CS 410/510 Introduction to Quantum Computing

Lecture 9

Portland State U, Spring 2017 — *May 02, 2017*

Lecturer: Fang Song — *Scribe: Mohamed Abidalrekab*

Version: October 9, 2017

1 Basic Definitions

A group $(G, \cdot)$ is non-empty set G with a binary operation '$\cdot$' with the following proprieties:

1. closure: $g_1 \cdot g_2 \in G, \forall g_1, g_2 \in G$
2. associativity: $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3) \forall g_1, g_2, g_3 \in G$
3. identity: There exists $e \in G$ such that $\forall g \in G, g \cdot e = e \cdot g = g$
4. inverse: for all $g \in G$ there exists $g^{-1} \in G$ such that $g \cdot g^-1 = e$ and $g^{-1} \cdot g = e$.

Any group G called finite iff the number of elements in G is finite, and the order of a finite group G is the number of element in that group which denoted as $|G|$. A group G is said to be "Abelian Group" if $g_1 g_2 = g_2 g_1, \forall g_1, g_2 \in G$. The Group Z_n of integers modulo n with multiplication operation is an example of a finite Abelian group [1].

2 Hidden Subgroup Problem (HSP)

Problem Statement: Let G be a finite abelian group, and $H \subseteq G$ be a subgroup of G. We are giving a function $f : G \to S$ as an oracle which is constant on each coset of H and distinct on distinct cosets i.e.,

$$f(g) = f(g') \text{ iff there is an } h \in H \text{ such that } g = hg' .$$

The goal is to find H. The hidden subgroup problems include order-finding, period-finding, logarithms, and many other problems can be solved using a number of operations polynomial in $log|G|$ [1].

Examples

- The Symmetric group on N elements, or S_N is the group who's underlying set is the set of all bijections from $[N] = 0, 1, 2, ...N - 1$ to itself. so each set has its own inverse and identity transformation belongs to the same set.
- The Dihedral group D_N is the group who's underlying set ig the set of symmetries of an N-sided regular polygon where a group of operation should be composed of symmetrical sub operations.

Examples of HSP problems:

Table 1: Hidden Group problem

Problem	the Group	type of the Group
Simon's	Z_2^n	Abelian
Factoring/Period Finding	Z_N	Abelian
Discrete Log	$Z_N \times Z_N$	Abelian
Pell's Equation/Princp. Ideal Problem	R	Abelian
Graph Isomorphism	S_n(Symmetric Group)	Non-Abelian
Shortest Vector Problem	D_N (Dihedral Group)	Non-Abelian

- The underlying group G associated with the problem is Abelian, in which case we can solve the problem with $poly(\log |G|)$ number of gates and calls to the provided oracle O_f. This is the case with the first four of the problems listed in the table above. [1].
- The underlying group G associated with the problem is non-Abelian, in which case we can have an algorithm that has $poly(\log |G|)$ calls to the oracle function O_f, but it may need and exponential number of gates to run successfully.

3 Grover Search Algorithm

Unstructured Grover's algorithm is a quantum algorithm to find a special element within a search space "database" in number of attempts $O(\sqrt{N})$ comparing to classical algorithms which can do it at least $\Omega(N)$ where N is the number of elements in that database. The search is called unstructured because there is no guarantee of how the database is sorted.

3.1 Problem Definition:

- Given oracle function: $f : \{0,1\}^n \rightarrow \{0,1\}$. Assume that there is a unique x^* such that $f(x^*) = 1$.
- Output: x^*.

To mark the special element classically, we need to try $\Omega(2^n)$ attempt, while randomly it takes 2^{n-1}. using Quantum algorithm it can be achieved using only $\Theta(\sqrt{2^n})$ queries.

3.2 Algorithm's procedure:

schematically, the search algorithm operation is shown in figure (2), the algorithm uses a single n qubit register. The Hadamard transform is used to put the input into superposition state.

