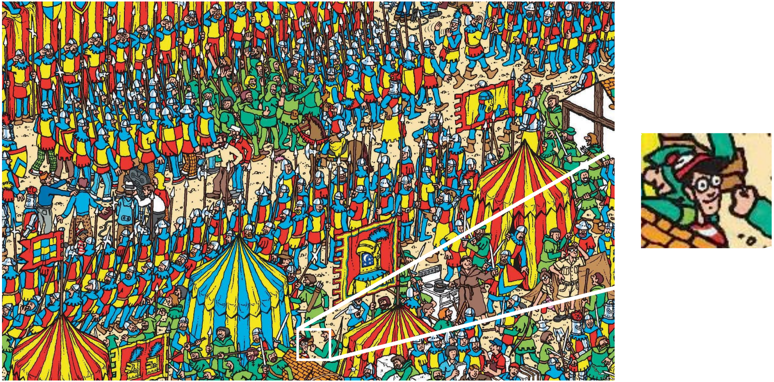
Quantum Computation
Unstructured search and Grover's algorithm

Luís Soares Barbosa & Renato Neves

MSc Physics Engineering

Universidade do Minho, 2023-24

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

Example: password recognition

- $f(x) = 1 \quad \text{iff} \quad x = 123456789$ (f knows the password)
- $f(x) = 1 \quad \text{iff} \quad hash(x) = \text{c9b93f3f0682250b6cf8331b7ee68fd8}$
  (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 $f : 2^n \longrightarrow 2$ such that there exists a unique number, encoded by a binary string w, st

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

determine w.

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

where n is the number of qubits necessary to represent the input (i.e. the search space)

(Variants of) this algorithm can be applied in a multitude of scenarios:

- Searching through unstructured databases
- Finding passwords
- Route planning
- Solving SAT problems (and NP-problems in general)

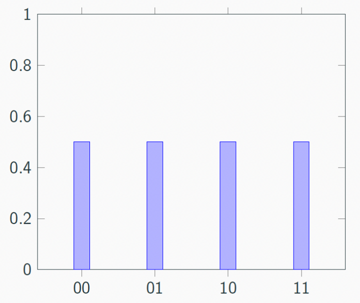
Key Ideas

As seen in previous cases, quantum algorithms resort to

1. superposition
2. interference
   (to decrease amplitude of wrong answers and increase amplitude of the right ones)

Key Ideas: Superposition

Suppose $f : \{0,1\}^2 \to \{0,1\}$ with $f(10) = 1$



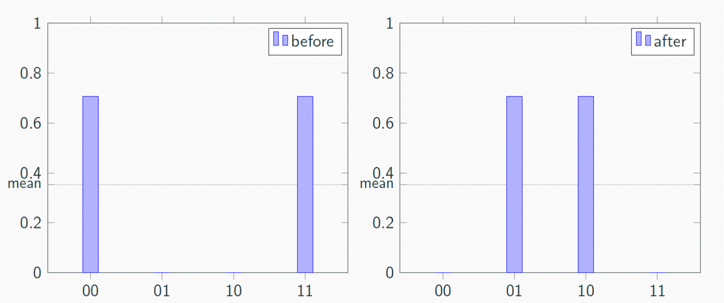
$$\frac{1}{2}\Big(00 + 01 + 10 + 11\Big)$$

Key Ideas: Interference

Act on amplitudes through the following map:

$$x \mapsto mean + (mean - x)$$

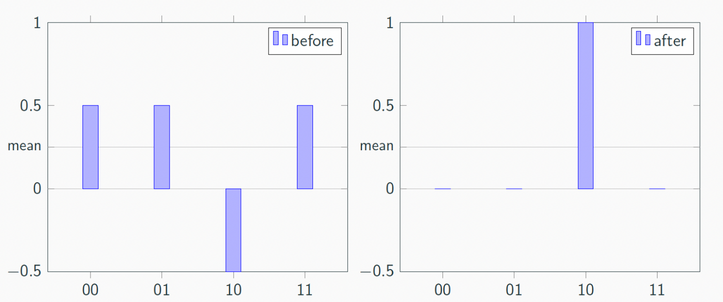
(inversion about the mean)



Intuitively mass of some states was given to others

Key Ideas: Interference

See the effect when the right amplitude has an opposite phase:



Intuitively, mass of wrong answers was given to the right one.

