ERATO セミナ 2010 - No. 09

Grover Search and its Applications

Byung-Soo Choi
梨花女子大学 研究教授

2010/8/3

Grover Search and its Applications

Byung-Soo Choi

bschoi3@gmail.com

Contents

Unit of Information

$|0\rangle$ Basis, logical value ZERO

$|1\rangle$ Basis, logical value ONE

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ Unit of Information by two basis

- Bit(Classical Unit of Information) when
  $\alpha = 1, \beta = 0 \Rightarrow |\psi\rangle = |0\rangle \ or \ \alpha = 0, \beta = 1 \Rightarrow |\psi\rangle = |1\rangle$
- Qubit(Quantum Unit of Information)
  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \alpha, \beta \in Complex\ Number, |\alpha|^2 + |\beta|^2 = 1$

Example) $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$

Basics of Quantum Computation

- Superposition
  - A qubit can represent two basis states simultaneously

Example) Two Qubits for Four Basis

$$
\begin{aligned}
|\psi_1\rangle \otimes |\psi_2\rangle &= \frac{1}{\sqrt{2}}(|0_1\rangle + |1_1\rangle) \otimes \frac{1}{\sqrt{2}}(|0_2\rangle + |1_2\rangle) \\
&= \frac{1}{4}(|0_1\rangle \otimes |0_2\rangle + |0_1\rangle \otimes |1_2\rangle + |1_1\rangle \otimes |0_2\rangle + |1_1\rangle \otimes |1_2\rangle) \\
&= \frac{1}{4}(|0_1\rangle|0_2\rangle + |0_1\rangle|1_2\rangle + |1_1\rangle|0_2\rangle + |1_1\rangle|1_2\rangle) \\
&= \frac{1}{4}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)
\end{aligned}
$$

n qubits can represent $|\psi\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{N-1} |k\rangle$

Exponential Reduction of Resource for State Space !!!!

Basics of Quantum Computation

- Entanglement
  - Space-like long distance correlation with no-signaling condition

Example) An Entangled State for two qubits

$$|\psi_{1\otimes 2}\rangle = \frac{1}{\sqrt{2}}(|0_1\rangle \otimes |0_2\rangle + |1_1\rangle \otimes |1_2\rangle)$$

If the state of first qubit is $|0_1\rangle$, then the state of second qubit MUST be $|0_2\rangle$

No signaling condition: No way to communicate faster than light !!!

Basics of Quantum Computation

- Interference
  - Two phases of a same basis can be interfered
    $\alpha|0\rangle + \beta|0\rangle = (\alpha + \beta)|0\rangle$

Basics of Quantum Computation

- Operation on quantum state
  - Unitary Operator for Evolving Quantum State

$$U|\psi_{init}\rangle \Rightarrow |\psi_{next}\rangle, where\, UU^{+} = I$$

  - Measurement Operator(Projection Operator)

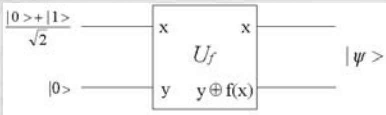
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad M = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) \qquad \langle k|m\rangle = \begin{cases} 1, \text{ if } k = m \\ 0, otherwise \end{cases}$$

If measure $|\psi\rangle$ by M, we can get the following state with corresponding probability

$$|\psi\rangle = \begin{cases} |0\rangle, P = |\alpha|^2 \\ |1\rangle, P = |\beta|^2 \end{cases}$$

Basics of Quantum Computation

- Quantum Parallelism



$$f(x): \{0,1\} \rightarrow \{0,1\}$$

$$|\psi> = \frac{|0, f(0)> + |1, f(1)>}{\sqrt{2}}$$

Basics of Quantum Computation

- General View of Quantum Computation

Initialize All Input Qubits → Make a Superposed State for All Search Space → Apply Necessary Unitary Operators with Oracle Calles → Measure Final State → If the final measurement output corresponds to the target solution, it stops. Otherwise, it redo all steps from beginning

Basics of Quantum Computation

- Bounded Quantum Probabilistic (BQP) Classes
  - Unless the quantum computation is sure success, the success probability is not unity
  - Hence, we have to redo the quantum computation several times