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

Then the quantum algorithm consists of repeated subroutines known as "Grover's operator" whose circuit is shown in figure 1. The algorithm itself can be broken into four steps:

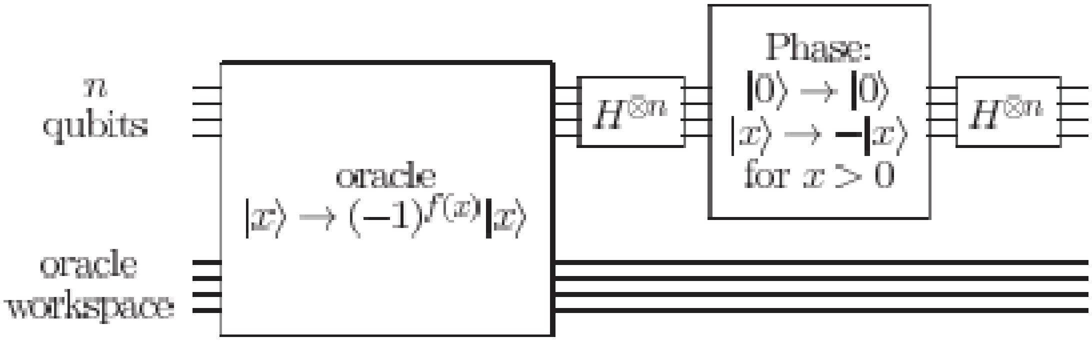

n
qubits
oracle
workspace
oracle
$|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$
$H^{\otimes n}$
Phase:
$|0\rangle \rightarrow |0\rangle$
$|x\rangle \rightarrow -|x\rangle$
for $x > 0$
$H^{\otimes n}$

Figure 1: The Circuit of Grover's algorithm

1. Apply the Oracle
$$Z_f\,|x\rangle = (-1)^{f(x)}\,|x\rangle \tag{2}$$
2. Apply the Hadamard transform $H^{\otimes\,n}$
3. Perform conditional phase shift for all computational basis state except $|0\rangle$ getting a phase shift -1.
$$Z_0\,|x\rangle = \begin{cases} -\,|x\rangle\,, & x = 0^n \\ |x\rangle\,, & otherwise \end{cases} \tag{3}$$
4. Apply the Hadamard transform $H^{\otimes\,n}$

$$G = H^{\otimes\,n} Z_o H^{\otimes\,n} Z_f = (-H^{\otimes\,n} 1 H^{\otimes\,n} + 2H^{\otimes\,n}\,|0\rangle\,\langle 0|\,H^{\otimes\,n})Z_f \tag{4}$$

we know that $-H^{\otimes\,n}1H^{\otimes\,n} + 2H^{\otimes\,n}\,|0\rangle\,\langle 0|\,H^{\otimes\,n} = 2\,|\psi\rangle\,\langle\psi| - I$ so that G "Grover's operator" can be rewritten as:

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

Repeating these steps many times and then measure increases the chance to get the right element. The overall Quantum operator applied by Grover's algorithm is shown in figure 2.

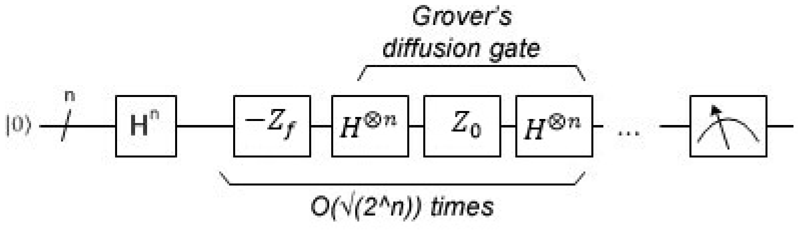


Figure 2: Grover's operations blocks

Theorem : The operation $2 |\psi\rangle \langle\psi| - I$ applied to a general state $\sum_k \alpha_k |k\rangle$ produces,

$$\sum_k [-\alpha_k + 2\langle\alpha\rangle] |k\rangle \tag{5}$$

where $\langle\alpha\rangle \equiv \sum_k \alpha_k / N$ is the mean value of α_k. that's why operator $2 |\psi\rangle \langle\psi| - I$ is called inversion about the mean operation.

