Algorithms Discussion group

An Introduction To Quantum Algorithms

By Jyoti Aneja

07/27/2016

Outline

- What are quantum algorithms?
- Examples
- Some background building (quantum registers and logic gates)
- Grover's Algorithm
- Example of Grover's algorithm
- Conclusion

What are quantum algorithms?

International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

1. INTRODUCTION

On the program it says this is a keynote speech—and I don't know what a keynote speech is. I do not intend in any way to suggest what should be in this meeting as a keynote of the subjects or anything like that. I have my own things to say and to talk about and there's no implication that anybody needs to talk about the same thing or anything like it. So what I want to talk about is what Mike Dertouzos suggested that nobody would talk about. I want to talk about the problem of simulating physics with computers and I mean that in a specific way which I am going to explain. The reason for doing this is something that I learned about from Ed Fredkin, and my entire interest in the subject has been inspired by him. It has to do with learning something about the possibilities of computers, and

- Richard Feynman pointed out that accurately and efficiently simulating quantum mechanical systems would be impossible on a classical computer, but that a new kind of machine, a computer itself built of quantum mechanical elements which obey quantum mechanical laws, might one day perform efficient simulations of quantum systems.

- Classical computers are inherently unable to simulate such a system using sub-exponential time and space complexity due to the exponential growth of the amount of data required to completely represent a quantum system.

- To simulate quantum systems we need efficient quantum algorithms.

- Quantum algorithms can also give huge speed up in solving classical problems of search etc.

Examples

- There have been many algorithms that have been developed for quantum computers.

<u>Few examples</u>

- Deutsch–Jozsa algorithm
- Simon's algorithm
- Quantum phase estimation algorithm
- Grover’s Algorithm
- Shorts algorithm
- Hidden subgroup problem
- Boson sampling problem

<u>Today We’ll talk about</u>

- Grover’s Algortihm

Background Building

- A quantum bit or “qubit” is just a complex superposition of classical bits.

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle|$$

- We will be talking in terms of computational basis i.e

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- Quantum registers are bit strings whose length determines the amount of information they can store. The state space of a size-n quantum register is :

$$|\psi_n\rangle = \sum_{i=0}^{2^n-1} a_i |i\rangle$$

- Eg for n =3, a quatum register is

$$\||\psi_2\rangle = a_0 |000\rangle + a_1 |001\rangle + a_2 |010\rangle + a_3 |011\rangle + a_4 |100\rangle + a_5 |101\rangle + a_6 |110\rangle + a_7 |111\rangle$$

Background Building

- Quantum Logic Gates : These are basically operators that evolve the states.
- One important example is the single-qubit Hadamard operator (Fair coin flip operator)

$$
-\boxed{H}- = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \langle 0| + \frac{|0\rangle - |1\rangle}{\sqrt{2}} \langle 1|
$$

$$
H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \langle 0|0\rangle + \frac{|0\rangle - |1\rangle}{\sqrt{2}} \langle 1|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}
$$

$$
H|1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \langle 0|1\rangle + \frac{|0\rangle - |1\rangle}{\sqrt{2}} \langle 1|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}
$$

- The probability distributions of the two results are exactly the same, the two states differing only by the phase of |1>.
- Notice what H does to a |0> state. We'll use this later.

Grover's Algorithm

- It was developed by an Indian mathematician Lov Grover in 1996.
- Grover's algorithm deals with searching a unique element in an unordered list.
- Classically this takes O(N) time.
- On a quantum computer, Grover's algorithm does this search in $O(\sqrt{N})$ operations.

THE ALGORITHM

Grover's ONE Iteration step

1. Initializing the state to all zeros.
2. Converting it to a uniform superposition
3. Applying the quantum ORACLE operator
4. Amplitude amplification

One Iteration

1. Begin with n qubits all initialized to 0.

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

2. Apply the n dimensional Hadamard operator which converts this into a uniform superposition of all possible 2^n states, with amplitude of each being $1/\sqrt{2^n}$

$$|\psi\rangle = H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

Recall that we're looking for a unique element. We don't necessarily know that element but can map it to a function such that f(x) = 1 for the unique element and f(x) = 0 otherwise.

