Lecture 9: Amplitude Amplification Algorithms

Lecturer: Jean-François Biasse *TA: Robert Hart*

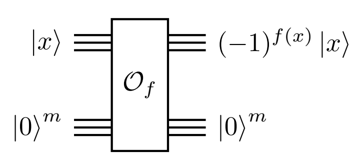
In this lecture, we focus on Grover's algorithm, and its generalization the quantum amplification strategy. The idea is that we are looking for one of M marked elements inside a set of $N > M$ elements. The marked elements $x \in \{1, \ldots, N\}$ satisfy $f(x) = 1$ for some function f. If we do not assume any particular structure (such as an ordering of the elements for example), then on the worst case scenario, a classical algorithm would need to evaluate f at $N - M$ elements before finding the correct one. On average, N/M elements could suffice. With a quantum computer however, we can get away with evaluating f only $\sqrt{M/N}$ time on average. Like the Deutsch-Jozsa algorithm, this result demonstrate the superiority of quantum computers over their classical counterpart for certain comptutational tasks.

9.1 Grover's search method

Grover's search algorithm starts with the state $|0\rangle^{\otimes n}$, and after applying $H^{\otimes n}$, we obtain the state

$$|\psi\rangle := \frac{1}{\sqrt{N}} \sum_x |x\rangle .$$

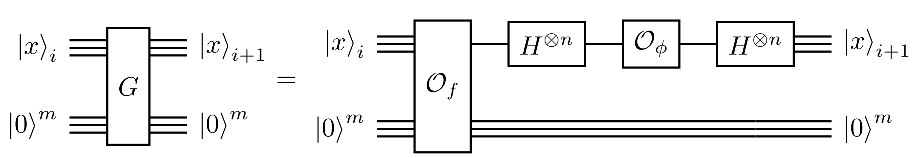
A measurement on the system in the sate $|\psi\rangle$ would yield a marked element with probability M/N. Grover's algorithm proposes to perform a series of computations aiming to raise the amplitude of the $|x\rangle$ for x a marked element while reducing all the other ones. At the end of the procedure, a measurement will likely yield a marked element. For this, we need a circuit that evaluates f. More specifically, we need to implement the circuit



We call this circuit the "oracle". A typical use case is when we know an efficient classical algorithm for f. Then using the methods previously seen, we can efficiently implement $\mathcal{O}_f$. The other essential ingredient is a conditional phase shift circuit called $\mathcal{O}_\phi$ that realizes the following transformation

$$\mathcal{O}_\phi |0\rangle = |0\rangle , \quad \text{and} \quad \mathcal{O}_\phi |x\rangle = - |x\rangle \quad \text{for} \quad x \neq 0.$$

Grover's algorithm is the repetition of an elementary step involving $\mathcal{O}_f$ and $\mathcal{O}_\phi$ that we call the "Grover iterate". It can be represented like this



Proposition 9.1 *The action of $H^{\otimes n}\mathcal{O}_\phi H^{\otimes n}$ is the linear operator $2\left|\psi\right\rangle\left\langle\psi\right| - I$, and the Grover operators is*

$$G = (2\left|\psi\right\rangle\left\langle\psi\right| - I)\,\mathcal{O}_f.$$

Proof: The conditional phase shift acts as $2\left|0\right\rangle\left\langle 0\right| - I$. Then by substituting it in $H^{\otimes n}\mathcal{O}_\phi H^{\otimes n}$ we get

$$\begin{aligned}
H^{\otimes n}\mathcal{O}_\phi H^{\otimes n} &= H^{\otimes n}2\left|0\right\rangle\left\langle 0\right| - I)(H^{\otimes n} \\
&= (2H^{\otimes n}\left|0\right\rangle\left\langle 0\right| - H^{\otimes n})H^{\otimes n} \\
&= 2H^{\otimes n}\left|0\right\rangle\left\langle 0\right| H^{\otimes n} - H^{\otimes n}H^{\otimes n} \\
&= 2\left|\psi\right\rangle\left\langle\psi\right| - I \quad \text{since} \quad H^{\otimes n}H^{\otimes n} = I \quad \text{and} \quad H^{\otimes n}\left|0\right\rangle = \left|\psi\right\rangle
\end{aligned}$$