4 Grover's Algorithm analysis

4.1 Geometric visualization

in this section i will closely follow Nielsen and Chuang's book to describe the geometrical meaning of Grover's algorithm. if we have a two dimensional space spanned by the starting vector $|\psi\rangle$ and a uniform superposition state of solution of the search problem, the Grover's operator can be regraded as a (rotation). To put this into formulation, let us have two normalized states:

$$|A\rangle \equiv \frac{1}{\sqrt{M}} \sum_x^M |x\rangle \tag{6}$$

$$|B\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x^{N-M} |x\rangle \tag{7}$$

where $\sum_x^M$ represents a sum over all x solution of search problem, while $\sum_x^{N-M}$ indicate all non-solution to the search problem. Thus the initial state of the algorithm $|\psi\rangle$ can be re-expressed as,

$$|\psi\rangle = \sqrt{\frac{M}{N}} |A\rangle + \sqrt{\frac{N-M}{N}} |B\rangle \tag{8}$$

That means the initial of our algorithm exits in a space spanned by two vector basis $|A\rangle$ and $|B\rangle$ as in figure 3.
by looking to figure 3, it turns out that G consists of two operation. first operation is the Oracle operation Z_f performs a reflection about $|B\rangle$ in the space spanned by $|A\rangle$ and $|B\rangle$, so that $Z_f(\aleph |A\rangle + \beta |B\rangle) = -a |A\rangle + b |B\rangle$. The second, $2 |\psi\rangle \langle\psi| - I$ also perform a reflection about $|\psi\rangle$, so that the outcome of product of both reflections is a rotation.
This means that $G^k |\psi\rangle$ remains in the same space spanned by basis for all k's where k is the number of iterations. let us assume that $cos(\theta) = \sqrt{\frac{N-M}{N}}$, and

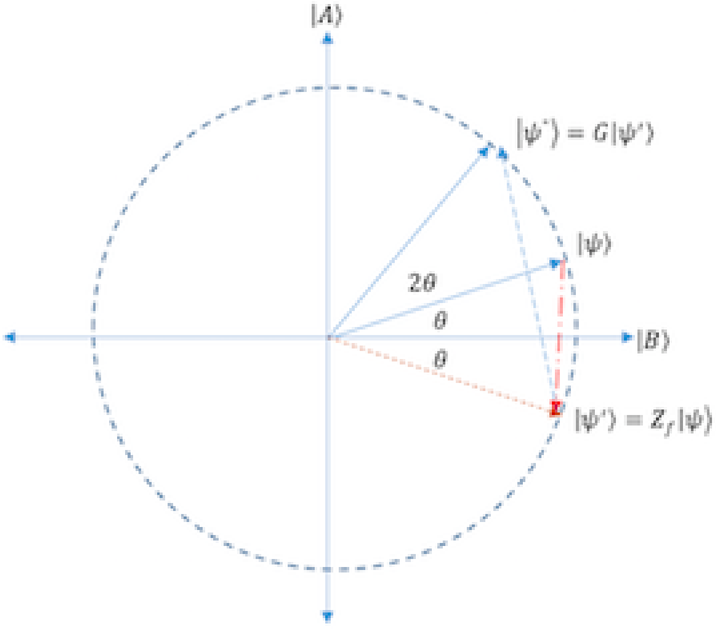
$$|\psi\rangle = sin(\theta) |A\rangle + cos(\theta) |B\rangle \tag{9}$$

As in figure 3, applying operator G on the state has the total effect of a rotation by 2θ

$$|\psi\rangle = sin(2\theta) |A\rangle + cos(2\theta) |B\rangle \tag{10}$$

Applying G on $|\psi\rangle$ for k times takes the state to:

$$G^k |\psi\rangle = sin((2k+1)\theta) |A\rangle + cos((2k+1)\theta) |B\rangle \tag{11}$$



$|A\rangle$
$|\psi^{''}\rangle = G|\psi'\rangle$
$|\psi\rangle$
2θ
θ
$|B\rangle$
θ
$|\psi'\rangle = Z_f|\psi\rangle$

Figure 3: The actions of single iteration of Grover's Algorithm

4.2 How many iteration is needed?

To get $|\psi\rangle$ as close as possible to $|A\rangle$ starting from the initial state $|\psi\rangle = sin(\theta)\,|A\rangle + cos(\theta)\,|B\rangle$, we rotate through $arcos(\sqrt{\frac{M}{N}})$ radius. so, then the Grover's algorithm iteration can be.

