Quantum computation: lecture 10

Grover's algorithm

Let $f : \{0,1\}^n \longrightarrow \{0,1\}$ be a Boolean function and $A = \{ x \in \{0,1\}^n : f(x) = 1 \}$

We are considering the search problem, namely to identify one element x of A with as few calls as possible to the oracle f.

Consider first the case where $A = \{x^*\}$, singleton:

Classically, identifying x^* may require up to $N = 2^n$ calls to the oracle f, in the worst case.

As we will see, Grover's quantum algorithm only requires $\sqrt{N} = 2^{n/2}$ calls to the oracle f to identify x^*.

Note: Grover's algorithm is usually presented solving the following problem: given a directory of N names in alphabetical order and corres-ponding phone numbers, it allows to recover the name corresponding to a given phone number in only $\sqrt{N}$ steps (instead of N steps classically).

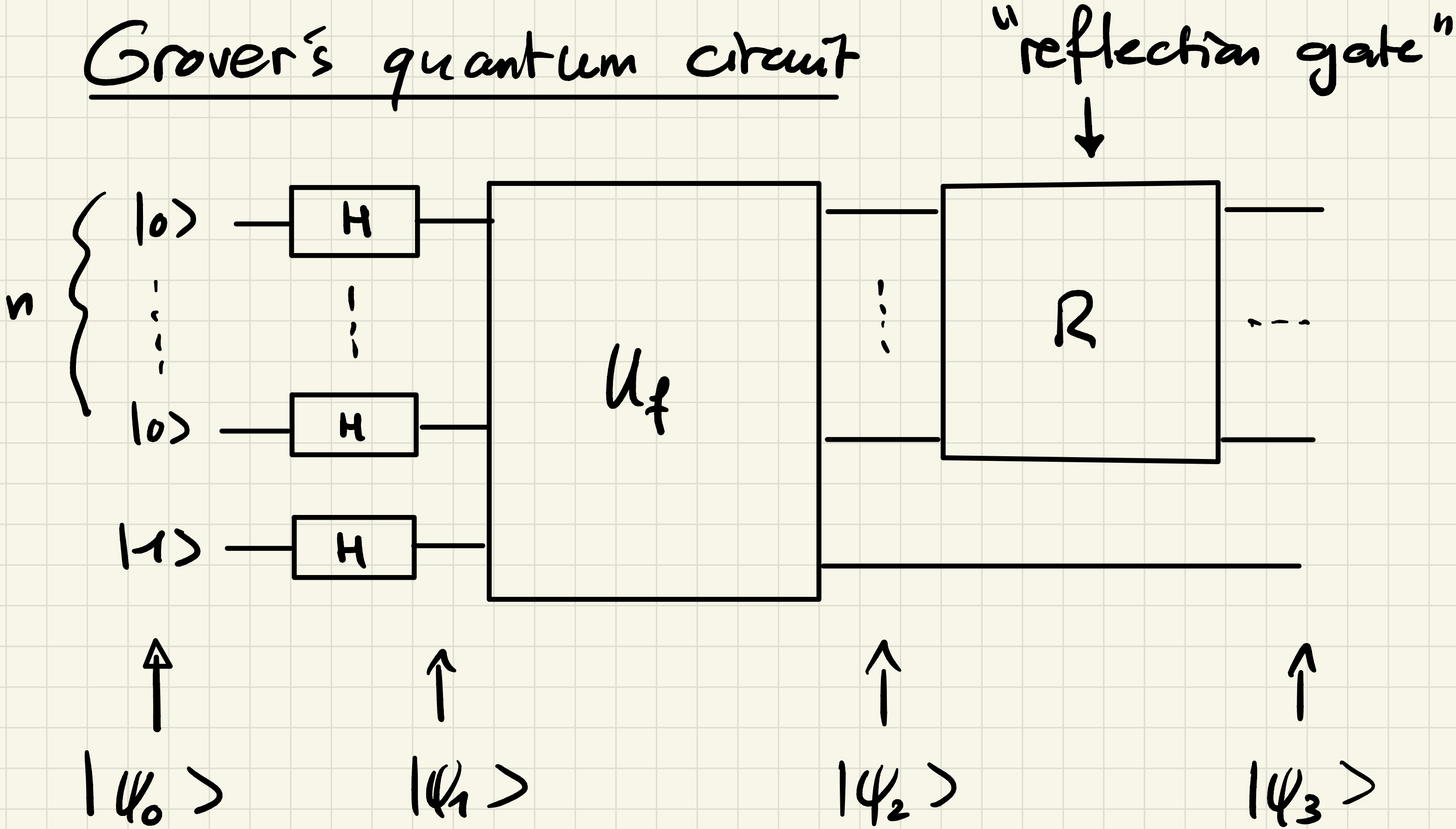
However, in order to work, Grover's algorithm requires us to build the gate U_f, which is not doable in the directory search pb, as we know nothing about the function f!

