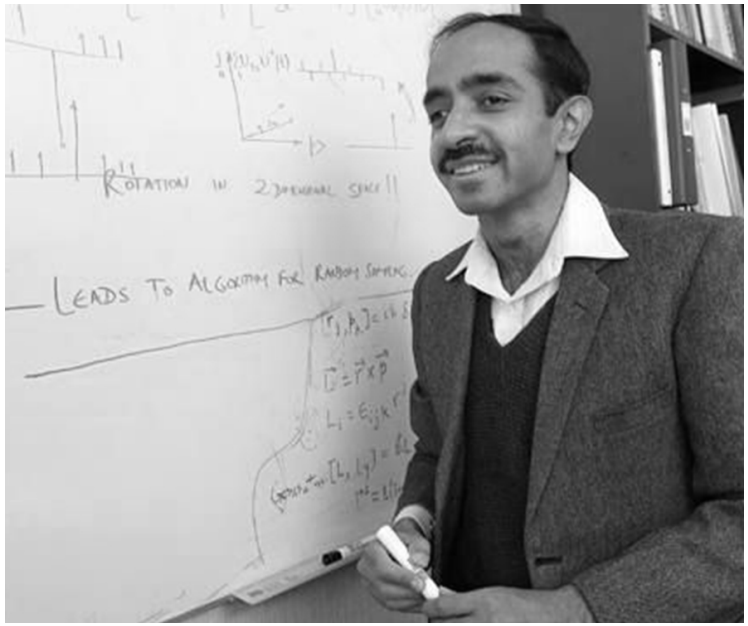
TRA-2-1 : Grover un algorithme utile

JM.Torres IBM Quantum France

15 novembre 2021

Lov Grover



Grover algorithm is associated to searching for an element in a non sorted list of $N = 2^n$ elements (which is not really a targeted case, but Grover algorithm proves to be useful in other use cases).

In the classic case, the search algorithm will require an average of N/2 trials (and up to N trials) with the quantum algorithm, the answer is provided in $\mathcal{O}(\sqrt{N})$

This is not an exponential advantage but a quadratic advantage. This one has been proved to be optimal (which is not always the case)

Grover's operator

We will search for an element w, and we are given an oracle U_f with $f : \{0,1\}^n \rightarrow \{0,1\}$ so that :

- $f(x) = 1$ if $x == w$
- $f(x) = 0$ in any other case

We also define $f_0 : \{0,1\}^n \rightarrow \{0,1\}$:

- $f_0(x) = 0$ if $x == 00...0$
- $f_0(x) = 1$ in any other case

Let us remind that :

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

Then for U_f we get :

$U_f : |w\rangle \rightarrow -|w\rangle$ and
$U_f : |x\rangle \rightarrow |x\rangle$ for all $x \neq w$

Grover's operator...

One can also write : $U_f = I - 2\left|w\right\rangle\left\langle w\right|$, in fact with that expression :

$$U_f\left|w\right\rangle = \left(I - 2\left|w\right\rangle\left\langle w\right|\right)\left|w\right\rangle = \left|w\right\rangle - 2\left|w\right\rangle\left\langle w|w\right\rangle = \left|w\right\rangle - 2\left|w\right\rangle = -\left|w\right\rangle$$

and if $x \neq w$:

$$U_f\left|x\right\rangle = \left(I - 2\left|w\right\rangle\left\langle w\right|\right)\left|x\right\rangle = \left|x\right\rangle - 2\left|w\right\rangle\underbrace{\left\langle w|x\right\rangle}_{=0} = \left|x\right\rangle$$

