COL7160 : Quantum Computing

Lecture 18: Grover Search

Instructor: Rajendra Kumar **Scribe:** Tirth Golwala

1 Grover Search

1.1 Unique search problem

Problem. We consider the unique search problem. Let

$$x = x_0 x_1 \cdots x_{N-1} \in \{0,1\}^N.$$

The promise is that there exists a unique index i such that

$$x_i = 1 \qquad \text{and} \qquad x_j = 0 \quad \text{for all } j \neq i.$$

The task is to find this marked index.
We would like to prepare the superposition

$$\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |x_i\rangle |i\rangle .$$

QRAM bottleneck. To do this, the string x must be stored in QRAM, that is, *Quantum Random Access Memory*. This is very expensive, and it becomes a bottleneck in algorithms that use Grover search.
Boolean function form. Instead of working directly with the database string, we introduce a Boolean function

$$f : \{0,1\}^n \to \{0,1\},$$

where x represents the index. The goal is to find an x such that

$$f(x) = 1.$$

Standard quantum procedure. We start with

$$|0\rangle^{\otimes n} |0\rangle ,$$

apply Hadamard gates on the first register to get

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

and then apply the oracle U_f, defined by

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle ,$$

to obtain

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle .$$

Query complexity. If the number of solutions is t, then Grover search gives an

$$O\left(\sqrt{\frac{N}{t}}\right)$$

algorithm. In particular, for a unique solution, we get an

$$O(\sqrt{N})$$

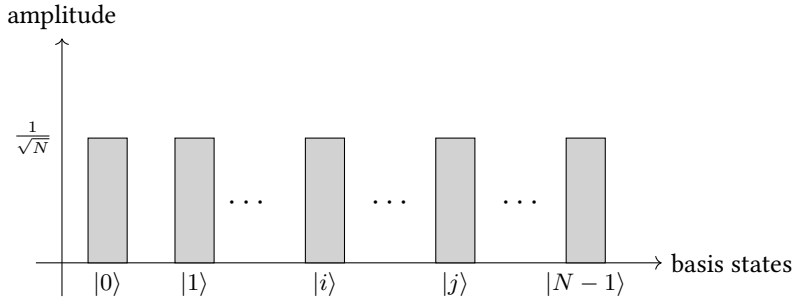
algorithm.

1.2 Amplitude evolution under the oracle and reflection

Before applying the oracle, every basis state has amplitude

$$\frac{1}{\sqrt{N}}.$$

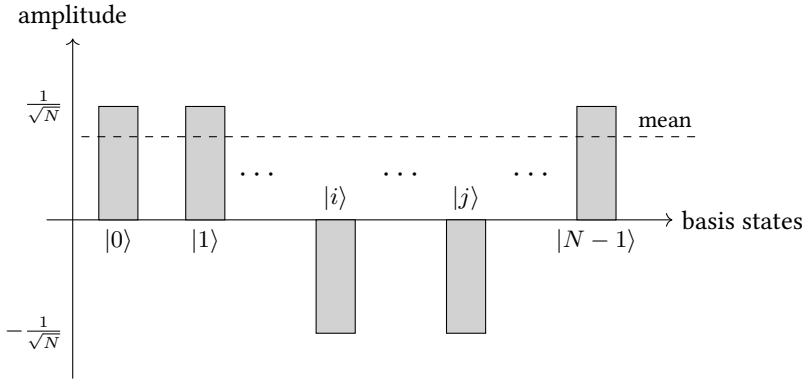
The following bar graph shows the uniform state. The special states i and j are written explicitly.



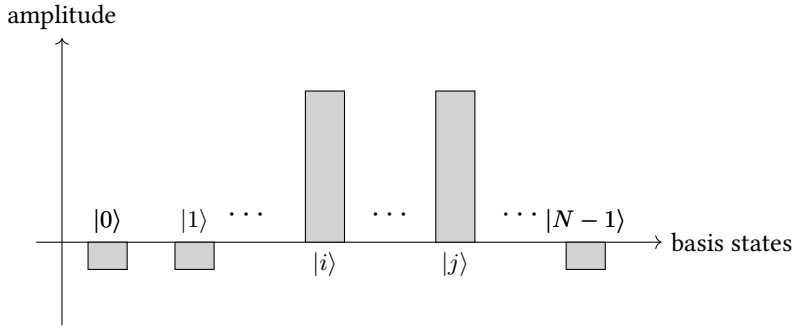
We can write the oracle as a phase oracle:

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

So the marked states now get a minus sign, while the unmarked states stay the same.
Phase flip. After applying the phase oracle, the amplitudes look like this.