Contents

- Basics of Quantum Computation
- General Properties of Grover Search
  - Idea
  - Analysis
- Weight Decision
  - Symmetric Two Weights
  - Asymmetric Two Weights
  - Multiple Weights
- Conclusion

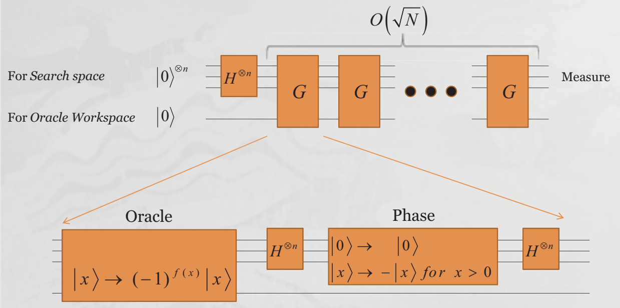
Search Problem

- Finds a certain x_t where $F(x_t)$=1 and x_t is n-bit number
  - $|x_i| = 2^n = N$
- Classical Oracle Query Complexity is $O(N)$
- Quantum Oracle Query Complexity is $O(\sqrt{N})$
  - Quadratic Speedup !!!

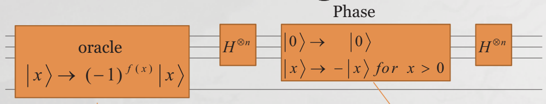
Basic Idea of Grover Search

- Lov Grover found a quantum search (1996)
- Basic Idea
  - Prepare and Initialize all input space
  - Apply Grover operator until only target input survive
    - Each Grover operator checks all function values for all input values simultaneously
      - Single Time Step for All Evaluations
    - Each Grover operator increases the phase amplitude of target input, and decreases the phase amplitudes of all other non-target inputs
      - Phase Amplitude increases linearly
  - Measure the final state, and hence only the target can be measured
    - The measurement probability is the square of the phase amplitude

Schematic circuit for the quantum search algorithm



Some Insights



$$\left.\begin{array}{l}|0\rangle \rightarrow |0\rangle \\ |x\rangle \rightarrow -|x\rangle \; for \; x>0\end{array}\right\} \Rightarrow (2|0\rangle\langle 0| - I)$$

$$\left.\begin{array}{l}|x\rangle, \; x \neq x_t \\ -|x\rangle, \; x = x_t\end{array}\right\} \Rightarrow (I - 2|x_t\rangle\langle x_t|)$$

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

$$\therefore \; G = (2|\psi\rangle\langle\psi| - I)(I - 2|x_t\rangle\langle x_t|)$$

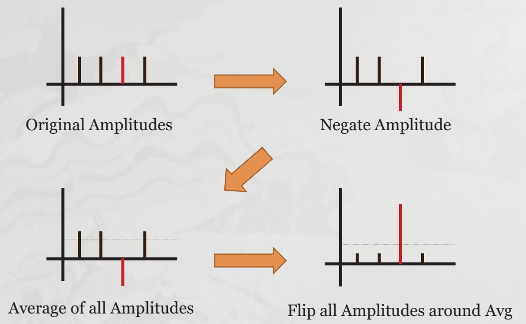
Some Insights

$(I - 2|x_t\rangle\langle x_t|)$: Inversion about the target

$(2|\psi\rangle\langle\psi| - I)$: Inversion about the average

$\therefore$ G= Inversion about the average * Inversion about the target

Example of Grover Search



Analysis

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

Let $|s\rangle = |x_t\rangle$ $\quad |ns\rangle = \sqrt{\frac{1}{N-1}} \sum_{x \neq x_t} |x\rangle$

$$\sin\frac{\theta}{2} = \frac{1}{\sqrt{N}} \qquad \cos\frac{\theta}{2} = \sqrt{\frac{N-1}{N}}$$

$$|\psi\rangle = \sin\frac{\theta}{2}|s\rangle + \cos\frac{\theta}{2}|ns\rangle$$