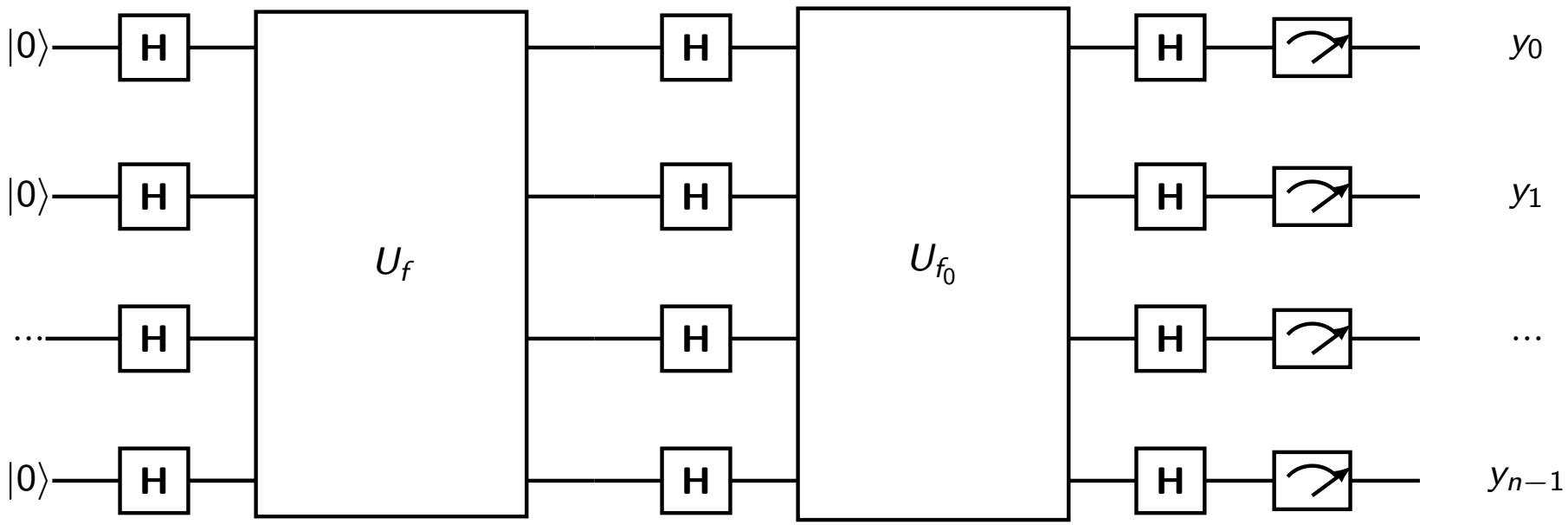
(because the bitstrings x different from w correspond to orthogonal states for w)

We can do the same for the function U_{f_0} :

$U_{f_0} : \left|0\right\rangle^{\otimes n} \rightarrow \left|0\right\rangle^{\otimes n}$ and
$U_{f_0} : \left|x\right\rangle \rightarrow -\left|x\right\rangle$ for all $x \neq 00...0$

And in this case, one can write : $U_{f_0} = 2\left|0\right\rangle\left\langle 0\right|^{\otimes n} - I$, we verify easily, as above, that this expression correspond to the definition of f_0.

Quantum circuit



(The bloc $U_f - H - U_f 0 - H$, is called V and will have to repeat itself r times)
We will prove that this algorithm will provide the result w ($y = w$ with a high probability).

Let us define $|s\rangle$, uniform superposition state, after the first Hadamard gates.

$$|s\rangle := H^{\otimes n} |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}} |x\rangle$$

Définitions

And

$$V := H^{\otimes n} U_{f_0} H^{\otimes n} = H^{\otimes n}(2\left|0\right\rangle\left\langle 0\right|^{\otimes n} - I)H^{\otimes n}$$

$$V := H^{\otimes n} 2\left|0\right\rangle\left\langle 0\right|^{\otimes n} H^{\otimes n} - H^{\otimes n} I H^{\otimes n}$$

$$V = 2H^{\otimes n}\left|0\right\rangle\left\langle 0\right|^{\otimes n} H^{\otimes n} - H^{\otimes n} H^{\otimes n}$$

$$V = 2\left|s\right\rangle\left\langle s\right| - I$$

Grover algorithm will apply $(V.U_f)^r$ onto state : $\left|s\right\rangle$

Now, let us define Σ the plane defined by $\left|s\right\rangle$ and $\left|w\right\rangle$, and let us define $\left|w^{\perp}\right\rangle$ being the vector in Σ and ortohgonal to $\left|w\right\rangle$:

$$\left|w^{\perp}\right\rangle := \frac{1}{\sqrt{2^n - 1}} \sum_{x \neq w} \left|x\right\rangle$$

Definitions...

Then $|s\rangle$ can be defined as a linear combination of $|w\rangle$ and $\left|w^{\perp}\right\rangle$:

$$|s\rangle := \frac{\sqrt{2^n - 1}}{\sqrt{2^n}} \left|w^{\perp}\right\rangle + \frac{1}{\sqrt{2^n}} |w\rangle$$

Finally, we define the angle θ such that :

$$|s\rangle := \cos\frac{\theta}{2} \left|w^{\perp}\right\rangle + \sin\frac{\theta}{2} |w\rangle$$