The mean amplitude is positive, but it is smaller than $\frac{1}{\sqrt{N}}$, because only a few states have negative amplitude.
Now we reflect the amplitudes about the mean. After this step, the marked states get a large positive amplitude, while the unmarked states have a small negative amplitude.



So the overall picture is:

- start with a uniform superposition,
- apply the phase oracle to flip the marked amplitudes,
- reflect the amplitudes about the mean,

1.3 The OR gate and phase oracles

To implement the reflection step, we first consider an n-bit OR gate.
The OR function is defined as $f_{OR} : \{0,1\}^n \to \{0,1\}$ such that:

$$f_{OR}(x) = \begin{cases} 0 & \text{if } x = 0^n \\ 1 & \text{otherwise} \end{cases}$$

The circuit size for this gate is $O(n)$.
We assume access to a phase oracle Z_{OR} based on this function. This oracle acts on the computational basis as:

$$Z_{OR} |x\rangle = \begin{cases} |x\rangle & \text{if } x = 0^n \\ -|x\rangle & \text{otherwise} \end{cases}$$

Lemma 1. *The phase oracle Z_{OR} can be written as the operator:*

$$Z_{OR} = 2 |0^n\rangle \langle 0^n| - I$$

Proof. Consider the action of $2 |0^n\rangle \langle 0^n| - I$ on a basis state $|x\rangle$:

1. If $|x\rangle = |0^n\rangle$, then
$$(2 |0^n\rangle \langle 0^n| - I) |0^n\rangle = 2 |0^n\rangle (1) - |0^n\rangle = |0^n\rangle .$$
2. If $|x\rangle \neq |0^n\rangle$, then
$$(2 |0^n\rangle \langle 0^n| - I) |x\rangle = 2 |0^n\rangle (0) - |x\rangle = -|x\rangle .$$

This matches the definition of the Z_{OR} oracle. □

1.4 The Grover iterate

The Grover algorithm proceeds by repeatedly applying an operator G, known as the **Grover Iterate**.

Definition 1 (Grover Iterate)**.** The Grover Iterate G is defined as:

$$G = H^{\otimes n} Z_{OR} H^{\otimes n} Z_f$$

where Z_f is the phase oracle for the search problem, defined by $Z_f |x\rangle = (-1)^{f(x)} |x\rangle$.

We can simplify the first part of the iterate, $H^{\otimes n} Z_{OR} H^{\otimes n}$.
Using our previous derivation for Z_{OR}:

$$H^{\otimes n}(2 |0^n\rangle \langle 0^n| - I)H^{\otimes n}$$
$$= 2(H^{\otimes n} |0^n\rangle)(\langle 0^n| H^{\otimes n}) - H^{\otimes n} I H^{\otimes n}$$

Let $|U\rangle$ be the uniform superposition state, $|U\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$. We know that applying the Hadamard transform to the all-zero state yields this uniform superposition:

$$|U\rangle = H^{\otimes n} |0^n\rangle$$

Substituting $|U\rangle$ into the expression above, and noting that $H^{\otimes n} H^{\otimes n} = I$, we get:

$$H^{\otimes n} Z_{OR} H^{\otimes n} = 2 |U\rangle \langle U| - I$$

Thus, the Grover Iterate can be written in its most common form:

$$G = (2 |U\rangle \langle U| - I) Z_f$$

Remark 1. The operator $(2 |U\rangle \langle U| - I)$ represents a reflection about the uniform superposition state $|U\rangle$. In the context of the amplitudes, this is mathematically equivalent to the "reflection about the mean" described in the geometric intuition of the algorithm.

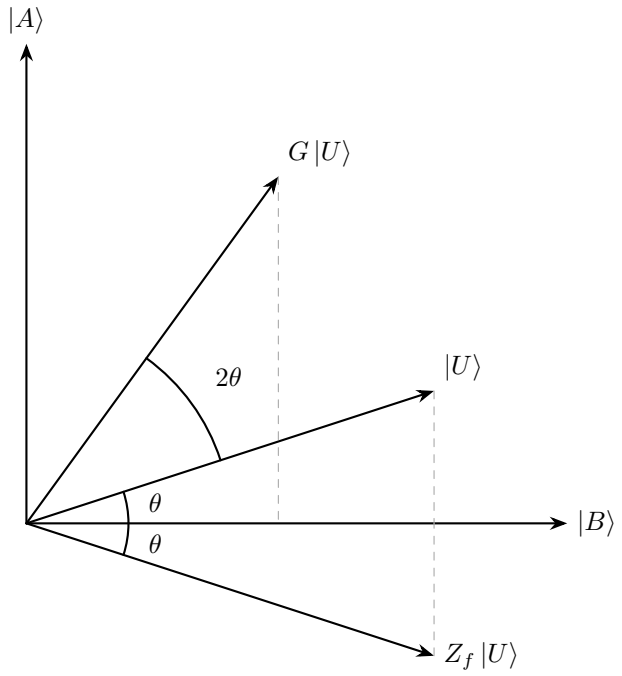
1.5 Good and bad subspace geometry

Now we compress the search space into a two-dimensional space spanned by the good and bad states.

