Grover Search and its Applications

Byung-Soo Choi

bschoi3@gmail.com
Contents

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

\[ |0\rangle \quad \text{Basis, logical value ZERO} \]
\[ |1\rangle \quad \text{Basis, logical value ONE} \]

\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad \text{Unit of Information by two basis} \]

- **Bit (Classical Unit of Information)** when
  \[ \alpha = 1, \beta = 0 \Rightarrow |\psi\rangle = |0\rangle \quad \text{or} \quad \alpha = 0, \beta = 1 \Rightarrow |\psi\rangle = |1\rangle \]

- **Qubit (Quantum Unit of Information)**
  \[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \alpha, \beta \in \text{Complex Number}, |\alpha|^2 + |\beta|^2 = 1 \]

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

\[ |\psi_1\rangle \otimes |\psi_2\rangle = \frac{1}{\sqrt{2}} (|0_1\rangle + |1_1\rangle) \otimes \frac{1}{\sqrt{2}} (|0_2\rangle + |1_2\rangle) \]

\[ = \frac{1}{4} (|0_1\rangle \otimes |0_2\rangle + |0_1\rangle \otimes |1_2\rangle + |1_1\rangle \otimes |0_2\rangle + |1_1\rangle \otimes |1_2\rangle) \]

\[ = \frac{1}{4} (|0_1\rangle |0_2\rangle + |0_1\rangle |1_2\rangle + |1_1\rangle |0_2\rangle + |1_1\rangle |1_2\rangle) \]

\[ = \frac{1}{4} (|00\rangle + |01\rangle + |10\rangle + |11\rangle) \]

\( n \) 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

\[ |\psi_{1\otimes2}\rangle = \frac{1}{\sqrt{2}} (|0_1\rangle \otimes |0_2\rangle + |1_1\rangle \otimes |1_2\rangle) \]

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

  \[ U |\psi_{\text{init}}\rangle \Rightarrow |\psi_{\text{next}}\rangle, \text{where } UU^* = I \]

- Measurement Operator (Projection Operator)

  \[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad M = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \quad \langle k|m\rangle = \begin{cases} 1, \text{ if } k = m \\ 0, \text{ otherwise} \end{cases} \]

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

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

\[
f(x): \{0,1\} \rightarrow \{0,1\}
\]
General View of Quantum Computation

- Initialize All Input Qubits
- Make a Superposed State for All Search Space
- Apply Necessary Unitary Operators with Oracle Calls
- 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

For Search space
\[ |0\rangle^\otimes n \]

\[ H^\otimes n \]

\[ G \]

\[ G \]

\[ \cdots \]

\[ G \]

Measure

For Oracle Workspace
\[ |0\rangle \]

Oracle

\[ |x\rangle \rightarrow (-1)^{f(x)} |x\rangle \]

Phase

\[ H^\otimes n \]

\[ |0\rangle \rightarrow |0\rangle \]

\[ |x\rangle \rightarrow -|x\rangle \text{ for } x > 0 \]

\[ O(\sqrt{N}) \]
Some Insights

Phase

\[ \begin{align*}
|0\rangle & \rightarrow |0\rangle \\
|x\rangle & \rightarrow -|x\rangle \text{ for } x > 0
\end{align*} \]

\[
\begin{align*}
|x\rangle, x \neq x_t & \Rightarrow \left( I - 2 |x_t\rangle \langle x_t| \right) \\
- |x\rangle, x = x_t & \Rightarrow \left( I - 2 |x_t\rangle \langle x_t| \right)
\end{align*}
\]

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

\[
\therefore \quad G = (2 |\psi\rangle \langle \psi| - I) \left( I - 2 |x_t\rangle \langle x_t| \right)
\]
Some Insights

\[
(I - 2| x_t \rangle \langle x_t |) \quad \text{: Inversion about the target}
\]

\[
\left(2 | \psi \rangle \langle \psi | - I \right) \quad \text{: Inversion about the average}
\]

\[
\therefore \quad G = \text{Inversion about the average} \ast \text{Inversion about the target}
\]
Example of Grover Search