The result on G follows since the Grover iterate is the composition of $\mathcal{O}_f$ with the above block. ∎

Proposition 9.2 *The operator $2\left|\psi\right\rangle\left\langle\psi\right| - I$ realizes the following operation*

$$\sum_x \alpha_x \left|x\right\rangle \longmapsto \sum_x (-\alpha_x + 2\langle\alpha\rangle)\left|x\right\rangle,$$

where $\langle\alpha\rangle := \frac{1}{N}\sum_x \alpha_x$. We call this operation the inversion about the mean.

Proof: We have the following identities

$$\begin{aligned}
(2\left|\psi\right\rangle\left\langle\psi\right| - I)\left(\sum_x \alpha_x\left|x\right\rangle\right) &= 2\left|\psi\right\rangle\left\langle\psi\right|\left(\sum_x \alpha_x\left|x\right\rangle\right) - \sum_x \alpha_x\left|x\right\rangle \\
&= 2\left|\psi\right\rangle\sum_x \alpha_x\left\langle\psi|x\right\rangle - \sum_x \alpha_x\left|x\right\rangle \\
&= 2\left|\psi\right\rangle\sum_x\left(\frac{1}{\sqrt{N}}\sum_x \alpha_x\right) - \sum_x \alpha_x\left|x\right\rangle \\
&= 2\langle\alpha\rangle\sqrt{N}\left|\psi\right\rangle - \sum_x \alpha_x\left|x\right\rangle \\
&= 2\langle\alpha\rangle\sum_x\left|x\right\rangle - \sum_x \alpha_x\left|x\right\rangle
\end{aligned}$$

∎

There is an elegant interpretation of the action of the Grover iterate that helps quantifying how many interations are required to ensure the optimum probability of measuring a marked element. Let $S \subseteq \{1, \ldots N\}$ be the set of marked elements of cardinality $|S| = M < N$. Additionally, we define the states

$$\left|\alpha\right\rangle = \frac{1}{\sqrt{N-M}}\sum_{x\notin S}\left|x\right\rangle \quad \text{and} \quad \left|\beta\right\rangle = \frac{1}{\sqrt{M}}\sum_{x\in S}\left|x\right\rangle$$

We clearly see that $\left|\alpha\right\rangle \perp \left|\beta\right\rangle$, and that

$$\left|\psi\right\rangle = \sqrt{\frac{N-M}{N}}\left|\alpha\right\rangle + \sqrt{\frac{M}{N}}\left|\beta\right\rangle$$

Proposition 9.3 *The Grover iterate G acts on* $\mathrm{Span}\{\left|\alpha\right\rangle, \left|\beta\right\rangle\}$ *as*

$$G = \begin{pmatrix}\cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta)\end{pmatrix},$$

where θ is defined by $\cos(\theta/2) = \sqrt{\frac{N-M}{N}}$ and $\sin(\theta/2) = \sqrt{\frac{M}{N}}$. This means that G acts as a rotation of angle θ.

