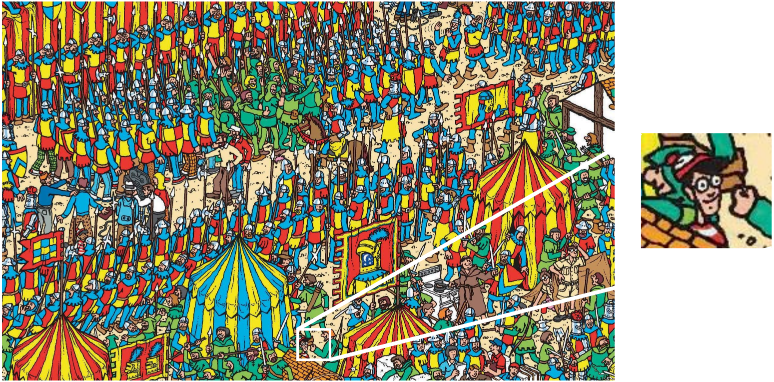
Quantum Computation
(Lecture 2)

Luís Soares Barbosa

MSc Physics Engineering

Universidade do Minho, 2021-22

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 $f : 2^n \longrightarrow 2$ 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

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

An oracle for f

As usual, an oracle encapsulates the reversible computation of f 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: Let $N = 2^n$, then

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

An oracle for f

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

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

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

Thus,

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

An oracle for f

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

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

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:

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

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

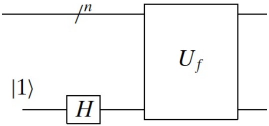
which can be expressed as

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

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.

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

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:

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

W 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

$$H^{\otimes 2}|00\rangle \ = \ \frac{1}{2}\sum_{k=0}^{3}|k\rangle$$

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

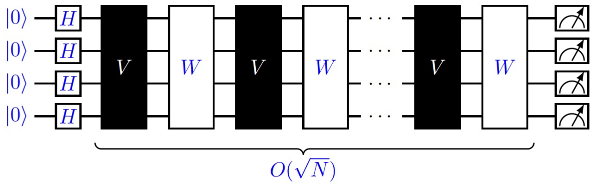
$$2\overbrace{\begin{bmatrix}\frac{1}{4}\\ \frac{1}{4}\\ \frac{1}{4}\\ \frac{1}{4}\end{bmatrix}}^{\alpha\sum_k|k\rangle} - \overbrace{\begin{bmatrix}\frac{1}{2}\\ -\frac{1}{2}\\ \frac{1}{2}\\ \frac{1}{2}\end{bmatrix}}^{\sum_k \alpha_k|k\rangle} = \begin{bmatrix}\frac{2}{4}-\frac{1}{2}\\ \frac{2}{4}+\frac{1}{2}\\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

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

The Grover iterator

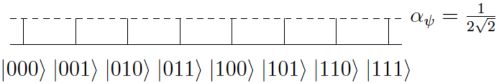
$$
\begin{aligned}
G &= WV \\
&= H^{\otimes n} P H^{\otimes n} V \\
&= (2|\psi\rangle\langle\psi| - I)(I - 2|a\rangle\langle a|)
\end{aligned}
$$

The Grover circuit

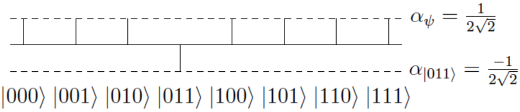


Example: $N = 8,\ a = 3$

Starting point:



After the oracle



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

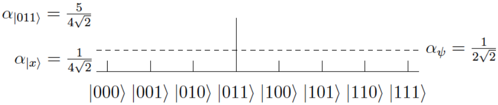
Inversion about the average

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

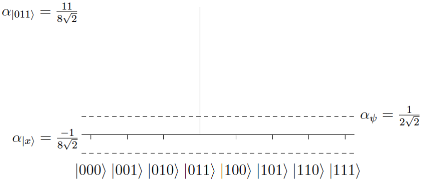
As $|\psi\rangle = \frac{1}{2\sqrt{2}}\sum_{k=0}^{7}|k\rangle$, we end up with

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

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



Making a second iteration yields



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

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