Original Amplitudes

Average of all Amplitudes

Negate Amplitude

Flip all Amplitudes around Avg
Analysis

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

Let

\( |s\rangle = |x_i\rangle \quad \quad |ns\rangle = \sqrt{\frac{1}{N-1}} \sum_{x \neq x_i} |x\rangle \)

\[
\sin \frac{\theta}{2} = \frac{1}{\sqrt{N}} \\
\cos \frac{\theta}{2} = \sqrt{\frac{N-1}{N}}
\]

\( |\psi\rangle = \sin \frac{\theta}{2} |s\rangle + \cos \frac{\theta}{2} |ns\rangle \)
Analysis

Basis Vector: \( \begin{pmatrix} nS \\ S \end{pmatrix} \) \( \Rightarrow \) \( \ket{\psi} = \begin{pmatrix} \cos \frac{\theta}{2} \\ \theta \\ \sin \frac{\theta}{2} \end{pmatrix} \)

\[
(I - 2\bra{x_t}\ket{x_t}) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (2\bra{\psi}\ket{\psi} - I) = \begin{pmatrix} \cos 2\cdot \frac{\theta}{2} & \sin 2\cdot \frac{\theta}{2} \\ \sin 2\cdot \frac{\theta}{2} & -\cos 2\cdot \frac{\theta}{2} \end{pmatrix}
\]

\[
G = \begin{pmatrix} \cos 2\cdot \frac{\theta}{2} & -\sin 2\cdot \frac{\theta}{2} \\ \sin 2\cdot \frac{\theta}{2} & \cos 2\cdot \frac{\theta}{2} \end{pmatrix} = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \quad \Rightarrow \quad R(\theta)
\]
Analysis

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

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

\[ P_{success} = \left| \langle s \mid G^k \mid \psi \rangle \right|^2 = \sin^2 \left( k\theta + \frac{\theta}{2} \right) \]

\[ \sin^2 \left( k\theta + \frac{\theta}{2} \right) \Rightarrow 1, \quad P_{success} \Rightarrow 1 \]

\[ k\theta + \frac{\theta}{2} = \frac{\pi}{2} \quad k = \frac{\pi}{2\theta} - \frac{1}{2} \]

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

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}} \]

\[ k = \frac{\pi \sqrt{N}}{4} - \frac{1}{2} \quad \therefore O\left(\sqrt{N}\right) \]
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
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 $f$**
  \[
  w = \frac{\text{# of solutions}}{\text{# of all inputs}}
  \]

- **Symmetric Weight Condition**
  \[
  \{w_1, w_2 | w_1 + w_2 = 1, 0 < w_1 < w_2 < 1\}
  \]

- **Symmetric Weight Decision Problem**
  Decide the exact weight $w$ of $f$ with the symmetric weight condition

- **Limited Weight Decision Problem**
  \[
  w_1 = \sin^2\left(\frac{1}{2} \frac{k\pi}{2k+1}\right) \quad w_2 = \cos^2\left(\frac{1}{2} \frac{k\pi}{2k+1}\right)
  \]
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

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

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

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

\[ Z |s\rangle = \begin{pmatrix} 0 \\ 0 \\ +1 \end{pmatrix} \]
$\omega_1 + \omega_2 = 1$

$|s\rangle = \begin{pmatrix} 0 \\ 0 \\ +1 \end{pmatrix}$

$|\psi_{\omega_2}\rangle$

$|\psi_{\omega_1}\rangle$

$|ns\rangle = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}$
\( w_1 = 1/4 \)

\[ |s\rangle = \begin{pmatrix} 0 \\ 0 \\ +1 \end{pmatrix} \]

\[ |\psi_1\rangle \]

\[ |\psi_0\rangle = \begin{pmatrix} \sin \frac{\pi}{3} \\ 0 \\ -\cos \frac{\pi}{3} \end{pmatrix} \]

\[ |ns\rangle = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix} \]
\[ w_2 = \frac{3}{4} \]

\[
\begin{pmatrix}
\sin \frac{2\pi}{3} \\
0 \\
-\cos \frac{2\pi}{3}
\end{pmatrix} = |\psi_0\rangle
\]

\[
|s\rangle = \begin{pmatrix} 0 \\ 0 \\ +1 \end{pmatrix}
\]

\[
|\psi_1\rangle = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}
\]

\[
|ns\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}
\]
One Query is Sufficient