Analysis

Basis Vector: $\begin{pmatrix} |ns\rangle \\ |s\rangle \end{pmatrix} \Rightarrow |\psi\rangle = \begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix}$

$$\left(I - 2|x_t\rangle\langle x_t|\right) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \left(2|\psi\rangle\langle\psi| - I\right) = \begin{pmatrix} \cos 2\bullet\frac{\theta}{2} & \sin 2\bullet\frac{\theta}{2} \\ \sin 2\bullet\frac{\theta}{2} & -\cos 2\bullet\frac{\theta}{2} \end{pmatrix}$$

$$G = \begin{pmatrix} \cos 2\bullet\frac{\theta}{2} & -\sin 2\bullet\frac{\theta}{2} \\ \sin 2\bullet\frac{\theta}{2} & \cos 2\bullet\frac{\theta}{2} \end{pmatrix} = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \Rightarrow R(\theta)$$

Analysis

$$G|\psi\rangle = \begin{pmatrix} \cos 2\bullet\frac{\theta}{2} & -\sin 2\bullet\frac{\theta}{2} \\ \sin 2\bullet\frac{\theta}{2} & \cos 2\bullet\frac{\theta}{2} \end{pmatrix} \begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix} = \begin{pmatrix} \cos\left(\theta + \frac{\theta}{2}\right) \\ \sin\left(\theta + \frac{\theta}{2}\right) \end{pmatrix}$$

$$\therefore\ G^k|\psi\rangle = \begin{pmatrix} \cos\left(k\theta + \frac{\theta}{2}\right) \\ \sin\left(k\theta + \frac{\theta}{2}\right) \end{pmatrix}$$

Analysis

$$P_{sucess} = \left|\langle s|G^k|\psi\rangle\right|^2 = \sin^2\left(k\theta + \frac{\theta}{2}\right)$$

$$\sin^2\left(k\theta + \frac{\theta}{2}\right) => 1,\ P_{sucess} => 1$$

$$k\theta + \frac{\theta}{2} = \frac{\pi}{2} \qquad k = \frac{\pi}{2\theta} - \frac{1}{2}$$

$$\sin\frac{\theta}{2} = \frac{1}{\sqrt{N}}.$$

$$If\ N\ is\ large,\ \frac{1}{\sqrt{N}} \to 0,\ \sin\frac{\theta}{2} \to 0,\ \sin\frac{\theta}{2} \to \frac{\theta}{2},\ \therefore \frac{\theta}{2} \approx \frac{1}{\sqrt{N}}$$

$$k = \frac{\pi\sqrt{N}}{4} - \frac{1}{2} \qquad \therefore O\left(\sqrt{N}\right)$$

Contents

- General Properties of Grover Search
  - Idea
  - Analysis
- Weight Decision
  - Symmetric Two Weights
  - Asymmetric Two Weights
  - Multiple Weights
- Conclusion

Symmetric Two Weight Decision

"Exact quantum algorithm to distinguish Boolean functions of different weights",

Samuel L Braunstein, Byung-Soo Choi, Subhamoy Maitra, and Subhroshekhar Ghosh,

Journal of Physics A: Mathematical and Theoretical, ***40****(29) 8441-8454,*

http://dx.doi.org/10.1088/1751-8113/40/29/017

Motivation

- We can exploit the quantum computation for cryptanalysis
  - Cryptanalysis: Analyze the security of secure functions
  - Usually, it takes large volume of computation, and hence computationally hard to crack the secure functions
- In this work, as the basic level, we can consider to check the weight of Boolean functions

Definitions

- **Weight w of a Boolean function f**
  w = # of solutions / # of all inputs
- **Symmetric Weight Condition**
  $\{w_1, w_2 \mid w_1 + w_2 = 1,\ 0 < w_1 < w_2 < 1\}$
- **Symmetric Weight Decision Problem**
  Decide the exact weight w of f with the symmetric weight condition
- **Limited Weight Decision Problem**

$$w_1 = \sin^2\left(\frac{1}{2}\frac{k\pi}{2k+1}\right) \qquad w_2 = \cos^2\left(\frac{1}{2}\frac{k\pi}{2k+1}\right)$$