Proof: Let us evaluate the action of the Grover iterate on $|\alpha\rangle$.

$$\begin{aligned}
G|\alpha\rangle &= \frac{G}{\sqrt{N-M}}\sum_{x\notin S}|x\rangle \\
&= (2|\psi\rangle\langle\psi| - I)\frac{1}{\sqrt{N-M}}\sum_{x\notin S}|x\rangle \\
&= \frac{2}{\sqrt{N-M}}|\psi\rangle\langle\psi|\sum_{x\notin S}|x\rangle - \frac{1}{\sqrt{N-M}}\sum_{x\notin S}|x\rangle \\
&= \frac{2}{\sqrt{N}\sqrt{N-M}}|\psi\rangle\sum_{x\notin S}1 - \frac{1}{\sqrt{N-M}}\sum_{x\notin S}|x\rangle \\
&= \frac{2\sqrt{N-M}}{N}\sum_{x}|x\rangle - \frac{1}{\sqrt{N-M}}\sum_{x\notin S}|x\rangle \\
&= \frac{2\sqrt{N-M}}{N}\sum_{x\in S}|x\rangle + \left(\frac{2\sqrt{N-M}}{N} - \frac{1}{\sqrt{N-M}}\right)\sum_{x\notin S}|x\rangle \\
&= \underbrace{\frac{2\sqrt{M}\sqrt{N-M}}{N}}_{\sin(\theta)}\underbrace{\frac{1}{\sqrt{M}}\sum_{x\in S}|x\rangle}_{|\beta\rangle} + \underbrace{\frac{2(N-M)}{N} - 1}_{\cos(\theta)}\underbrace{\frac{1}{\sqrt{N-M}}\sum_{x\notin S}|x\rangle}_{|\alpha\rangle}.
\end{aligned}$$

Thus $G|\alpha\rangle = \cos(\theta)|\alpha\rangle + \sin(\theta)|\beta\rangle$. Likewise, we can prove that $G|\beta\rangle = -\sin(\theta)|\alpha\rangle + \cos(\theta)|\beta\rangle$, which shows that G acts like a rotation of angle θ. ∎

Since we start with the state $|\psi\rangle = \cos(\theta/2)|\alpha\rangle + \sin(\theta/2)|\beta\rangle$, the state we reach after k iterations is

$$G^k|\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle.$$

To maximize our chances to measure an element in S, we want that $\frac{2k+1}{2}\theta \approx \frac{\pi}{2}$. This leads us to choose $k = \left\lfloor \frac{\pi}{2\theta} - \frac{1}{2} \right\rceil$ where $\lfloor x \rceil$ denotes the rounding of x to the nearest integer. In particular, this means that

$$\left|\frac{2k+1}{2}\theta - \frac{\pi}{2}\right| \leq \theta\left|k - \left(\frac{\pi}{2\theta} - \frac{1}{2}\right)\right| \leq \frac{\theta}{2}.$$

When we assume that $M \leq N/2$, we can choose $\theta \in [0, \pi/2]$, and therefore, $0 \leq \theta/2 \leq \pi/4$, and we have

$$\frac{\sqrt{2}}{2} \leq \sin\left(\frac{2k+1}{2}\theta\right) \leq 1.$$

Proposition 9.4 *Assuming that $M \leq N/2$, a measurement of the state after $k \leq \left\lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rceil$ yields $x \in S$ with probability at least $\frac{1}{2}$.*

Proof: We have seen that after $k = \left\lfloor \frac{\pi}{2\theta} - \frac{1}{2} \right\rceil$ a projective measurement with respect to $|\beta\rangle$ leaves the system in the state $|\beta\rangle$ (a superposition of all solutions) with probability

$$\sin^2\left(\frac{2k+1}{2}\theta\right) \geq \frac{1}{2}.$$

Since we have

$$\frac{\theta}{2} \geq \sin\left(\frac{\theta}{2}\right) = \sqrt{\frac{M}{N}},$$

we can conclude that $k = \left\lfloor \frac{\pi}{2\theta} - \frac{1}{2} \right\rceil \leq \left\lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rceil$. ■

9.2 Amplitude amplification

Grover's search algorithm can be viewed as a special case of a more general family of search algorithm: *amplitude amplification* algorithms. These algorithms assume the knowledge of an algorithm A that produces a superposition over all possible outcomes with certain weights

$$A\left|0\right\rangle^{\otimes n} = \sum_{x<N} \alpha_x \left|x\right\rangle \left|\text{junk}(x)\right\rangle = \left|\psi\right\rangle.$$