$$R = CI(\frac{arcos(\sqrt{\frac{M}{N}})}{2\theta}) \tag{12}$$

times rotates $|\psi\rangle$ to within angle $\theta \leq \pi/2$ where "CI" means rounding to nearest integer. Note that when $M \ll N$ we have $\theta \simeq sin(\theta) \simeq (\sqrt{\frac{M}{N}})$, given probability of error at most $\frac{M}{N}$
Note: the number of iteration depends on M (the number of solution) but not the identity of these solutions. from 12 note that $R \leq \frac{pi}{4\theta}$ so, the upper bound of R is decided by the lower bound on θ[1].Assuming that $M \leq N/2$ [1],

$$\theta \geq sin(\theta) = \sqrt{\frac{M}{N}} \tag{13}$$

from 12, 13, yield

$$R \leq \frac{\pi}{4}\sqrt{\frac{N}{M}} \tag{14}$$

So, Grover's algorithm call the oracle R times in order to obtain the solution to the search problem with high probability.

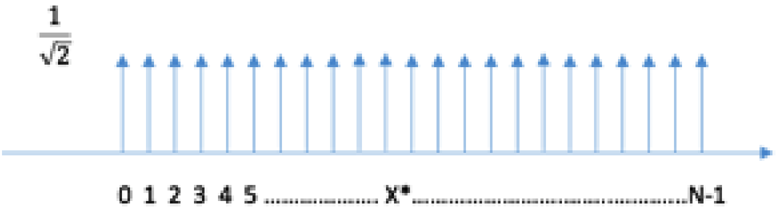
5 Different Approach to Grover's Algorithm

5.1 Amplitude Amplification

Remember that our search problem is given an ability to query an Oracle $O\left|x\right\rangle\left|q\right\rangle = \left|x\right\rangle\left|q \otimes f(x)\right\rangle$ obtain a special element (or elements) such that $f(x^*) = 1$ stored in a database. the output will be x^* procedure of implementing Grover's as follows:

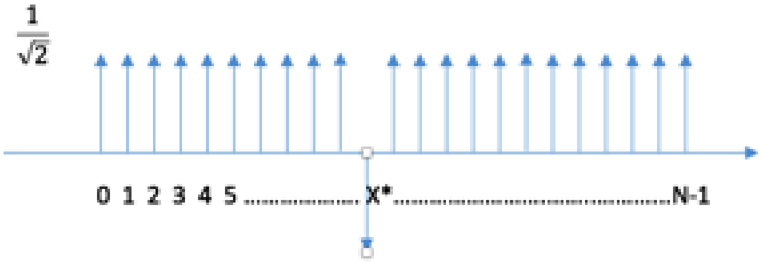
1. initiate state $\left|0\right\rangle^{\otimes n}\left|0\right\rangle$
2. apply $H^{\otimes n}$ to the first n qubit and HX to the next qubit.

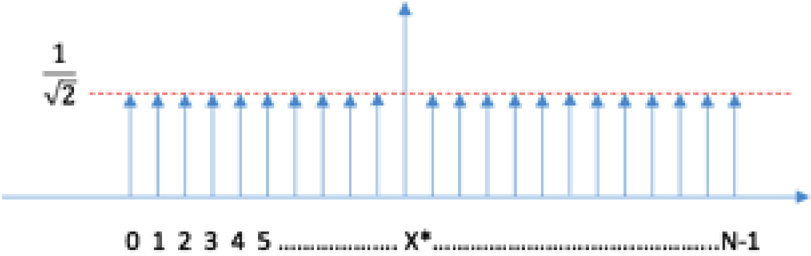
$$\longmapsto \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}\left[\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}\right]$$



3. apply the oracle followed by $2\left|\psi\right\rangle\left\langle\psi\right| - I$ the overall operation yeild:

$$\longmapsto [(2\left|\psi\right\rangle\left\langle\psi\right| - I)Z_f]^{\otimes R}\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}\left|x\right\rangle\left[\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}\right] \simeq \left|x*\right\rangle\left[\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}\right] \tag{15}$$