Definition 2 (Good and bad states)**.** Define

$$|A\rangle = \frac{1}{\sqrt{t}} \sum_{x:\, f(x)=1} |x\rangle\,, \qquad |B\rangle = \frac{1}{\sqrt{N-t}} \sum_{x:\, f(x)=0} |x\rangle\,.$$

Here $|A\rangle$ represents the *good* states and $|B\rangle$ represents the *bad* states.



If we draw $|B\rangle$ on the x-axis and $|A\rangle$ on the y-axis, then $|U\rangle$ makes an angle θ with the x-axis, where

$$\theta = \sin^{-1}\sqrt{\frac{t}{N}}.$$

With this notation, the uniform superposition can be written as

$$|U\rangle = \sqrt{\frac{t}{N}}\;|A\rangle + \sqrt{\frac{N-t}{N}}\;|B\rangle\,.$$

Since $f(x) = 1$ on the good states, applying the phase oracle changes the sign of the $|A\rangle$ component:

$$Z_f\,|U\rangle = -\sqrt{\frac{t}{N}}\;|A\rangle + \sqrt{\frac{N-t}{N}}\;|B\rangle\,.$$

To understand this in the $\{|U\rangle\,, |U_\perp\rangle\}$ basis, define

$$|U_\perp\rangle = \sqrt{\frac{N-t}{N}}\;|A\rangle - \sqrt{\frac{t}{N}}\;|B\rangle\,.$$

This state is orthogonal to $|U\rangle$, since

$$\langle U|U_\perp\rangle = \sqrt{\frac{t}{N}}\sqrt{\frac{N-t}{N}} - \sqrt{\frac{N-t}{N}}\sqrt{\frac{t}{N}} = 0.$$

Now write

$$s = \sqrt{\frac{t}{N}}, \qquad c = \sqrt{\frac{N-t}{N}}.$$

Then

$$|U\rangle = s\,|A\rangle + c\,|B\rangle\,, \qquad |U_\perp\rangle = c\,|A\rangle - s\,|B\rangle\,.$$

Solving for $|A\rangle$ and $|B\rangle$,

$$|A\rangle = s\,|U\rangle + c\,|U_\perp\rangle\,, \qquad |B\rangle = c\,|U\rangle - s\,|U_\perp\rangle\,.$$

Substituting into $Z_f\,|U\rangle = -s\,|A\rangle + c\,|B\rangle$, we get

$$Z_f\,|U\rangle = -s(s\,|U\rangle + c\,|U_\perp\rangle) + c(c\,|U\rangle - s\,|U_\perp\rangle),$$

so

$$Z_f\,|U\rangle = (c^2 - s^2)\,|U\rangle - 2sc\;|U_\perp\rangle\,.$$

Therefore, if we write

$$Z_f\,|U\rangle = \alpha\,|U\rangle + \beta\,|U_\perp\rangle\,,$$

then

$$\alpha = c^2 - s^2 = \frac{N-2t}{N}, \qquad \beta = -2sc = -\frac{2\sqrt{t(N-t)}}{N}.$$

Using

$$\sin\theta = \sqrt{\frac{t}{N}}, \qquad \cos\theta = \sqrt{\frac{N-t}{N}},$$

we have

$$\alpha = \cos 2\theta, \qquad -\beta = \sin 2\theta.$$

So

$$Z_f\,|U\rangle = \cos 2\theta\;|U\rangle - \sin 2\theta\;|U_\perp\rangle\,.$$

Now apply the reflection operator $2\,|U\rangle\langle U| - I$. Since it fixes $|U\rangle$ and flips the sign of the orthogonal component, we get

$$(2\,|U\rangle\langle U| - I)Z_f\,|U\rangle = \alpha\,|U\rangle - \beta\,|U_\perp\rangle = \cos 2\theta\;|U\rangle + \sin 2\theta\;|U_\perp\rangle\,.$$

Hence

$$G\,|U\rangle = \cos 2\theta\;|U\rangle + \sin 2\theta\;|U_\perp\rangle\,.$$

Note that $G\,|U\rangle$ makes an angle of 2θ with $|U\rangle$, and hence an angle of $\theta + 2\theta = 3\theta$ with the $|B\rangle$-axis.