But please be patient: we will see later other interesting applications of Grover's algorithm.

Note also that we will consider in general functions f with $|A| = M \in \{1..N\}$.

Surprisingly perhaps, considering this generalization (without focusing on the case $M=1$) will help us visualize better how the algorithm works!

Grover's quantum circuit



Let us compute (as already done multiple times)

- $$|\varphi_1\rangle = H|0\rangle \otimes \dots \otimes H|0\rangle \otimes H|1\rangle$$

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

$$\left[= \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \right]$$

- $$|\varphi_2\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}} (-1)^{f(x)} |x\rangle \otimes |-\rangle$$

So far, nothing new. Now, remember that in our case, $M = |A| = \{x : f(x) = 1\}$, so $N - M = |A^c|$
$= \{x : f(x) = 0\}$.

Therefore:

$$|\psi_2\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \otimes |-\rangle$$

$$= \frac{1}{\sqrt{N}} \cdot \left(\sqrt{\frac{N-M}{N-M}} \sum_{x \in A^c} |x\rangle - \sqrt{\frac{M}{N}} \sum_{x \in A} |x\rangle \right) \otimes |-\rangle$$

$$= \left(\sqrt{\frac{N-M}{N}} \left(\frac{1}{\sqrt{N-M}} \sum_{x \in A^c} |x\rangle \right) - \sqrt{\frac{M}{N}} \left(\frac{1}{\sqrt{M}} \sum_{x \in A} |x\rangle \right) \right) \otimes |-\rangle$$

Let us write $|P\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \in A^c} |x\rangle$

and $|s\rangle = \frac{1}{\sqrt{M}} \sum_{x \in A} |x\rangle$: both $|P\rangle$ and $|s\rangle$

are quantum states (normalized to 1)

and $|\varphi_2\rangle$ can be rewritten as

$$|\varphi_2\rangle = \left(\sqrt{\frac{N-M}{N}}\,|P\rangle - \sqrt{\frac{M}{N}}\,|s\rangle\right) \otimes |-\rangle$$

[From now on, we will forget the extra $|-\rangle$ state.]

Note also that $\left(\sqrt{\frac{N-M}{N}}\right)^2 + \left(\sqrt{\frac{M}{N}}\right)^2 = \frac{N-M}{N} + \frac{M}{N} = 1$,

so there exists $\theta_0 \in [0, \frac{\pi}{2}]$ such that

$$\cos\theta_0 = \sqrt{\frac{N-M}{N}} \quad \text{and} \quad \sin\theta_0 = \sqrt{\frac{M}{N}}$$

