$$\sin((2k+1)\theta) \approx 1 \quad \text{i.e.} \quad (2k+1)\theta \approx \frac{\pi}{2}$$

which leads to

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

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

- 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 $|a\rangle$



Multiple solutions

$$\boxed{\text{There } M \text{ (out of } 2^n = N\text{) input strings evaluating to 0 by } f}$$

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

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

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

Quantum algorithms

Recall the generic idea: engineering quantum effects as computational resources

Classes of algorithms

- Algorithms with superpolynomial speed-up, typically based on the quantum Fourier transform, include Shor's algorithm for prime factorization. The level of resources (qubits) required is not yet currently available.
- Algorithms with quadratic speed-up, typically based on amplitude amplification, as in the variants of Grover's algorithm for unstructured search. Easier to implement in current NISQ technology, typical component of other algorithms.
- Quantum simulation — not covered in this course.

... and we are done!

What have we covered

- Reactive systems:
  - classical interaction (communication)
  - + programmed parallelism (operators, e.g. $\|$)
  - + engineering
- Quantum systems:
  - quantum interaction (entanglement)
  - + physical/natural parallelism (superposition)
  - + engineering

... and we are done!

Where to look further

- Reactive computation is the base of the everyware — namely in its extensions to hybrid (discrete-continuous) programming and cyber-physical systems.
  Covered in the Formal Methods profile in the MSc on Informatics Engineering.
- Quantum computation is an extremely young and challenging area, looking for young people either with a theoretic or experimental profile.
  Get in touch if you are interested in pursuing studies/research in the area at UMinho, INESC TEC and INL.

Universidade do Minho

HASLab HIGH-ASSURANCE SOFTWARE LABORATORY

INL INTERNATIONAL IBERIAN NANOTECHNOLOGY LABORATORY