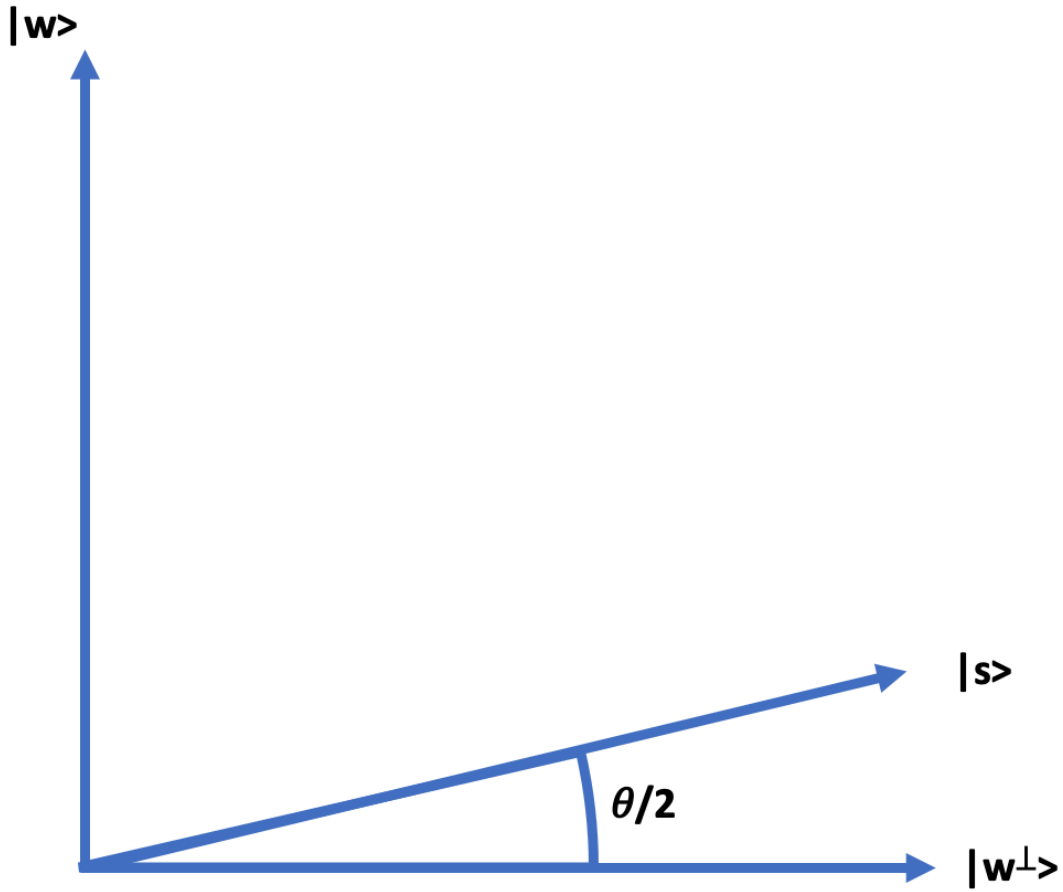
Which means :