Grover Search in Hilbert Space

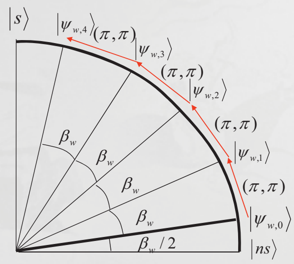
$$|\psi_{w,0}\rangle = \sin\frac{\beta_w}{2}|s\rangle + \cos\frac{\beta_w}{2}|ns\rangle$$

$$G = -I_{|\psi_{w,0}\rangle}(\theta) I_{|s\rangle}(\phi)$$

$$I_{|\psi\rangle}(\theta) \equiv I - (1 - e^{i\theta})|\psi\rangle\langle\psi|$$

$$\theta = \phi = \pi$$

$$G = -I_{|\psi_{w,0}\rangle}(\pi) I_{|s\rangle}(\pi)$$
$$= (2|\psi_{w,0}\rangle\langle\psi_{w,0}| - I)(I - 2|s\rangle\langle s|)$$



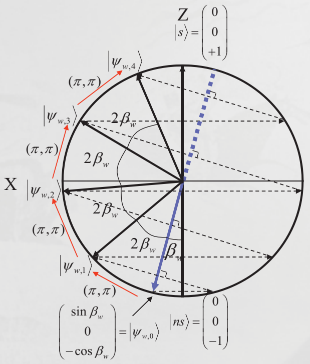
$$|\psi_{w,k}\rangle = \sin(2k+1)\frac{\beta_w}{2}|s\rangle + \cos(2k+1)\frac{\beta_w}{2}|ns\rangle$$

Grover Search in Bloch Sphere

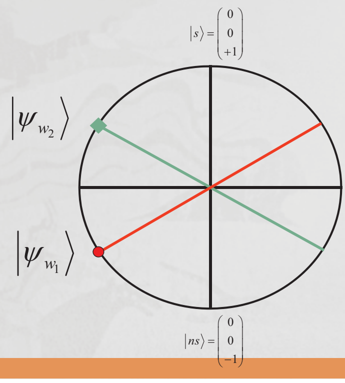
$$|\psi_{w,0}\rangle = \begin{pmatrix} \sin\beta_w \\ 0 \\ -\cos\beta_w \end{pmatrix}$$

$$G = -e^{i(\frac{\theta}{2}+\frac{\phi}{2})} R_{|\psi_{w,0}\rangle}(-\theta) R_{|s\rangle}(-\phi)$$

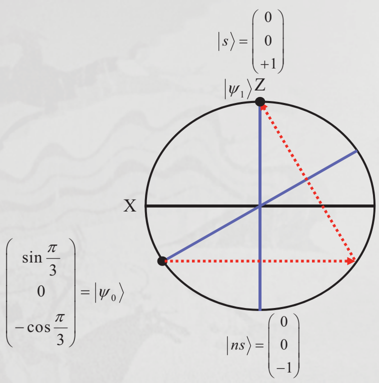
$$|\psi_{w,k}\rangle = \begin{pmatrix} \sin((2k+1)\beta_w) \\ 0 \\ -\cos((2k+1)\beta_w) \end{pmatrix}$$



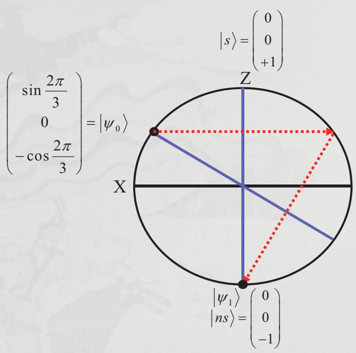
$w_1 + w_2 = 1$



$w_1 = 1/4$



$w_2 = 3/4$

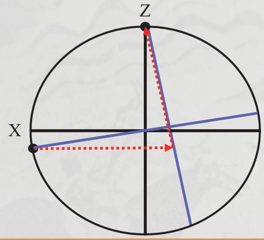


One Query is Sufficient

- When w_1 = ¼ and w_2 = ¾, One Query is Sufficient
- If the final measurement output is one of solutions, $w=w_1$
- If the final measurement output is one of non-solutions, $w=w_2$

