Grover's Search

Selman Özleyen

Technische Universität München
School of Computation, Information and Technology

December 2022

Problem Definition

We would like to find a specific entry from an unsorted database consisting of N entries. We can model this like the following:

1. Let the index of the desired element be w.
2. Let f be a function $f : [N-1] \rightarrow \{0,1\}$ s.t. $f(w) = 1$ and $f(x) = 0$ for all other elements.
3. We have f but we don't have w, so we want to find it.

Grover's Oracle

We access f with an *oracle*. It can be written as a unitary operator U_w defined as below,

$$U_w|x\rangle = \begin{cases} |x\rangle & \text{if } x \neq w \\ -|x\rangle & \text{if } x = w \end{cases}$$

Note that $|x\rangle = |x_{n-1}...\rangle|x_1\rangle|x_0\rangle$ where $n = \lceil \log N \rceil$.

Grover's Oracle: Example

Example: Consider the case when we have 8 entries and the winner index is 2. Our oracle looks like

$$U_w = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Quantum Oracles

In general, such quantum oracles for search algorithms are usually written as the following.

- Let $f(x)$ be a classical function s.t. $f(x) = 1$ if x is what we search for, else $f(x) = 0$.
- Usually, the effect is written as $U_f|x\rangle = (-1)^{f(x)}|x\rangle$.
- There can be more than one x s.t. $f(x) = 1$ in general.
- We focus on the case when there is only one solution.
- But the algorithm also works for multiple solutions!

In short, Quantum Oracles flip the phase of the solution state.

Grover's Oracle in Practice

How to implement an oracle without knowing the solution?

1. Create a classical (possibly irreversible) circuit that recognizes the solution.
2. Construct a reversible classical circuit from it.
3. Use *phase kickback* and *uncomputation* to turn this circuit into an oracle[1].

We won't cover the details of *phase kickback* and *uncomputation* concepts.

[1] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. 2011. ISBN: 1107002176.

Grover's Oracle in Practice: Wrap Up

But in general we should know that

- It is easy to convert a problem into an oracle form.
- Because we don't need to find the solution, verifying it is usually enough[2].
- For example, we can create a circuit to verify a Sudoku solution.
- Which is much easier than finding a Sudoku solution.

[2] A tA v et al. *Qiskit: An Open-source Framework for Quantum Computing*. 2021. DOI: 10.5281/zenodo.2573505.

Algorithm Outline

Grover's algorithm can be summarized as two stages.

1. Create a quantum oracle.
2. Apply *amplitude amplification*

In the following, we will cover amplitude amplification.

Amplitude Amplification: Operators & Notation

Let $|\boldsymbol{s}\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |\boldsymbol{x}\rangle$ and $|\boldsymbol{s'}\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq w} |\boldsymbol{x}\rangle$. We define the following operators:

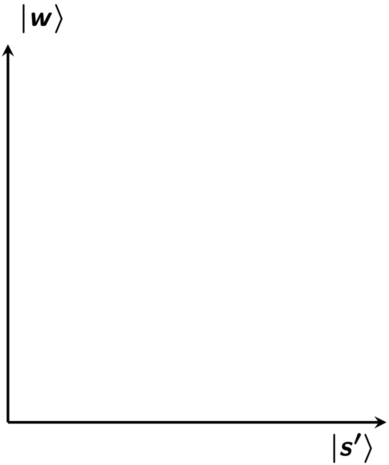
(i) $U_s = 2|\boldsymbol{s}\rangle\langle\boldsymbol{s}| - I$

(ii) $U_w = I - 2|\boldsymbol{w}\rangle\langle\boldsymbol{w}|$

Notice that U_w is still the oracle, just written differently.

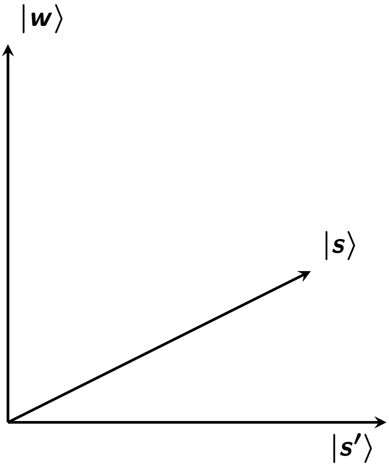
Amplitude Amplification: Geometric View

Recall that $|\boldsymbol{s}\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |\boldsymbol{x}\rangle$
and $|\boldsymbol{s'}\rangle = \frac{1}{\sqrt{N-1}} \sum_{x\neq w} |\boldsymbol{x}\rangle$.



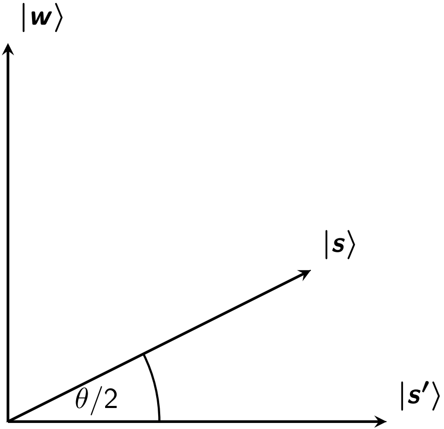
Amplitude Amplification: Geometric View

We know that $|s\rangle$ lies between $|w\rangle$ and $|s'\rangle$



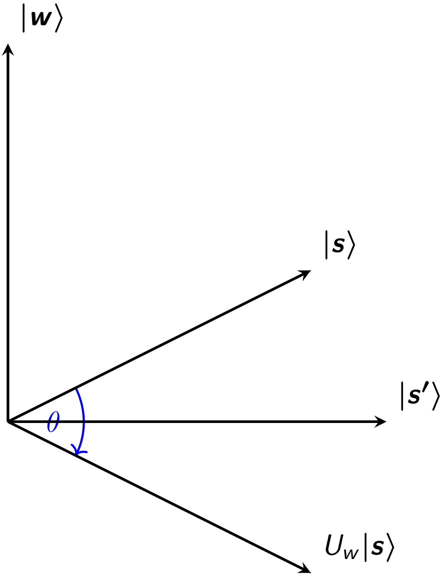
Amplitude Amplification: Geometric View

Let's denote the angle between $|\boldsymbol{s}\rangle$ and $|\boldsymbol{s'}\rangle$ as $\theta/2$