$$\sin\frac{\theta}{2} = \frac{1}{\sqrt{2^n}}$$

$$\theta = 2\arcsin\frac{1}{\sqrt{2^n}}$$

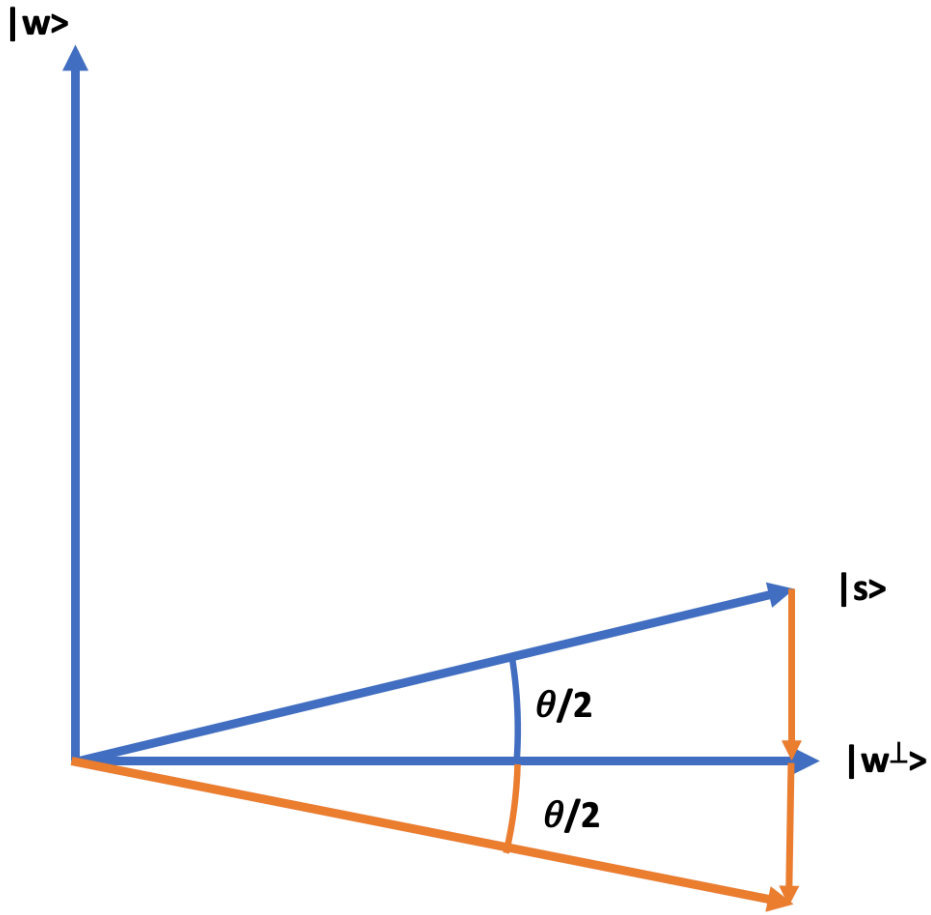
Grover algo, step 1

- The quantum circuit starts with $H^{\otimes n}$, which prepares $|s\rangle$



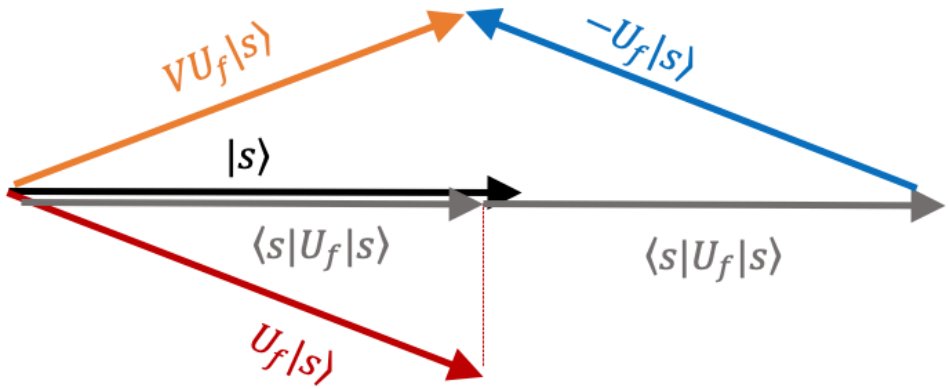
Grover algo, step 2

- $U_f = I - 2\left|w\right\rangle\left\langle w\right|$ is applied to $\left|s\right\rangle$ which gives : $\left|s\right\rangle$ minus two times the value of $\left\langle w|s\right\rangle$ in the direction of $-\left|w\right\rangle$. Which brings the result under $\left|w^{\perp}\right\rangle$ (it is a symmetry about the axis $\left|w^{\perp}\right\rangle$).



Grover Algo, étape 3

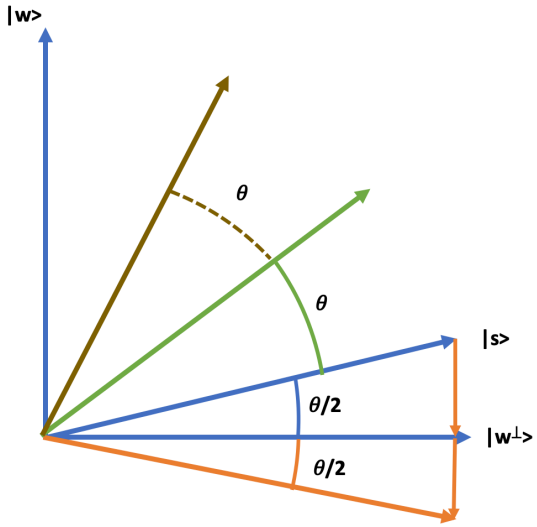
Then we apply $V = 2|s\rangle\langle s| - 1$: reflexion around $|s\rangle$, at this point we have performed a rotation of θ for the vector $|s\rangle$



(indeed $U_f|s\rangle$ has first made a symmetry of $|s\rangle$ about $|w^{perp}\rangle$ (which was away of $\theta/2$, so a rotation of θ to go from $|s\rangle$ to $U_f|s\rangle$. The symmetry around $|s\rangle$ results in a rotation of $|s\rangle$ of angle θ from its initial position).

Repetition

Applying operator V r times, vector $|s\rangle$ will have seen a rotation of $r\theta$



So we will choose r such that $r\theta + \frac{\theta}{2} \approx \frac{\pi}{2}$ to get as close as possible of $|w\rangle$, so $r \approx \frac{\pi}{2\theta} - \frac{1}{2}$, and remind that we have defined θ as a function of the number of qubits : $\theta = 2 \arcsin \frac{1}{\sqrt{2^n}}$

So we get this formula for r : $r \approx \frac{\pi}{4 \arcsin \frac{1}{\sqrt{2^n}}} - \frac{1}{2}$

When n grows arcsin of a small quantity almost equals this small quantity (also note that the term $\frac{1}{2}$ can be neglected), we are left with :

$$r \approx \frac{\pi}{4}\sqrt{2^n} = \mathcal{O}(\sqrt{N})$$

So we will choose the integer nearest to the value of r.

Efficacity

Finally, what is the probability of measuring w ?