1. Now the apply the Oracle operator.
2. Oracle is basically a black-box function, and this quantum oracle is a quantum black-box, meaning it can observe and modify the system without collapsing it to a classical state.

$$|x\rangle \xrightarrow{\mathcal{O}} (-1)^{f(x)} |x\rangle$$

One Iteration cont.

Amplitude amplification involved 2 steps.

1. Conditional phase shift of all elements except |0> . This is done by applying $2|0\rangle\langle 0| - I$
2. Another application of Hadamard gate. $H^{\otimes n}[2|0\rangle\langle 0| - I]H^{\otimes n}$

This would give $2|\psi\rangle\langle\psi| - I$

One Iteration cont.

Amplitude amplification involved 2 steps.

1. Conditional phase shift of all elements except |0> . This is done by applying $2|0\rangle\langle 0| - I$
2. Another application of Hadamard gate. $H^{\otimes n}[2|0\rangle\langle 0| - I]H^{\otimes n}$

This would give $2|\psi\rangle\langle\psi| - I$

To Summarize

1. $\|0\rangle^{\otimes n}$	initial state
2. $H^{\otimes n}\|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}\|x\rangle = \|\psi\rangle$	apply the Hadamard transform to all qubits
3. $[(2\|\psi\rangle\langle\psi\| - I)\mathcal{O}]^R\|\psi\rangle \approx \|x_0\rangle$	apply the Grover iteration $R \approx \frac{\pi}{4}\sqrt{2^n}$ times
4. x_0	measure the register

Small Example

Consider a system of 3 qubits and we're searching for the string 011. i.e. $x_0 = |011>$

Grovers algorithm begins by applying Hadamard operator to |000>

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

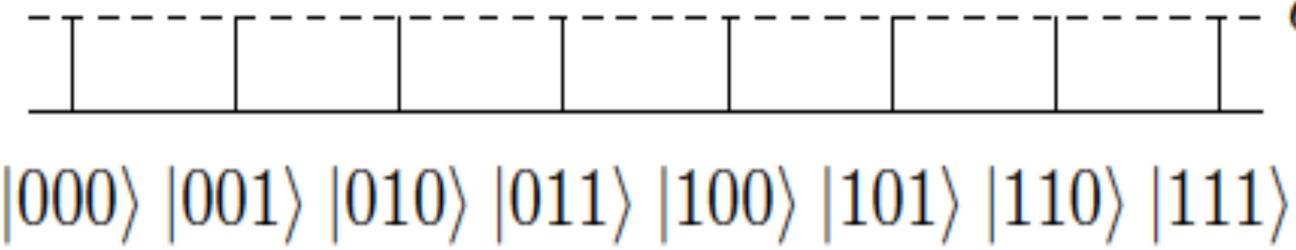
Small Example

Consider a system of 3 qubits and we're searching for the string 011. i.e. $x_0 = |011>$

Grovers algorithm begins by applying Hadamard operator to |000>

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

Geometrically the equal superposition of states resulting from the first Hadamard transform look like