Sure Success with One Query

- If ¼ <= w <=1 and w is known before, One Query is Sufficient to find any One of Solutions by Finding Two phases



D.P. Chi and J. Kim,
"Quantum database search by a single query"
in *First NASA International Conference on Quantum Computing and Quantum Communications, Palm Springs, 1998*, edited by C.P. Williams (Springer, Berlin, 1998)

Limited Weight-Decision Algorithm

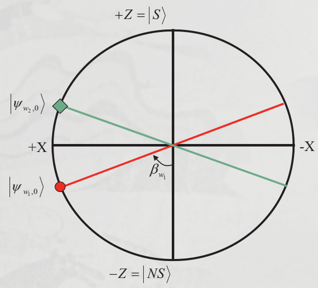
$$w_1 = \sin^2(\frac{1}{2}\frac{k\pi}{2k+1}) \qquad |\psi_{w_1,k}\rangle = \begin{pmatrix} \sin(k\pi) \\ 0 \\ -\cos(k\pi) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ -\cos(k\pi) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ (-1)^{k+1} \end{pmatrix}$$

$$w_2 = \cos^2(\frac{1}{2}\frac{k\pi}{2k+1}) = \sin^2(\frac{1}{2}\frac{(k+1)\pi}{2k+1}) \qquad |\psi_{w_2,k}\rangle = \begin{pmatrix} \sin((k+1)\pi) \\ 0 \\ -\cos((k+1)\pi) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ -\cos((k+1)\pi) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ (-1)^{k} \end{pmatrix}$$

Limited Weight-Decision Algorithm

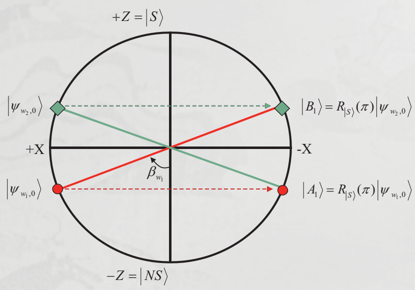
Apply k Grover operators to $|\psi_{w,0}\rangle$
Measure $|\psi_{w,k}\rangle$ in the computation basis
Let the measured result be $\hat{x}$
If k is even and $f(\hat{x})$=1, $w=w_2$ else $w=w_1$
If k is odd and $f(\hat{x})$=1, $w=w_1$ else $w=w_2$