After r calls to the oracle and the measurement, we will get the state $|w\rangle$.

worst case we end up in a state closer than $\frac{\theta}{2}$ (because we do rotations by step θ each time)

So probability $P(w)$ is at worst (corresponding to the max angle $\frac{\theta}{2}$) :

$$P(w) = \cos^2 \frac{\theta}{2}$$

Then :

$$P(w) \geq 1 - \sin^2 \frac{\theta}{2}$$

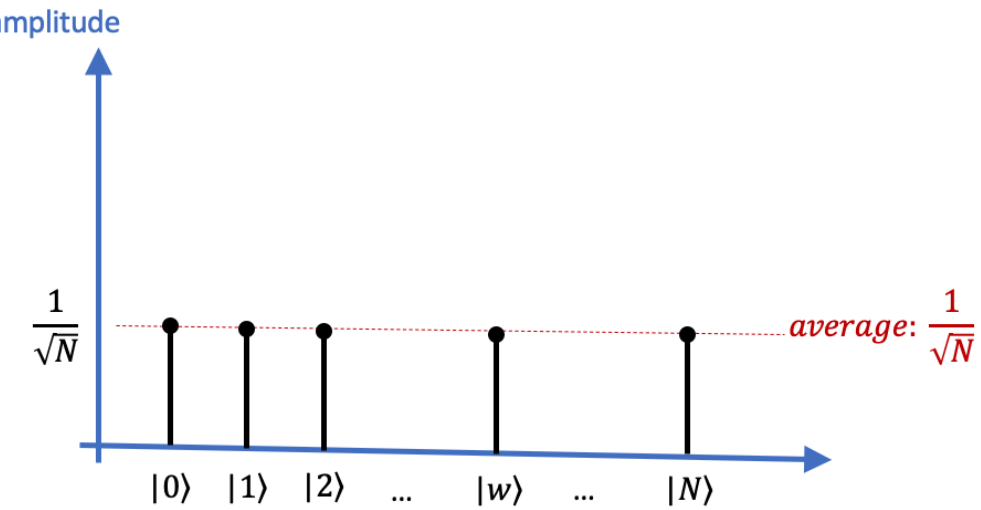
(because we have $\sin \frac{\theta}{2} = \frac{1}{\sqrt{2^n}}$)

$$P(w) \geq 1 - \frac{1}{2^n}$$

This value goes to 1 when n increases.

Amplitude amplification

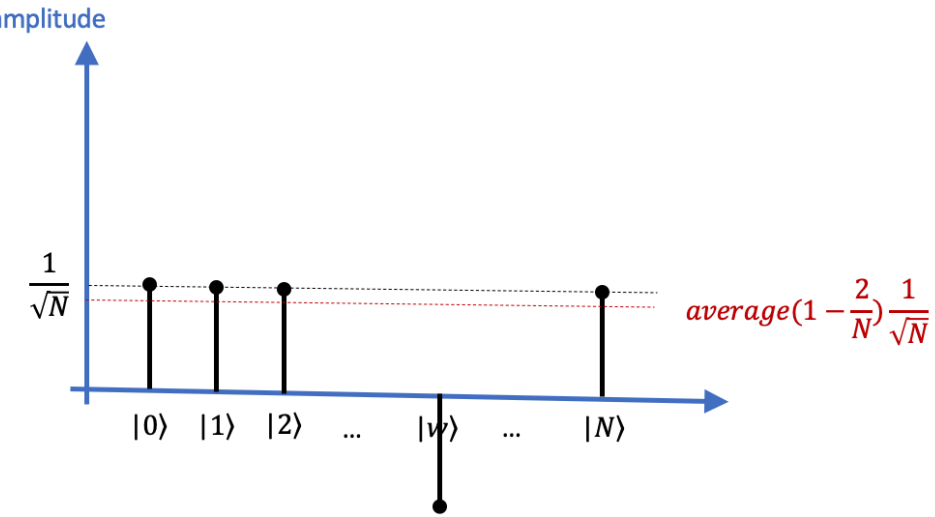
Something worth noticing in the Grover algorithm is the notion of amplitude amplification :
Let's go back to the Grover algorithm steps :
Once in the state $|s\rangle = H^{\otimes n}|0\rangle^{\otimes n}$, every state carries the same amplitude :



Amplitude average is $\frac{1}{\sqrt{N}}$.

Amplitude amplification

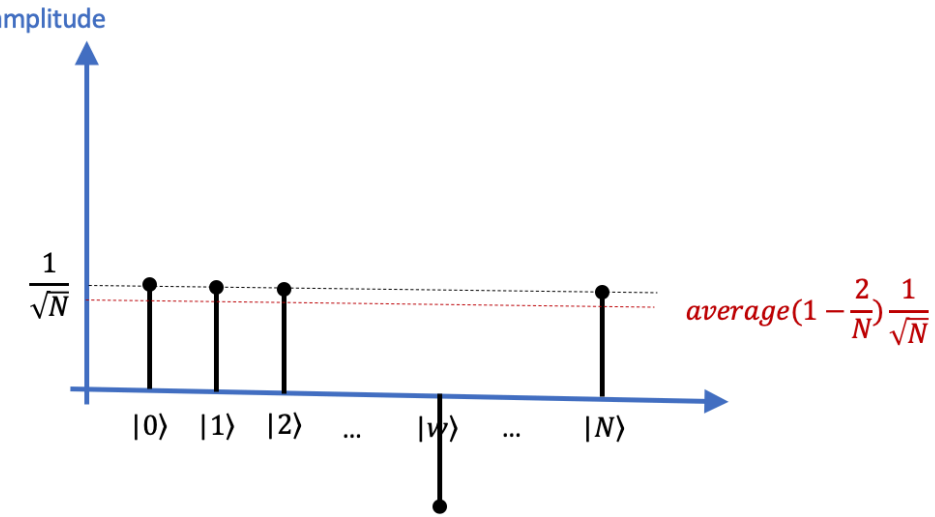
Next we apply U_f to $|s\rangle$
(and by definition and construction of U_f, the states$|k\rangle$ for $k \neq w$ are left unchanged (the $|k\rangle$ and $|w\rangle$ are orthogonal with each others), and $|w\rangle$ becomes $-|w\rangle$, so we get the state :