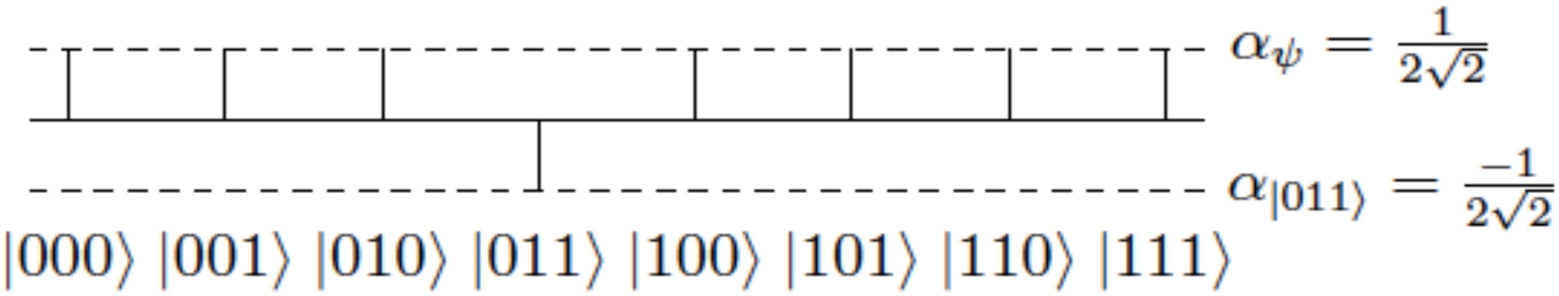
$$\alpha_\psi = \frac{1}{2\sqrt{2}}$$

When Oracle is called

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

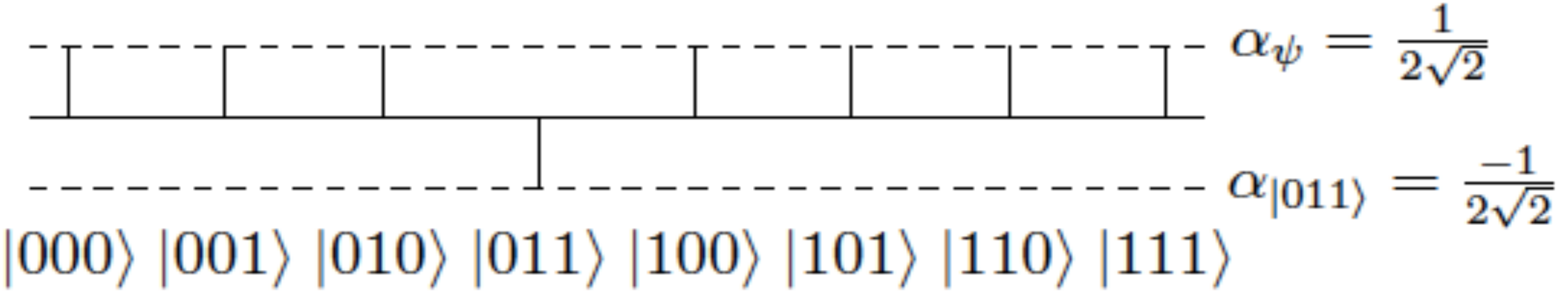
When Oracle is called

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



When Oracle is called

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

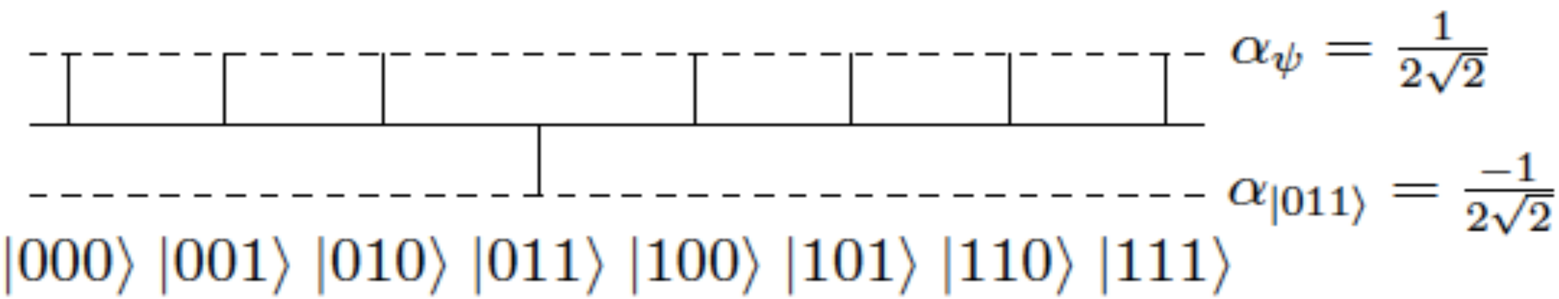


When amplitude amplification is applied

$$[2|\psi\rangle\langle\psi| - I]|x\rangle$$

When Oracle is called

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



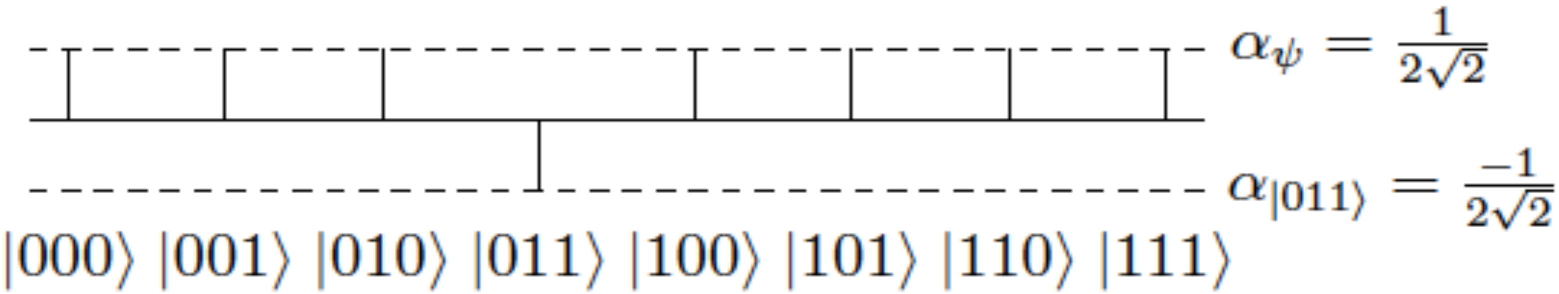
When amplitude amplification is applied

$$[2|\psi\rangle\langle\psi| - I]\,|x\rangle$$

$$\models [2|\psi\rangle\langle\psi| - I]\left[|\psi\rangle - \frac{2}{2\sqrt{2}}|011\rangle\right]$$

When Oracle is called

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



When amplitude amplification is applied