When Two Steps are Sufficient



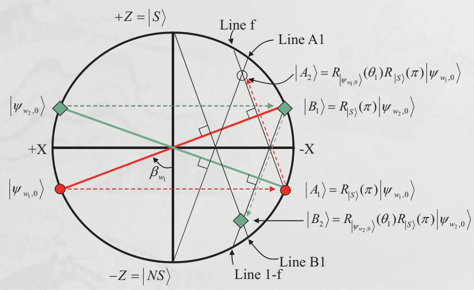
When Two Steps are Sufficient

$R_{|S\rangle}(\pi)|\psi_{w,0}\rangle$



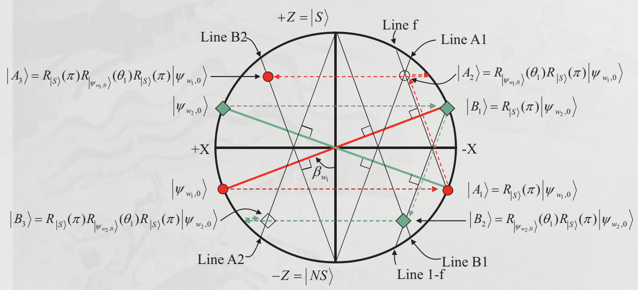
When Two Steps are Sufficient

$R_{|\psi_{w,0}\rangle}(\theta_1)R_{|S\rangle}(\pi)|\psi_{w,0}\rangle$

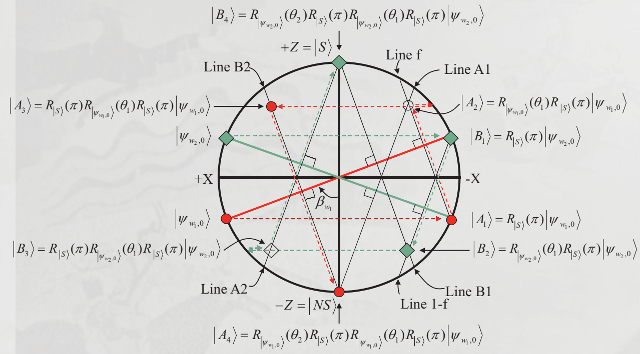


When Two Steps are Sufficient

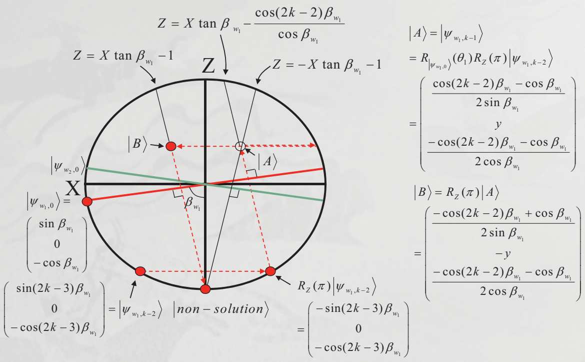
$R_{|S\rangle}(\pi)R_{|\psi_{w,0}\rangle}(\theta_1)R_{|S\rangle}(\pi)|\psi_{w,0}\rangle$



When Two Steps are Sufficient



Even K



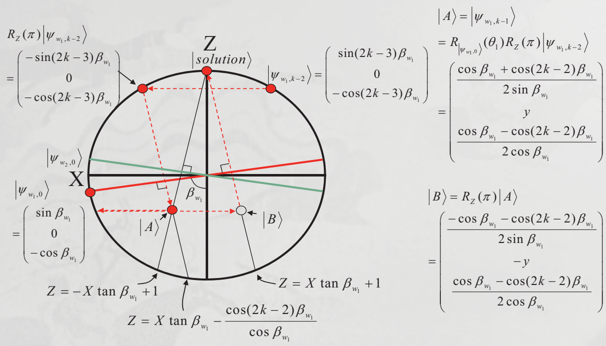
$$|\psi_{w_1,0}\rangle=\begin{pmatrix}\sin\beta_{w_1}\\0\\-\cos\beta_{w_1}\end{pmatrix}\qquad \begin{pmatrix}\sin(2k-3)\beta_{w_1}\\0\\-\cos(2k-3)\beta_{w_1}\end{pmatrix}=|\psi_{w_1,k-2}\rangle$$

$$R_Z(\pi)|\psi_{w_1,k-2}\rangle=\begin{pmatrix}-\sin(2k-3)\beta_{w_1}\\0\\-\cos(2k-3)\beta_{w_1}\end{pmatrix}$$

$$|A\rangle=|\psi_{w_1,k-1}\rangle=R_{|\psi_{w_1,0}\rangle}(\theta_1)R_Z(\pi)|\psi_{w_1,k-2}\rangle=\begin{pmatrix}\frac{\cos(2k-2)\beta_{w_1}-\cos\beta_{w_1}}{2\sin\beta_{w_1}}\\ y\\ \frac{-\cos(2k-2)\beta_{w_1}-\cos\beta_{w_1}}{2\cos\beta_{w_1}}\end{pmatrix}$$

$$|B\rangle=R_Z(\pi)|A\rangle=\begin{pmatrix}\frac{-\cos(2k-2)\beta_{w_1}+\cos\beta_{w_1}}{2\sin\beta_{w_1}}\\ -y\\ \frac{-\cos(2k-2)\beta_{w_1}-\cos\beta_{w_1}}{2\cos\beta_{w_1}}\end{pmatrix}$$