Now the average has become : $(1 - \frac{2}{N}).\frac{1}{\sqrt{N}}$

Amplitude amplification

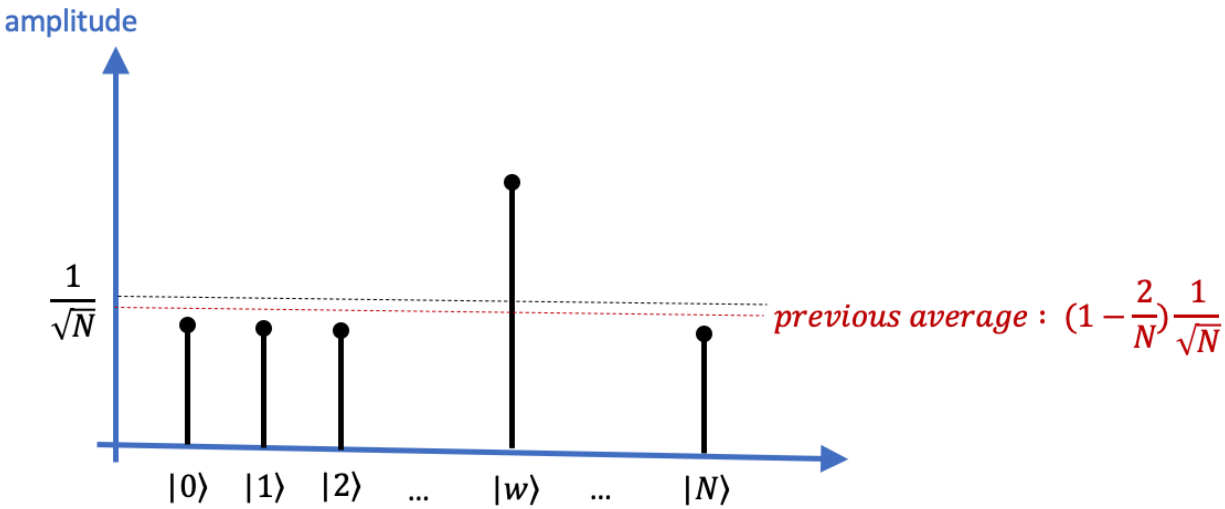
Next we apply U_f to $|s\rangle$
(and by definition and construction of U_f, the states$|k\rangle$ for $k \neq w$ are left unchanged (the $|k\rangle$ and $|w\rangle$ are orthogonal with each others), and $|w\rangle$ becomes $-|w\rangle$, so we get the state :



Now the average has become : $(1 - \frac{2}{N}).\frac{1}{\sqrt{N}}$

Amplitude amplification

Next iteration :



... and so on

Amplitude amplification

Now we apply $V = 2|s\rangle\langle s| - I$: let's show that this operator has the effect of reversing each state amplitude around the average of states amplitude :
Let $|\Psi\rangle$ be a quantum state of n qubits :

$$|\Psi\rangle = \sum_{i=1}^{n} \alpha_i |i\rangle$$

Applying V to $|\Psi\rangle$

$$V|\Psi\rangle = (2|s\rangle\langle s| - I)|\Psi\rangle$$

$$V|\Psi\rangle = (2\frac{1}{\sqrt{N}}\sum_j |j\rangle \frac{1}{\sqrt{N}}\sum_k \langle k| - I)|\Psi\rangle$$

$$V|\Psi\rangle = (2\frac{1}{N}\sum_j |j\rangle \sum_k \langle k| - I)\sum_i |i\rangle$$

$$V|\Psi\rangle = 2\frac{1}{N}\sum_j |j\rangle \sum_k \langle k| \sum_i \alpha_i |i\rangle - \sum_i \alpha_i |i\rangle$$

Amplitude amplification

We evaluate $\sum_k \langle k| \sum_i \alpha_i |i\rangle$
In fact when $i = k$ then $\langle k|i\rangle = 1$ and when $i \neq k$ then $\langle k|i\rangle = 0$