$$[2|\psi\rangle\langle\psi| - I]|x\rangle$$

$$= [2|\psi\rangle\langle\psi| - I]\left[|\psi\rangle - \frac{2}{2\sqrt{2}}|011\rangle\right]$$

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

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

In terms of the equal superposition state

$$=\frac{1}{2}\left[\frac{1}{2\sqrt{2}}\sum_{x=0}^{7}|x\rangle\right]+\frac{1}{\sqrt{2}}|011\rangle$$

In terms of the equal superposition state

$$=\frac{1}{2}\left[\frac{1}{2\sqrt{2}}\sum_{x=0}^{7}|x\rangle\right]+\frac{1}{\sqrt{2}}|011\rangle$$

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

In terms of the equal superposition state

$$= \frac{1}{2}\left[\frac{1}{2\sqrt{2}}\sum_{x=0}^{7}|x\rangle\right] + \frac{1}{\sqrt{2}}|011\rangle$$

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

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

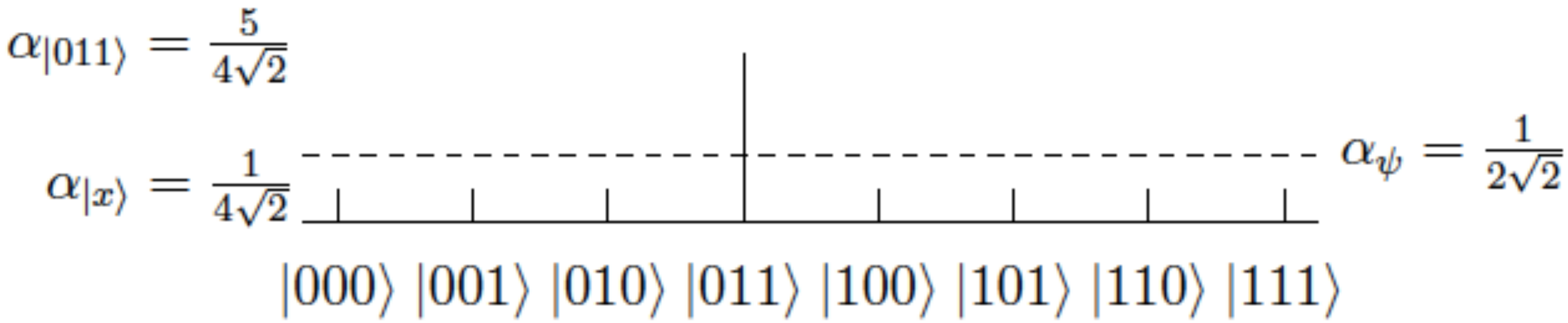
In terms of the equal superposition state