4. measure x*

6 Worked Example

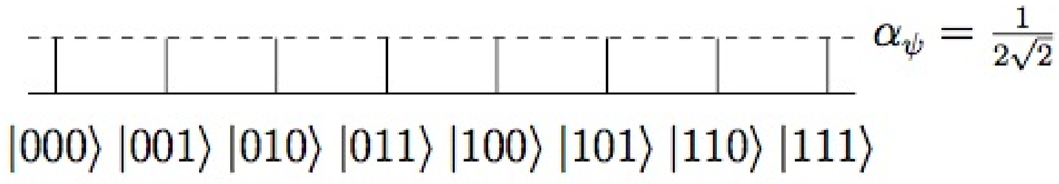
[Note: this example is adapted from reference [2] as is] consider a system of 2^3 states, and we are looking for a special binary state $x_0 = 011$. therefore, to represent this system, we need $n = 3$ qubits . The overall state can be written as:

$$|x\rangle = \alpha_0 |000\rangle + \alpha_1 |001\rangle + \alpha_2 |010\rangle + \alpha_3 |011\rangle + \alpha_4 |100\rangle + \alpha_5 |101\rangle + \alpha_6 |110\rangle + \alpha_7 |111\rangle \tag{16}$$

where α_i are the amplitude probability of a state $|x_i\rangle$, and Grover algorithm is initialized in state $1\,|000\rangle$. Next step is to apply Hadamard transformation to obtain a state in the form of eq. 16.

$$H^{\otimes 3} |000\rangle = \frac{1}{2\sqrt{2}} |000\rangle + \frac{1}{2\sqrt{2}} |001\rangle + ... + \frac{1}{2\sqrt{2}} |111\rangle = \frac{1}{2\sqrt{2}} \sum_{x=0}^{7} |x\rangle = |\psi\rangle \tag{17}$$

to have a complete picture of the state, it is better to switch to geometric interpretations of probability amplitudes of each component. These components stay real throughout Grover's algorithm, so they can be represented as lines perpendicular to the axis! as shown in the earlier examples.



Now, it is reasonable to make 2 iteration of Grover's in order to obtain the solution which is inferred from $\frac{\pi\sqrt{8}}{4} \approx 2.22$ then it is rounded to nearest integer [**?**].
In the first iteration:
we call the oracle, then perform inversion about the average which is also called "Diffusion transform"

$$|x\rangle = \frac{1}{2\sqrt{2}} |000\rangle + \frac{1}{2\sqrt{2}} |001\rangle + \frac{1}{2\sqrt{2}} |010\rangle - \frac{1}{2\sqrt{2}} |011\rangle .... + \frac{1}{2\sqrt{2}} |111\rangle \tag{18}$$

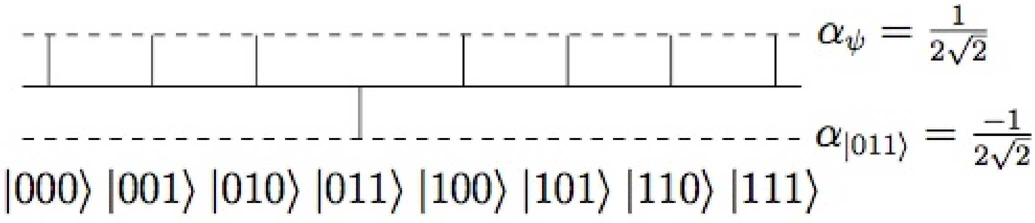
Notice that the state $|x_0\rangle = |011\rangle$ is flipped in sign after applying the Oracle. in the next figure, the geometric interpretation of what the oracle did.
Now, we are going to apply the Diffusion operator! $2 |\psi\rangle \langle\psi| - I$ which increases the amplitude by their difference from the average, or decreases it if the difference is negative.

$$[2 |\psi\rangle \langle\psi| - I] |x\rangle \ = [2 |\psi\rangle \langle\psi| - I][|\psi\rangle - \frac{2}{2\sqrt{2}} |011\rangle] \tag{19}$$

$$= 2 |\psi\rangle \langle\psi|\psi\rangle - |\psi\rangle - \frac{2}{\sqrt{2}} |\psi\rangle \langle\psi|011\rangle + \frac{1}{\sqrt{2}} |011\rangle \tag{20}$$

where $\langle\psi|\psi\rangle = 1$, and since $|011\rangle$ is one of the state basis vector, yield $\langle\psi|011\rangle = \frac{1}{2\sqrt{2}}$

$$2 |\psi\rangle - |\psi\rangle - \frac{2}{\sqrt{2}} (\frac{1}{2\sqrt{2}}) |\psi\rangle + \frac{1}{\sqrt{2}} |011\rangle \tag{21}$$