Odd K



$$R_Z(\pi)|\psi_{w_1,k-2}\rangle=\begin{pmatrix}-\sin(2k-3)\beta_{w_1}\\0\\-\cos(2k-3)\beta_{w_1}\end{pmatrix}\qquad |\psi_{w_1,k-2}\rangle=\begin{pmatrix}\sin(2k-3)\beta_{w_1}\\0\\-\cos(2k-3)\beta_{w_1}\end{pmatrix}\qquad |\psi_{w_1,0}\rangle=\begin{pmatrix}\sin\beta_{w_1}\\0\\-\cos\beta_{w_1}\end{pmatrix}$$

$$|A\rangle=|\psi_{w_1,k-1}\rangle=R_{|\psi_{w_1,0}\rangle}(\theta_1)R_Z(\pi)|\psi_{w_1,k-2}\rangle=\begin{pmatrix}\frac{\cos\beta_{w_1}+\cos(2k-2)\beta_{w_1}}{2\sin\beta_{w_1}}\\ y\\ \frac{\cos\beta_{w_1}-\cos(2k-2)\beta_{w_1}}{2\cos\beta_{w_1}}\end{pmatrix}$$

$$|B\rangle=R_Z(\pi)|A\rangle=\begin{pmatrix}\frac{-\cos\beta_{w_1}-\cos(2k-2)\beta_{w_1}}{2\sin\beta_{w_1}}\\ -y\\ \frac{\cos\beta_{w_1}-\cos(2k-2)\beta_{w_1}}{2\cos\beta_{w_1}}\end{pmatrix}$$

Phase Conditions for θ_1

$|\psi_{w_1,k-2}\rangle \rightarrow A$

Based on Even K

$$R_{|\psi_{w_1,0}\rangle}(\theta_1)R_z(\pi)\begin{pmatrix}\sin(2k-3)\beta_{w_1}\\0\\-\cos(2k-3)\beta_{w_1}\end{pmatrix}=\begin{pmatrix}\frac{\cos(2k-2)\beta_{w_1}-(-1)^k\cos\beta_{w_1}}{2\sin\beta_{w_1}}\\ y\\ \frac{-\cos(2k-2)\beta_{w_1}-(-1)^k\cos\beta_{w_1}}{2\cos\beta_{w_1}}\end{pmatrix}$$

$$y=\sin\theta_1\sin(2k-2)\beta_{w_1}$$

$$\cos\theta_1=\frac{(-1)^k\cos\beta_{w_1}-2\cos\beta_{w_1}\cos(2k-2)\beta_{w_1}}{\sin 2\beta_{w_1}\sin(2k-2)\beta_{w_1}}$$

Phase Conditions for θ_2

$$R_{|\psi_{w_1,0}\rangle}(\theta_2)\begin{pmatrix}\frac{-\cos(2k-2)\beta_{w_1}+(-1)^k\cos\beta_{w_1}}{2\sin\beta_{w_1}}\\ -y\\ \frac{-\cos(2k-2)\beta_{w_1}-(-1)^k\cos\beta_{w_1}}{2\cos\beta_{w_1}}\end{pmatrix}=\begin{pmatrix}0\\0\\-(-1)^k\end{pmatrix}$$

$$\cos\theta_2=\frac{(-1)^k\sin 2\beta_{w_1}(y\sin\theta_1-(-1)^k\sin\beta_{w_1})}{\cos\beta_{w_1}\cos 2\beta_{w_1}-(-1)^k(2k-2)\beta_{w_1}}$$

Symmetric Weight-Decision Algorithm

Symmetric Weight Decision Algorithm

$|\psi_{w,0}\rangle = |0\rangle^{\otimes n}|1\rangle,\ i=0$

If $w_1 \le \sin^2\frac{\pi}{5}, k=2,$

Otherwise k satisfies $\sin^2(\frac{k-1}{2k-1}\frac{\pi}{2}) < w_1 \le \sin^2(\frac{k}{2k+1}\frac{\pi}{2})$

$\frac{k-1}{2k-1}\pi < \beta_{w_1} \le \frac{k}{2k+1}\pi \qquad \beta_{w_1} + \beta_{w_2} = \pi$

While $i < (k-2)$ do

$\{\ |\psi_{w,i+1}\rangle = -I_{|\psi_{w,0}\rangle}(\pi) I_{|s\rangle}(\pi) |\psi_{w,i}\rangle, i = i+1 \quad \}$