$$= \frac{1}{2}\left[\frac{1}{2\sqrt{2}}\sum_{x=0}^{7}|x\rangle\right] + \frac{1}{\sqrt{2}}|011\rangle$$

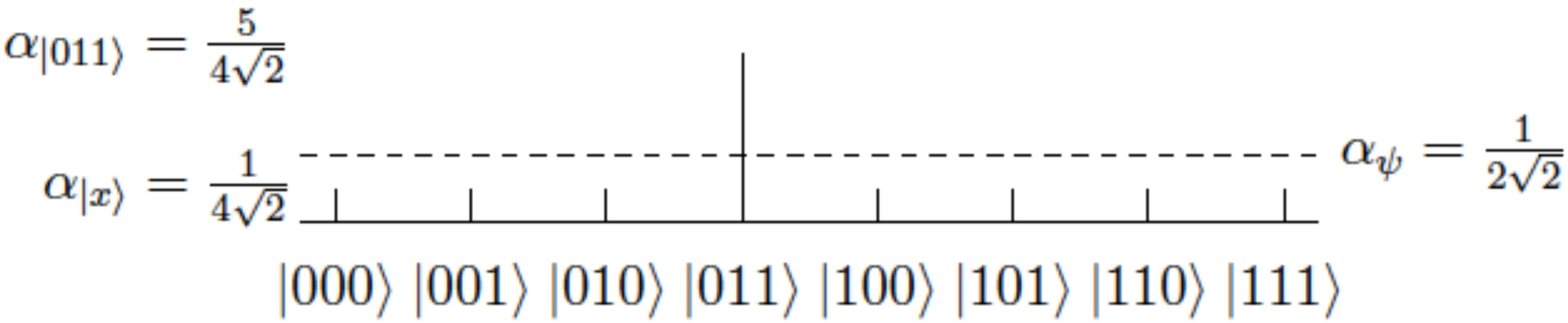
$$= \frac{1}{4\sqrt{2}}\sum_{\substack{x=0\\x\neq 3}}^{7}|x\rangle + \frac{1}{4\sqrt{2}}|011\rangle + \frac{1}{\sqrt{2}}|011\rangle$$

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

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



First iteration done!



First iteration done!