$\alpha_\psi = \frac{1}{2\sqrt{2}}$
$\alpha_{|011\rangle} = \frac{-1}{2\sqrt{2}}$
$|000\rangle$ $|001\rangle$ $|010\rangle$ $|011\rangle$ $|100\rangle$ $|101\rangle$ $|110\rangle$ $|111\rangle$

$$\frac{1}{2}\,|\psi\rangle + \frac{1}{\sqrt{2}}\,|011\rangle \tag{22}$$

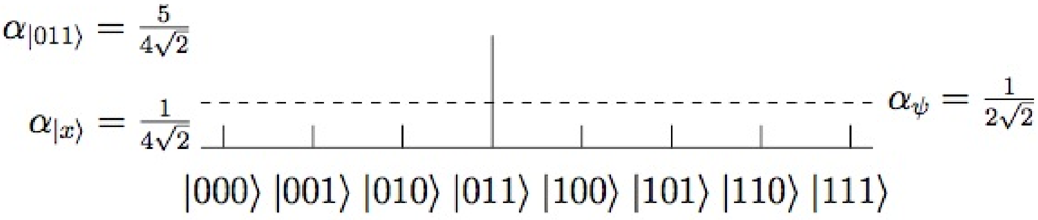
Substituting from equation 16,

$$= \frac{1}{2}[\frac{1}{2\sqrt{2}}\sum_{\substack{x=0\\x\neq 3}}^{7}|x\rangle] + \frac{1}{\sqrt{2}}\,|011\rangle \tag{23}$$

$$= \frac{1}{4\sqrt{2}}\sum_{\substack{x=0\\x\neq 3}}^{7}|x\rangle + \frac{1}{4\sqrt{2}}\,|011\rangle + \frac{1}{\sqrt{2}}\,|011\rangle \tag{24}$$

$$= \frac{1}{4\sqrt{2}}\sum_{\substack{x=0\\x\neq 3}}^{7}|x\rangle + \frac{5}{4\sqrt{2}}\,|011\rangle \tag{25}$$

Our final geometrical form of the state is,


$\alpha_{|011\rangle} = \frac{5}{4\sqrt{2}}$
$\alpha_{|x\rangle} = \frac{1}{4\sqrt{2}}$
$\alpha_\psi = \frac{1}{2\sqrt{2}}$
$|000\rangle$ $|001\rangle$ $|010\rangle$ $|011\rangle$ $|100\rangle$ $|101\rangle$ $|110\rangle$ $|111\rangle$

This the shape of a state by the end of first iteration of Grover's algorithm. Now, we are going to see how the state evolves after the second iteration.
Starting with,

$$|x\rangle = \frac{1}{4\sqrt{2}}\,|000\rangle + \frac{1}{4\sqrt{2}}\,|001\rangle + \frac{1}{4\sqrt{2}}\,|010\rangle + \frac{5}{4\sqrt{2}}\,|011\rangle + \frac{1}{4\sqrt{2}}\,|100\rangle + ... + \frac{1}{4\sqrt{2}}\,|111\rangle$$

We apply the same transformation as the first iteration, yield.

$$|x\rangle = \frac{1}{4\sqrt{2}}\,|000\rangle + \frac{1}{4\sqrt{2}}\,|001\rangle + \frac{1}{4\sqrt{2}}\,|010\rangle - \frac{5}{4\sqrt{2}}\,|011\rangle + \frac{1}{4\sqrt{2}}\,|100\rangle + ... + \frac{1}{4\sqrt{2}}\,|111\rangle \tag{26}$$

which equal to,

$$= \frac{1}{4\sqrt{2}} \sum_{\substack{x=0 \\ x\neq 3}}^{7} |x\rangle] - \frac{5}{4\sqrt{2}} |011\rangle \tag{27}$$

$$= \frac{1}{4\sqrt{2}} \sum_{\substack{x=0 \\ x\neq 3}}^{7} |x\rangle + \frac{5}{4\sqrt{2}} |011\rangle + \frac{1}{\sqrt{2}} |011\rangle \tag{28}$$

$$= \frac{1}{4\sqrt{2}} \sum_{x=0}^{7} |x\rangle - \frac{6}{4\sqrt{2}} |011\rangle = \frac{1}{2} |\psi\rangle - \frac{3}{2\sqrt{2}} |011\rangle \tag{29}$$