and $|\psi_2\rangle = \cos\theta_0 \, |P\rangle - \sin\theta_0 \, |S\rangle$

Likewise, observe that

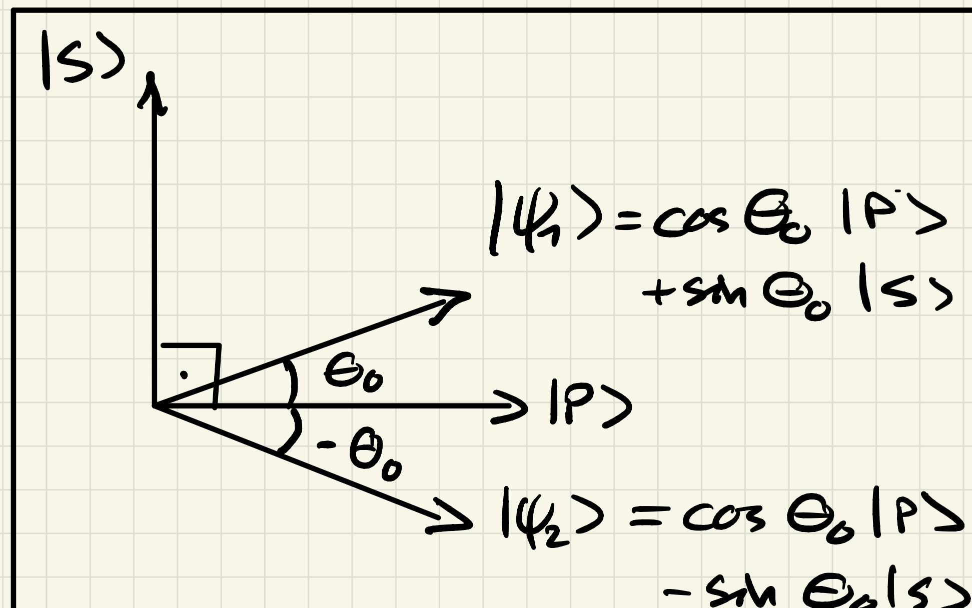
$$|\psi_1\rangle = \cos\theta_0 \, |P\rangle + \sin\theta_0 \, |S\rangle$$

(if we again forget the extra $|-\rangle$ state)

Geometric interpretation

$$|P\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \in A^c} |x\rangle \quad \text{and} \quad |S\rangle = \frac{1}{\sqrt{M}} \sum_{x \in A} |x\rangle$$

are orthogonal (as they share no common basis element), so we obtain the following picture:

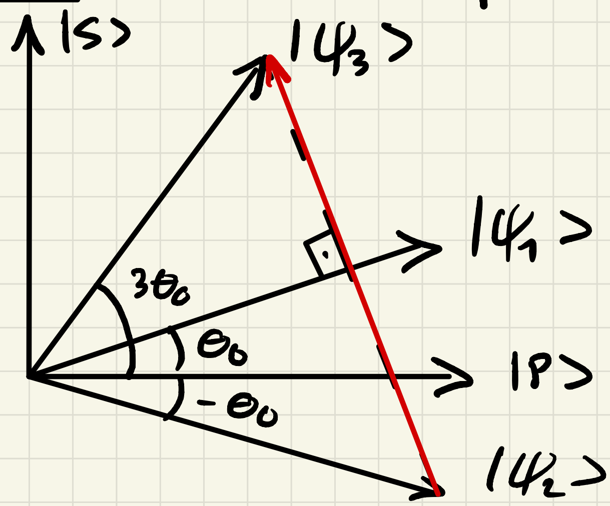


The action of the gate U_f on state $|\psi_1\rangle$ can therefore be interpreted as a <u>reflection</u> with respect to the axis $|P\rangle$!

But note that we do not know the axes $|P\rangle$ and $|S\rangle$; this is exactly what we are after; more precisely, our aim now is to push as much as possible the state of the system towards $|S\rangle$, which contains only elements $x \in A$.