$|\psi_{w,k-1}\rangle = -I_{|\psi_{w,0}\rangle}(-\theta_1) I_{|s\rangle}(\pi) |\psi_{w,k-2}\rangle, \qquad |\psi_{w,k}\rangle = -I_{|\psi_{w,0}\rangle}(-\theta_2) I_{|s\rangle}(\pi) |\psi_{w,k-1}\rangle$

Measure $|\psi_{w,k}\rangle$ in the computational basis

Let the result be $\hat{x}$

If k is odd and $f(\hat{x})=1$ then $w=w_1$ else $w=w_2$

If k is even and $f(\hat{x})=1$ then $w=w_2$ else $w=w_1$

Performance

- When k is given,
- Classical Lower Bound
  - At least $O(k^2)$
- Quantum Upper Bound
  - At most $O(k)$

Conclusions and Open Problems

- For General Weight Condition, an Exact Quantum Algorithm is possible
- When General Weights?
  - Only the condition: $0<w_1<w_2<1$
- When Multiple Weights?
  - $w_1, w_2, w_3, \ldots$
- What is the Lower Bound for Weight Decision Problems?

Contents

- General Properties of Grover Search
  - Idea
  - Analysis
- Weight Decision
  - Symmetric Two Weights
  - Asymmetric Two Weights
  - Multiple Weights
- Conclusion

Asymmetric Two Weight Decision

"Quantum Algorithm for the Asymmetric Weight Decision Problem and its Generalization to Multiple Weights",

Byung-Soo Choi and Samuel L. Braunstein

To Appear on Quantum Information Processing,

http://dx.doi.org/10.1007/s11128-010-0187-9

Motivation

- Extend the Symmetric Case to Asymmetric Case
- Problem
  - $0<w_1+w_2<2$

Basic Idea

- Modify the Oracle Function by Adding two qubits more to reduce the problem into the symmetric case
- $w_1 = n_1/N$, $w_2 = n_2/N$
- To satisfy $w_1' + w_2' = 1$, we modify the Oracle as

$$f'(x) = \begin{cases} f(x), & 0 \le x < N, \\ f(x), & N \le x < 2N, \\ 1, & 2N \le x < 2N + l, \\ 0, & 2N + l \le x < 4N \end{cases}$$

Basic Idea

$$w_1' = \frac{2n_1 + l}{4N} \qquad w_2' = \frac{2n_2 + l}{4N}$$

$$w_1' + w_1' = 1 \Rightarrow l = 2N - (n_1 + n_2)$$

Conclusion

- By adding more input space, we can reduce the asymmetric weight decision problem into the symmetric weight decision problem
- For adding more inputs, we just need only two qubits

Contents

- General Properties of Grover Search
  - Idea
  - Analysis
- Weight Decision
  - Symmetric Two Weights
  - Asymmetric Two Weights
  - Multiple Weights
- Conclusion

Motivation

- Given a Boolean function f, decide exactly the weight w of f where $w \in \{0 < w_1 < w_2 \cdots < w_m < 1\}$.

Basic Idea

Multiple Weight Decision Algorithm

Let $S = \{w1, w2, \ldots, wm\}$.
WHILE ($|S| = 1$)
{
  w_{min} = smallest weight from S.
  w_{max} = largest weight from S.
  Asymmetric Weight Decision Algorithm(w_{min}, w_{max}).
  $S = S$ – non_selected weight.
}
Return the exact weight as S.

Analysis

- Classical Query Complexity is O(N)
- Overall Complexity is $O\left(m\sqrt{N}\right)$
- When $m \le \sqrt{N}$, the proposed algorithm works faster than classical one

Contents

- General Properties of Grover Search
  - Idea
  - Analysis
- Weight Decision
  - Symmetric Two Weights
  - Asymmetric Two Weights
  - Multiple Weights
- Conclusion

Conclusion

- The Speedup of Grover search is quadratic, not exponential.
- However, the applications based on Grover search is very wide
- In this talk, we just discuss applications of Grover search for Weight Decision Problem of Boolean function
  - Symmetric Weight
  - Asymmetric Weight
  - Multiple Weights
- Since lots of classical algorithms are based on Search algorithm, Grover search can be utilized for them with showing quadratic speedup