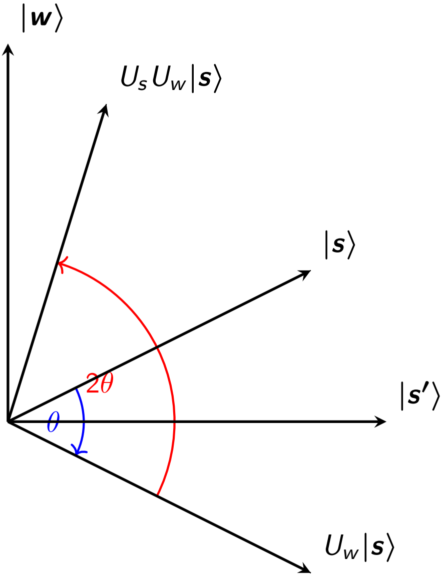
Amplitude Amplification: Geometric View

We apply U_w to $|\boldsymbol{s}\rangle$ because it acts as a reflection across $|\boldsymbol{s'}\rangle$.



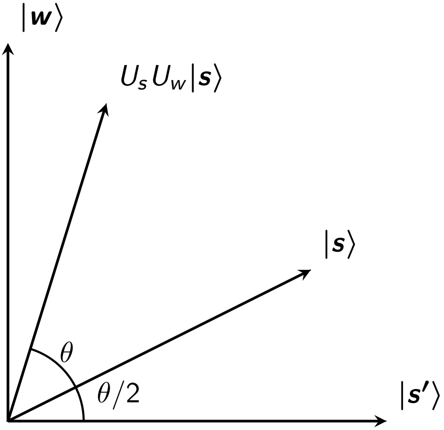
Amplitude Amplification: Geometric View

Then we apply U_s to $U_w|\boldsymbol{s}\rangle$ which acts as a reflection across $|\boldsymbol{s}\rangle$.


$|\boldsymbol{w}\rangle$
$U_sU_w|\boldsymbol{s}\rangle$
$|\boldsymbol{s}\rangle$
2θ
$|\boldsymbol{s'}\rangle$
θ
$U_w|\boldsymbol{s}\rangle$

Amplitude Amplification: Geometric View

The $|\boldsymbol{s}\rangle$ had a magnitude of $\sin(\theta/2)$ on $|\boldsymbol{w}\rangle$. The result $U_s U_w|\boldsymbol{s}\rangle$ has magnitude of $\sin(3\theta/2)$ on $|\boldsymbol{w}\rangle$



Amplitude Amplification: Applying Iterations

- $U_s U_w |\boldsymbol{s}\rangle$ has magnitude of $\sin(3\theta/2)$ on $|\boldsymbol{w}\rangle$.
- After r iterations: $(U_s U_w)^r |\boldsymbol{s}\rangle$ will have a magnitude of $\sin(\theta(r+1/2))$ on $|\boldsymbol{w}\rangle$.

Amplitude Amplification: Finding Number of Iterations

Following from the previous results, we conclude:

- The probability of measuring the solution is $\sin\left(\theta\left(r + 1/2\right)\right)^2$.
- By our definition of θ, we know $\theta = 2\arcsin\frac{1}{\sqrt{N}}$.
- We use this to maximize $\sin\left(\theta\left(r + 1/2\right)\right)^2$ w.r.t r.
- This is maximized when we set $r \approx \pi\sqrt{N}/4$.

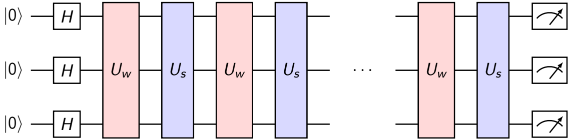
So we need $O(\sqrt{N})$ iterations to measure the solution with high probability. One can also show that the error is $O(1/N)$[3].

[3] Lov K. Grover. "Quantum Mechanics Helps in Searching for a Needle in a Haystack". In: 79.2 (1997), pp. 325–328.

Grover's Algorithm

To find our solution in $O(\sqrt{N})$ steps we:

1. Create a quantum oracle U_w
2. Compute $(U_s U_w)^r |\boldsymbol{s}\rangle$ with appropriate amount of r.
3. Measure the result.



Summary

We will see how this algorithm can be done in a quantum circuit.
But to summarize until now:

- It is conceptually easy to create a quantum oracle from classical circuits.
- Quantum computers can find an entry from an unsorted database in $O(\sqrt{N})$ iterations.
- While classical computers need $O(N)$.

References

- Grover, Lov K. "Quantum Mechanics Helps in Searching for a Needle in a Haystack". In: 79.2 (1997), pp. 325–328.
- Nielsen, Michael A. and Isaac L. Chuang. *Quantum Computation and Quantum Information*. 2011. ISBN: 1107002176.
- v, A tA et al. *Qiskit: An Open-source Framework for Quantum Computing*. 2021. DOI: 10.5281/zenodo.2573505.