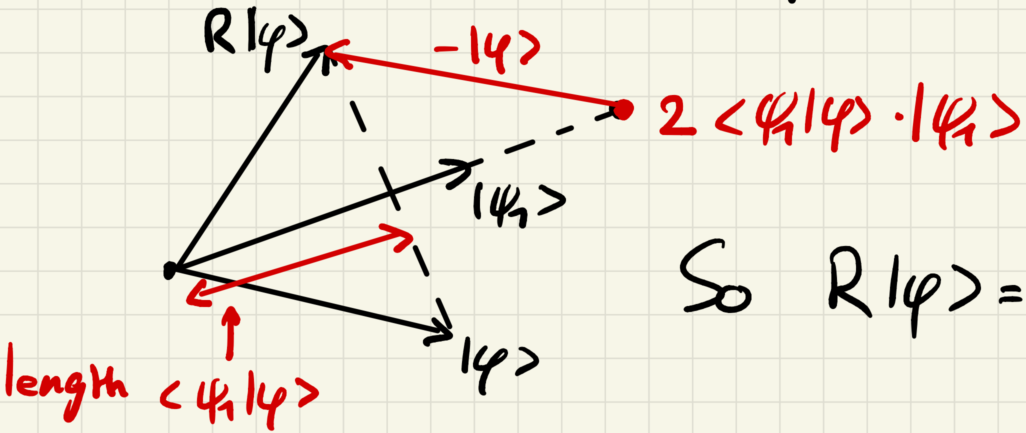
Reflection gate R

A first step in this direction is done by applying the gate R, which is another reflection with respect to state $|\varphi_1\rangle$:



Building such a gate R does not require using the function f again, as remember that $|\varphi_1\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle \left(\otimes |-\rangle \right)$, simply.

Here is the geometric procedure to build R:



So $R|\varphi\rangle = 2\langle\varphi_1|\varphi\rangle \cdot |\varphi_1\rangle - |\varphi\rangle$

We have $R|\varphi\rangle = 2\langle\varphi_1|\varphi\rangle \cdot |\varphi_1\rangle - |\varphi\rangle$

$$= 2\,|\varphi_1\rangle\cdot\langle\varphi_1|\varphi\rangle - |\varphi\rangle$$

$$= \Big(2\,\underbrace{|\varphi_1\rangle\langle\varphi_1|}_{\text{matrix !}} - I_n\Big)\cdot|\varphi\rangle$$

$$= \left(2\,H^{\otimes n}|\varphi_0\rangle\langle\varphi_0|H^{\otimes n} - I_n\right)\cdot|\varphi\rangle$$

$$= H^{\otimes n}\Big(2\,\underbrace{|\varphi_0\rangle}_{=|0\rangle\otimes\dots\otimes|0\rangle}\langle\varphi_0| - I_n\Big)H^{\otimes n}\cdot|\varphi\rangle$$

(we forget again state $|-\rangle$)

Exercise:

Build the gate $2|\psi_0\rangle\langle\psi_0| - I_n$

Hint: observe that

$$(2|\psi_0\rangle\langle\psi_0| - I_n)|\varphi\rangle$$

$$= \begin{cases} |\varphi\rangle & \text{if } |\varphi\rangle = |\psi_0\rangle = |0\rangle \otimes \dots \otimes |0\rangle \\ -|\varphi\rangle & \text{if } |\varphi\rangle \text{ is any other basis element} \end{cases}$$

Now, how to proceed from there on?

- With the successive application of U_f and R, the state evolves from

$$|\psi_1\rangle = \cos\theta_0 |P\rangle + \sin\theta_0 |s\rangle \qquad \text{angle } +\theta_0$$

to

$$|\psi_2\rangle = \cos\theta_0 |P\rangle - \sin\theta_0 |s\rangle \qquad \text{angle } -\theta_0$$

to

$$|\psi_3\rangle = \cos(3\theta_0) |P\rangle + \sin(3\theta_0) |s\rangle \qquad \text{angle } +3\theta_0$$

Therefore, the successive application of U_f and R corresponds to a <u>rotation of angle $+2\theta_0$</u>, which brings the state closer to state $|s\rangle$, which is our aim.

By <u>iterating this operation</u> an appropriate number of times, we can get arbitrarily close to $|s\rangle$ $\longrightarrow$ next week!