We are left with $\sum_k \alpha_k$ and so :

$$V|\Psi\rangle = 2\frac{1}{N}\sum_j |j\rangle \sum_k \alpha_k - \sum_i \alpha_i |i\rangle$$

We move $\sum_k \alpha_k$ to the left : and we note $\langle\alpha\rangle$ the average of α_k ($\frac{1}{N}\sum_k \alpha_k$), so we get thee following (we can also use the j summation index on the right term :

$$V|\Psi\rangle = 2\langle\alpha\rangle \sum_j |j\rangle - \sum_j \alpha_j |j\rangle$$

Then we can write :

$$V|\Psi\rangle = \sum_j (2\langle\alpha\rangle - \alpha_j)|j\rangle$$

For each α_j, this quantity : $2\langle\alpha\rangle - \alpha_j$ is indeed an inversion about the average.
because : $\alpha_j := \langle\alpha\rangle + \Delta_j$
Then $2\langle\alpha\rangle - \alpha_j$ equals $2\langle\alpha\rangle - (\langle\alpha\rangle + \Delta_j) = \langle\alpha\rangle - \Delta_j$

Case of multiple selected elements

If the oracle can select M elements, then the state we are looking for is an equal superposition of each state selected by the oracle :

$$|w\rangle := \frac{1}{M}\sum_{i=1}^{M}|w_i\rangle \qquad \text{and then} \qquad \left|w^{\perp}\right\rangle = \frac{1}{\sqrt{N-M}}\sum_{x\notin\{w_1,\dots w_M\}}|x\rangle$$

Then we define (af before) s et θ :

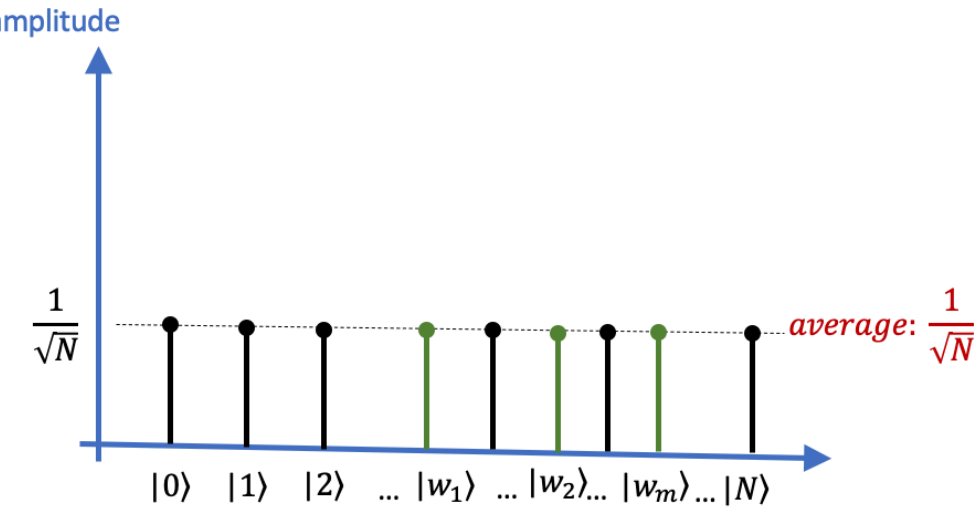
$$|s\rangle = \frac{\sqrt{N-M}}{\sqrt{N}}\left|w^{\perp}\right\rangle + \sqrt{\frac{M}{N}}|w\rangle = \cos\frac{\theta}{2}\left|w^{\perp}\right\rangle + \sin\frac{\theta}{2}|w\rangle$$

Then : $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$ (θ is a larger angle as compared to the single element case : the Grover algorithm will require less iterations.

$$r \approx \frac{\pi}{4\arcsin\sqrt{\frac{M}{N}}} = \mathcal{O}(\sqrt{\frac{M}{N}})$$