The strategy

1. Put all possible answers in uniform superposition
2. Label the right answer by flipping its phase
3. Amplify the amplitude of the right answer (through inversion about the mean)
4. Iterate through steps 2 and 3 until one can be sure to measure the right answer with high probability

Step 1: Label the solution

Let $N = 2^n$, then search space

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

can be expressed in terms of two states separating the solution state and the rest:

$$|w\rangle \;\text{ and }\; |r\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \in N, x \neq w} |x\rangle$$

which forms a basis for a 2-dimensional subspace of the original N-dimensional space. Thus,

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

Step 1: Label the solution

As discussed in the previous lecture, an oracle for f 'kicks back' the relevant phase:

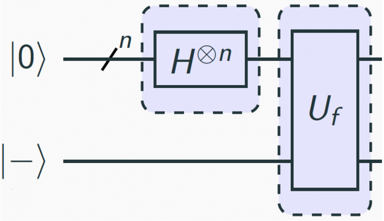
$$U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$$

In particular, if w is as solution of f it phase is flipped:

$$U_f|w\rangle|-\rangle = -|w\rangle|-\rangle$$

Step 1: Label the solution

Summing up, this circuit



encodes the following quantum state in the top quibits:

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

The solution is identified but an observer would be unable to retrieve it because the square of the amplitudes for any basis state is always $\frac{1}{N}$.

Step 2: Boost the right amplitude

The oracle performs a phase shift over an unknown state, marking the solution but not changing the probability of retrieving it.

Thus, one needs a mechanism to boost the probability of retrieving the solution, which will be accomplished by another phase shift, but now applied to well-known vectors.

Consider, the following program

$$P = 2|0\rangle\langle 0| - I$$

which flips basis states different from $|0\rangle$, i.e. applies a -1 phase shift to all vectors in the subspace orthogonal to $|0\rangle$, i.e. spanned by all the basis states $|x\rangle$, for $x \neq 0$.

Exercise

Show that this is indeed the case

Step 2: Boost the right amplitude

Exercise

Show that this is indeed the case

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

Thus, $P|x\rangle \; = \; -(-1)^{\delta_{x,0}}|x\rangle$

Step 2: Boost the right amplitude

Then, use P to define an operator

$$W = H^{\otimes n}\, P\, H^{\otimes n}$$

A simple calculation yields,

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

denoting $H^{\otimes n}|0\rangle$ by $|\psi\rangle$.

But does W boost the probability of finding the right solution?

Step 2: Boost the right amplitude

Exercise.

Show that

$$|\psi\rangle\langle\psi| = \frac{1}{N}\sum_{x,y\in N}|x\rangle\langle y|$$

for $N = 2^n$

Step 2: Boost the right amplitude

Exercise.

$$
\begin{aligned}
&|\psi\rangle\langle\psi| = \\
&= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \, \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \langle y| \\
&= \frac{1}{N} \sum_{x=0}^{N-1} |x\rangle \, \sum_{y=0}^{N-1} \langle y| \\
&= \frac{1}{N} \sum_{x,y \in N} |x\rangle\langle y|
\end{aligned}
$$

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

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

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:

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

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

Example: $N = 2^2 = 4,\ w = 01$

The algorithm starts with a uniform superposition

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

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

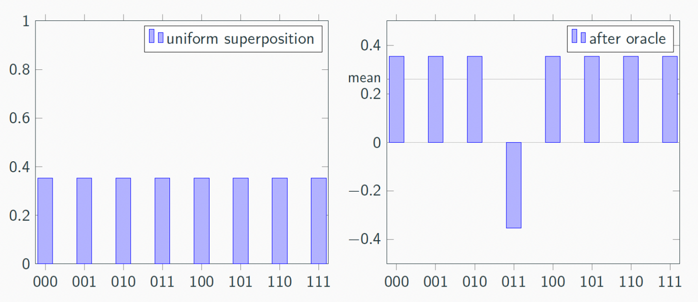
$$2\ \overbrace{\begin{bmatrix}\frac{1}{4}\\ \frac{1}{4}\\ \frac{1}{4}\\ \frac{1}{4}\end{bmatrix}}^{\alpha \sum_k |k\rangle} - \overbrace{\begin{bmatrix}\frac{1}{2}\\ -\frac{1}{2}\\ \frac{1}{2}\\ \frac{1}{2}\end{bmatrix}}^{\sum_k \alpha_k |k\rangle} = \begin{bmatrix}\frac{2}{4}-\frac{1}{2}\\ \frac{2}{4}+\frac{1}{2}\\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

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

Example: $N = 2^3 = 8,\ w = 011$

Starting point: all amplitudes $\alpha_k = \frac{1}{2\sqrt{2}}$

After the oracle: $\alpha_{011} = -\frac{1}{2\sqrt{2}}$; all the others remain.



Example: $N = 2^3 = 8$, $w = 011$

Exercise

Compute the inversion about the average at this stage, applying the W circuit.

Example: $N = 2^3 = 8,\ w = 011$

Inversion about the average

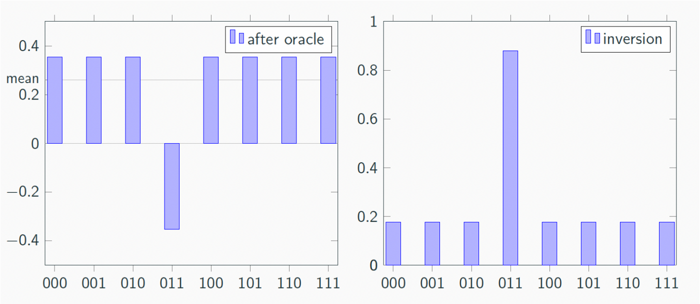
$$
\begin{aligned}
&(2|\psi\rangle\langle\psi| - I)\left(|\psi\rangle - \frac{2}{2\sqrt{2}}|011\rangle\right) \\
&= 2|\psi\rangle\langle\psi|\psi\rangle - |\psi\rangle - \frac{2}{\sqrt{2}}|\psi\rangle\langle\psi|011\rangle + \frac{1}{\sqrt{2}}|011\rangle \\
&= 2|\psi\rangle\langle\psi|\psi\rangle - |\psi\rangle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

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

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

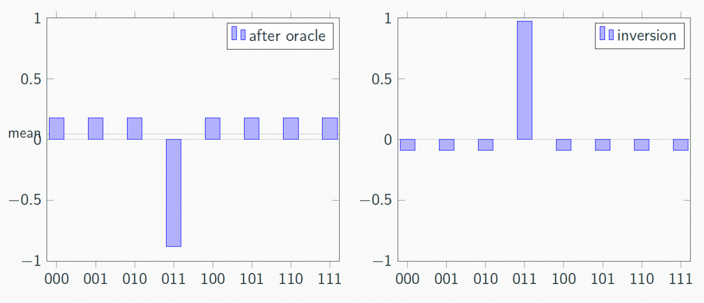
Example: $N = 2^3 = 8$, $w = 011$

In pictures:



Example: $N = 2^3 = 8,\ w = 011$

Making a second iteration yields



with

- $\alpha_{011} = \frac{11}{8\sqrt{2}}$
- all remaining amplitudes: $\frac{-1}{8\sqrt{2}}$