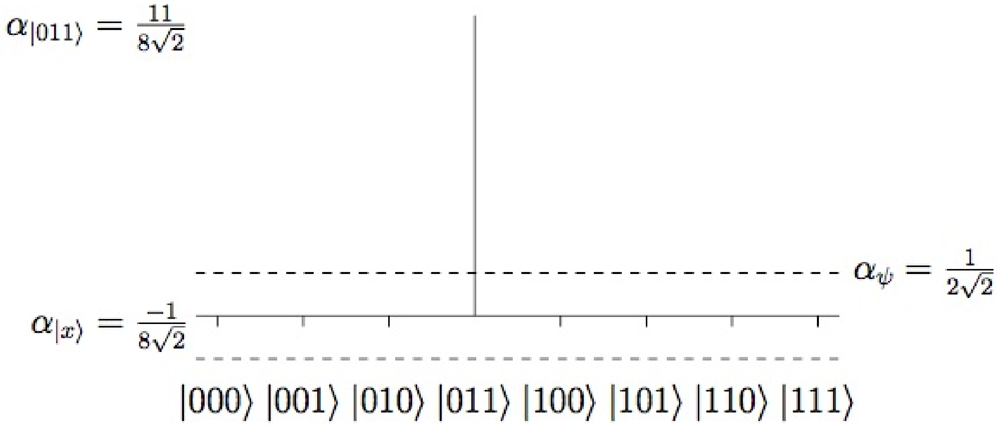


Figure 4: the Final geometrical interpretation of state x

Next step will be Querying the oracle and applying Diffusion operator,

$$[2 |\psi\rangle \langle\psi| - I][\frac{1}{2} |\psi\rangle - \frac{3}{2\sqrt{2}} |011\rangle]$$

$$[2(\frac{1}{2}) |\psi\rangle \langle\psi|\psi\rangle - \frac{1}{2}] |\psi\rangle - 2(\frac{3}{2\sqrt{2}}) |\psi\rangle \langle\psi|011\rangle + \frac{3}{2\sqrt{2}} |011\rangle \tag{30}$$

$$= \frac{-1}{4} |\psi\rangle + \frac{3}{2\sqrt{2}} |011\rangle$$

we can rewrite it as:

$$\frac{-1}{4} \left(\frac{1}{2\sqrt{2}} \sum_{\substack{x=0 \\ x\neq 3}}^{7} |x\rangle + \frac{1}{2\sqrt{2}} |011\rangle \right) + \frac{3}{2\sqrt{2}} |011\rangle \tag{31}$$

$$= \frac{-1}{8\sqrt{2}} \sum_{\substack{x=0 \\ x\neq 3}}^{7} |x\rangle + \frac{11}{8\sqrt{2}} |011\rangle \tag{32}$$

if we expanded it,

$$|x\rangle = \frac{-1}{8\sqrt{2}}|000\rangle + \frac{-1}{8\sqrt{2}}|001\rangle + \frac{-1}{8\sqrt{2}}|010\rangle + \frac{11}{8\sqrt{2}}|011\rangle + \frac{-1}{8\sqrt{2}}|100\rangle + ... + \frac{-1}{8\sqrt{2}}|111\rangle \tag{33}$$

Graphically, we represent that as the above figure (4) [2]. Now, when the measurement is conducted, the probability that the state $|011\rangle$ is selected is $\frac{11}{8\sqrt{2}}$ squared which is equaled to 94.5.

References

[1] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition, 2011.

[2] Emma Strubell. An introduction to quantum algorithms. *COS498 Chawathe Spring*, 2011.