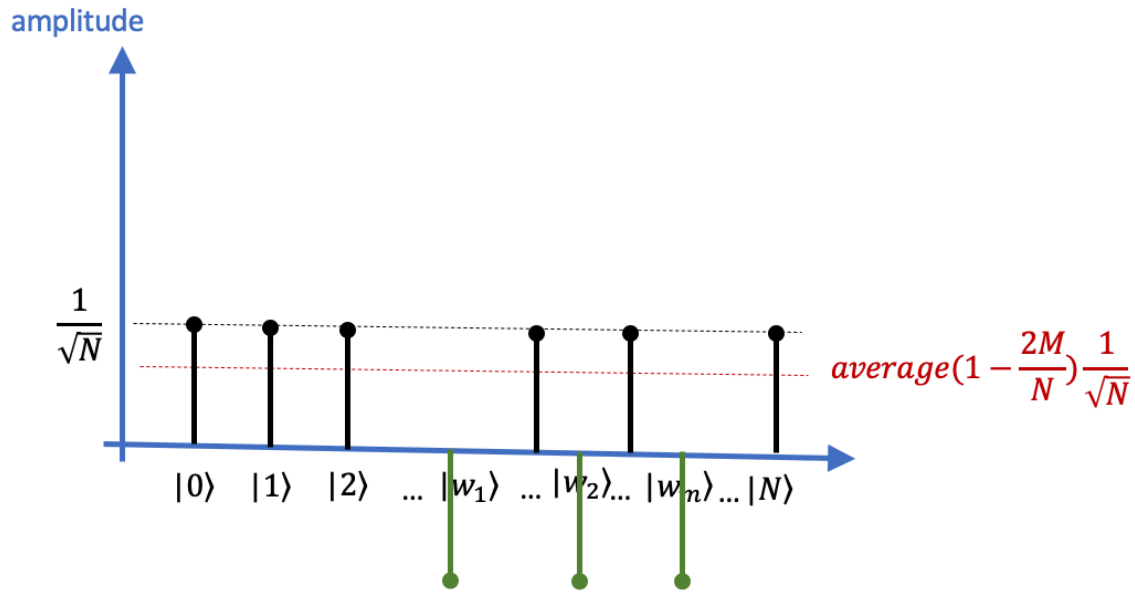
Case of multiple selected elements

The convergence appears to be even faster for the amplitude amplification in this case (compared to single marked element) : We start with :



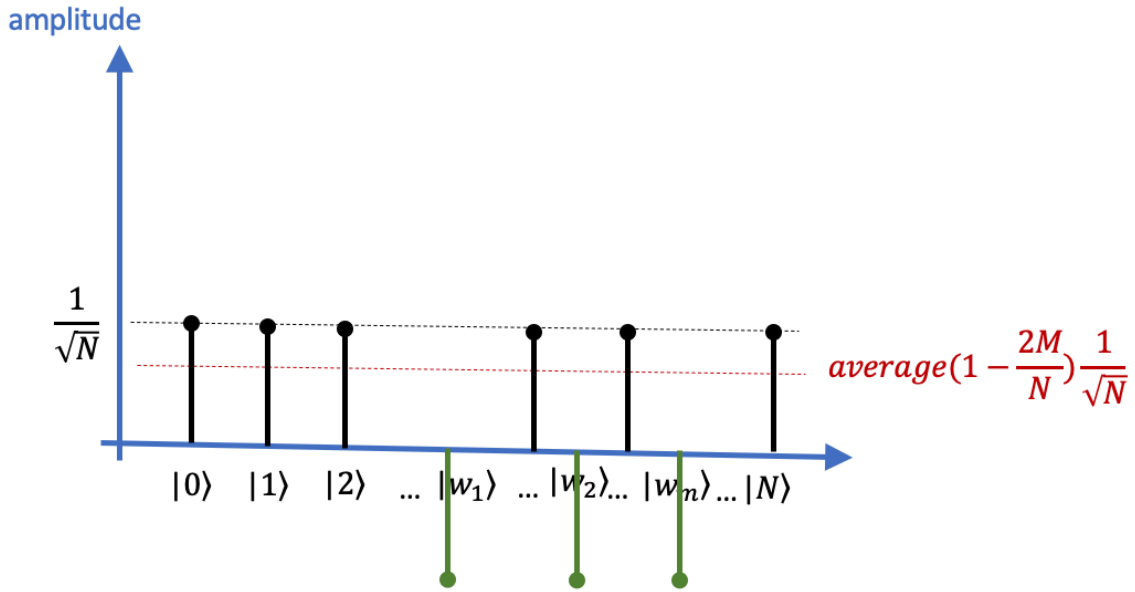
Case of multiple selected elements

Next ,we have :



Case of multiple selected elements

And so on :



Viewing Austin Gilliam (E...

Grover Adaptive Search for CPBO

Grover Adaptive Search for Constrained Polynomial Binary Optimization

Austin Gilliam,[1] Stefan Woerner,[2] and Constantin Gonciulea[1]

[1] *JPMorgan Chase*
[2] *IBM Research – Zurich*

(Dated: December 10, 2019)

In this paper we discuss Grover Adaptive Search (GAS) for Constrained Polynomial Binary Optimization (CPBO) problems, and in particular, Quadratic Unconstrained Binary Optimization (QUBO) problems, as a special case. GAS can provide a quadratic speed-up for combinatorial optimization problems compared to brute force search. However, this requires the development of efficient oracles to represent problems and flag states that satisfy certain search criteria. In general, this can be achieved using quantum arithmetic, however, this is expensive in terms of Toffoli gates as well as required ancilla qubits, which can be prohibitive in the near-term. Within this work, we develop a way to construct efficient oracles to solve CPBO problems using GAS algorithms. We demonstrate this approach and the potential speed-up for the portfolio optimization problem, i.e. a QUBO, using simulation. However, our approach applies to higher-degree polynomial objective functions as well as constrained optimization problems.

arXiv:abs/1912.04088