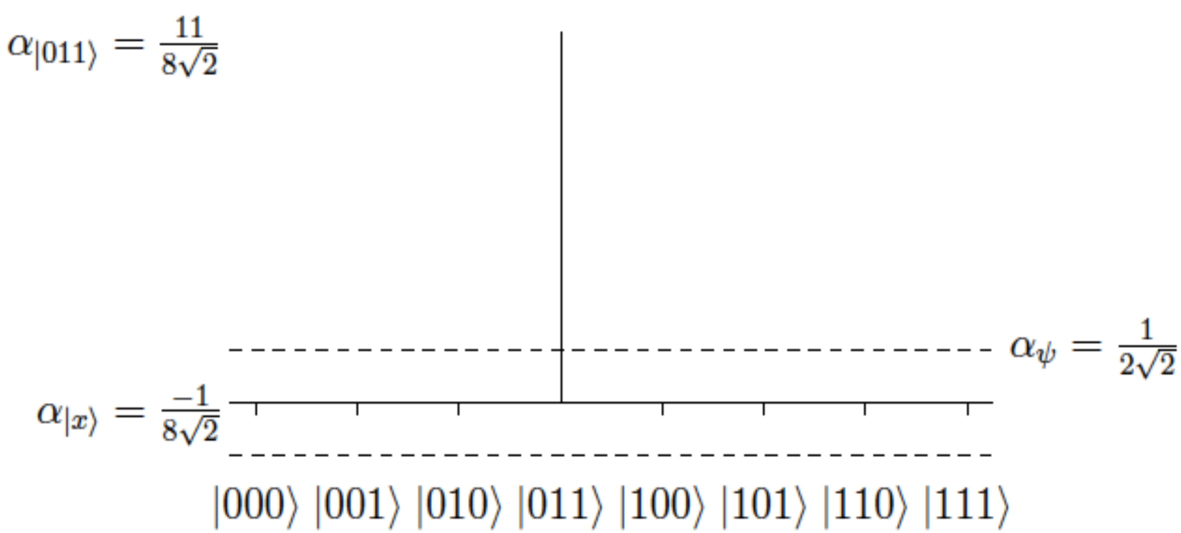
Now if we apply another iteration

$$
\begin{aligned}
|x\rangle &= \frac{1}{4\sqrt{2}}|000\rangle + \frac{1}{4\sqrt{2}}|001\rangle + \frac{1}{4\sqrt{2}}|010\rangle - \frac{5}{4\sqrt{2}}|011\rangle + \ldots + \frac{1}{4\sqrt{2}}|111\rangle \\
&= \frac{1}{4\sqrt{2}}\sum_{\substack{x=0 \\ x\neq 3}}^{7}|x\rangle - \frac{5}{4\sqrt{2}}|011\rangle \\
&= \frac{1}{4\sqrt{2}}\sum_{x=0}^{7}|x\rangle - \frac{6}{4\sqrt{2}}|011\rangle \\
&= \frac{1}{2}|\psi\rangle - \frac{3}{2\sqrt{2}}|011\rangle
\end{aligned}
$$

After some simple math

$$
\begin{aligned}
&[2|\psi\rangle\langle\psi| - I]\left[\frac{1}{2}|\psi\rangle - \frac{3}{2\sqrt{2}}|011\rangle\right] \\
&= 2\left(\frac{1}{2}\right)|\psi\rangle\langle\psi|\psi\rangle - \frac{1}{2}|\psi\rangle - 2\left(\frac{3}{2\sqrt{2}}\right)|\psi\rangle\langle\psi|011\rangle + \frac{3}{2\sqrt{2}}|011\rangle \\
&= |\psi\rangle - \frac{1}{2}|\psi\rangle - \frac{3}{\sqrt{2}}\left(\frac{1}{2\sqrt{2}}\right)|\psi\rangle + \frac{3}{2\sqrt{2}}|011\rangle \\
&= -\frac{1}{4}|\psi\rangle + \frac{3}{2\sqrt{2}}|011\rangle \\
&= -\frac{1}{4}\left[\frac{1}{2\sqrt{2}}\sum_{\substack{x=0\\x\neq 3}}^{7}|x\rangle + \frac{1}{2\sqrt{2}}|011\rangle\right] + \frac{3}{2\sqrt{2}}|011\rangle \\
&= -\frac{1}{8\sqrt{2}}\sum_{\substack{x=0\\x\neq 3}}^{7}|x\rangle + \frac{11}{8\sqrt{2}}|011\rangle
\end{aligned}
$$

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



Now when we measure

Now when the system is observed, the probability that the state representative of the correct solution, |011>, will be measured is 94:5%. The probability of finding an incorrect state is 5.5%; Grover's algorithm is more than 17 times more likely to give the correct answer than an incorrect one with an input size of N = 8, and the error only decreases as the input size increases.

Although Grover’s algorithm is probabilistic, the error truly becomes negligible as N grows large.

Thanks!

- Referrences :
https://people.cs.umass.edu/~strubell/doc/quantum_tutorial.pdf
- https://www.cs.cmu.edu/~odonnell/quantum15/lecture04.pdf
- https://en.wikipedia.org/wiki/Grover%27s_algorithm