In the case of Grover's algorithm, $A = H^{\otimes n}$, but in general, the measurement of $\left|\psi\right\rangle$ yields $x \in S$ with probability

$$1 > p = \sum_{x\in S} |\alpha_x|^2 > 0$$

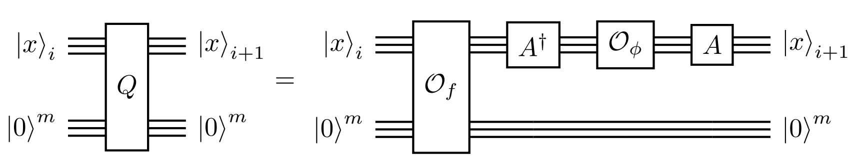
that is not necessarily M/N (it is hopefully better than that, otherwise we can Grover's algorithm). We define the states

$$\left|\alpha\right\rangle = \frac{1}{\sqrt{1-p}} \sum_{x\notin S} \alpha_x \left|x\right\rangle \left|\text{junk}(x)\right\rangle \quad \text{and} \quad \left|\beta\right\rangle = \frac{1}{\sqrt{p}} \sum_{x\in S} \alpha_x \left|x\right\rangle \left|\text{junk}(x)\right\rangle$$

We clearly see that $\left|\alpha\right\rangle \perp \left|\beta\right\rangle$, and that

$$\left|\psi\right\rangle = \sqrt{1-p}\left|\alpha\right\rangle + \sqrt{p}\left|\beta\right\rangle$$

We define the search iteration as



where the states $\left|x\right\rangle_i$ include the qubits necessary to hold the junk space. Similarly to the Grover iterate, we have the following result with the new notations.

Proposition 9.5 *The action of $A\mathcal{O}_\phi A^\dagger$ is the linear operator $2\left|\psi\right\rangle\left\langle\psi\right| - I$, and the amplitude amplification iterate is*

$$Q = \left(2\left|\psi\right\rangle\left\langle\psi\right| - I\right)\mathcal{O}_f.$$

Still following the analogy with the Grover search method, we can view the amplitude amplification as a rotation.

Proposition 9.6 *The amplitude amplification iterate Q acts on* $\mathrm{Span}\{|\alpha\rangle, |\beta\rangle\}$ *as*

$$G = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix},$$

where θ is defined by $\cos(\theta/2) = \sqrt{1-p}$ and $\sin(\theta/2) = \sqrt{p}$. This means that Q acts as a rotation of angle θ.

Since we start with the state $|\psi\rangle = \cos(\theta/2)|\alpha\rangle + \sin(\theta/2)|\beta\rangle$, the state we reach after k iterations is

$$Q^k |\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle .$$

As before, the probability of measuring $x \in S$ at the end of the procedure is $\sin\left(\frac{2k+1}{2}\theta\right)^2$. We perform the minimum number of iterations k such that $\sin\left(\frac{2k+1}{2}\theta\right) \approx \sin(\pi/2)$. Following the same arguments as before, we get the following bound on the number of iterations required.

Proposition 9.7 *Assuming that $p \leq 1/2$, a measurement of the state after $k \leq \left\lceil \frac{\pi}{4}\sqrt{p} \right\rceil$ yields $x \in S$ with probability at least $\frac{1}{2}$.*

This means that amplitude amplification uses an algorithm that would take $O(1/p)$ steps to return $x \in S$ with probability $1/2$ as a subroutine of another algorithm that only $O(1/\sqrt{p})$ steps to return $x \in S$ with probability $1/2$. This generalizes Grover's algorithm that uses the uniform superposition of all $x < N$, which takes $O(M/N)$ attempts through measurements to return $x \in S$ as a subroutine of a procedure that only takes $O\left(\sqrt{\frac{M}{N}}\right)$ steps.