Example: $N = 2^3 = 8,\ w = 011$

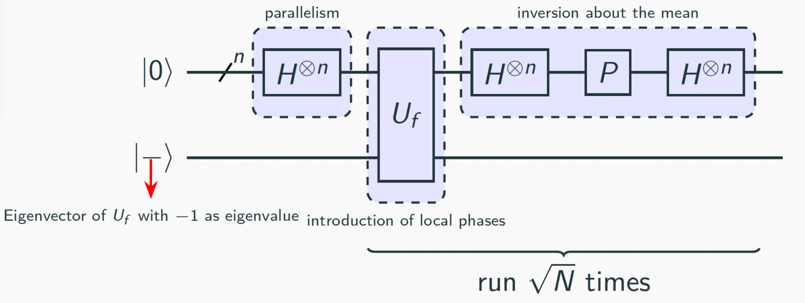
The probability of measuring the state corresponding to the solution is

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

Thus,

$\boxed{\text{This is an iterative algorithm}}$

Grover algorithm : The iterator $G = WU_f$



Question

How many iterations are needed?

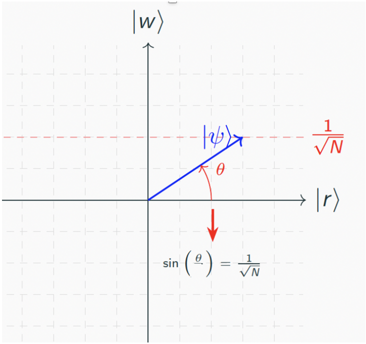
What's behind the scenes?

- 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.

A geometric perspective on G

Initial state: $|\psi\rangle = \frac{1}{\sqrt{N}}|w\rangle + \sqrt{\frac{N-1}{N}}|r\rangle$

$|w\rangle$ and $|r\rangle$ form a orthonormal basis for a 2-dimensional real vector space in which one may analyse Grover's algorithm.



A geometric perspective on G

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

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

A geometric perspective on G

G has two components:

- Oracle V which applies a phase shift to $|w\rangle$: reflection over $|r\rangle$.
  Actually, $V = 2|r\rangle\langle r| - I$ (or, equivalently, $I - |w\rangle\langle w|$). Thus,

$$V(\alpha_w|w\rangle + \alpha_r|r\rangle) \;=\; -\alpha_w|w\rangle + \alpha_r|r\rangle$$

- Amplifier $W = 2|\psi\rangle\langle\psi| - I$ which applies a phase shift to all vectors in the subspace orthogonal to $|\psi\rangle$: reflection over $|\psi\rangle$.

Exercise.

Express the action of V in the basis $|\psi\rangle, |\overline{\psi}\rangle$ to perform afterwards the second reflection.

A geometric perspective on G

Exercise.

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

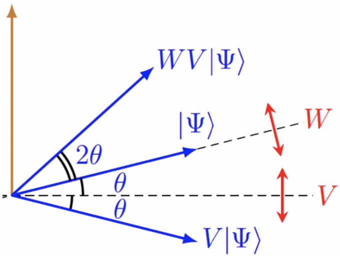
$$\begin{aligned}
V|\psi\rangle &= -\sin\theta|a\rangle + \cos\theta|r\rangle \\
&= -\sin\theta(\sin\theta|\psi\rangle + \cos\theta|\overline{\psi}\rangle) + \cos\theta(\cos\theta|\psi\rangle - \sin\theta|\overline{\psi}\rangle) \\
&= -\sin^2\theta|\psi\rangle - \sin\theta\cos\theta|\overline{\psi}\rangle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

A geometric perspective on G

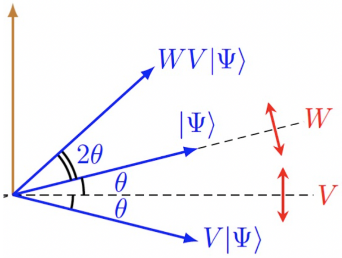
Then, the second reflection over $|\psi\rangle$ yields the effect of the Grover iterator:

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

which boils down to a 2θ rotation:



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

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

where $\lfloor x \rceil$ denotes the integer closest to x.

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

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

Complexity

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

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

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

On the other hand,
Execution time wrt (classical) exhaustive search:

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