- When \( w_1 = \frac{1}{4} \) and \( w_2 = \frac{3}{4} \), 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 $\frac{1}{4} \leq w \leq 1$ 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”
Limited Weight-Decision Algorithm

\[ w_1 = \sin^2 \left( \frac{1}{2} \frac{k\pi}{2k+1} \right) \]
\[ w_2 = \cos^2 \left( \frac{1}{2} \frac{k\pi}{2k+1} \right) \]
\[ w_2' = \sin^2 \left( \frac{1}{2} \frac{(k+1)\pi}{2k+1} \right) \]

\[ |\psi_{w_1,k}\rangle = \begin{pmatrix} 
\sin(k\pi) \\
0 \\
-\cos(k\pi)
\end{pmatrix} = \begin{pmatrix} 
0 \\
0 \\
-\cos(k\pi)
\end{pmatrix} = \begin{pmatrix} 
0 \\
0 \\
(-1)^{k+1}
\end{pmatrix} \]

\[ |\psi_{w_2,k}\rangle = \begin{pmatrix} 
\sin((k+1)\pi) \\
0 \\
-\cos((k+1)\pi)
\end{pmatrix} = \begin{pmatrix} 
0 \\
0 \\
-\cos((k+1)\pi)
\end{pmatrix} = \begin{pmatrix} 
0 \\
0 \\
(-1)^{k}
\end{pmatrix} \]

---

**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

\[ +Z = |S\rangle \]

\[ -Z = |NS\rangle \]
When Two Steps are Sufficient

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

+Z = |S\rangle

\[ |\psi_{w_2,0}\rangle \]

\[ |\psi_{w_1,0}\rangle \]

\[ |B_1\rangle = R_{|S\rangle} (\pi) |\psi_{w_2,0}\rangle \]

\[ |A_1\rangle = R_{|S\rangle} (\pi) |\psi_{w_1,0}\rangle \]

\[ +X \]

\[ -X \]

\[ \beta_{w_1} \]

\[ -Z = |NS\rangle \]
When Two Steps are Sufficient

\[ R_{\psi_{w,0}}(\theta_1) R_{S}(\pi) \psi_{w,0} \]
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

\[ |B_4\rangle = R_{\psi_{w_2,0}}(\theta_2) R_{|S\rangle}(\pi) R_{\psi_{w_2,0}}(\theta_1) R_{|S\rangle}(\pi) |\psi_{w_2,0}\rangle \]

\[ +Z = |S\rangle \]

\[ |A_3\rangle = R_{|S\rangle}(\pi) R_{\psi_{w_1,0}}(\theta_1) R_{|S\rangle}(\pi) |\psi_{w_1,0}\rangle \]

\[ |B_2\rangle = R_{|S\rangle}(\pi) |\psi_{w_2,0}\rangle \]

\[ -Z = |NS\rangle \]

\[ |A_4\rangle = R_{\psi_{w_1,0}}(\theta_2) R_{|S\rangle}(\pi) R_{\psi_{w_1,0}}(\theta_1) R_{|S\rangle}(\pi) |\psi_{w_1,0}\rangle \]

\[ |A_2\rangle = R_{\psi_{w_1,0}}(\theta_1) R_{|S\rangle}(\pi) |\psi_{w_1,0}\rangle \]

\[ |B_1\rangle = R_{|S\rangle}(\pi) |\psi_{w_2,0}\rangle \]

\[ |B_3\rangle = R_{|S\rangle}(\pi) R_{\psi_{w_2,0}}(\theta_1) R_{|S\rangle}(\pi) |\psi_{w_2,0}\rangle \]

\[ |A_1\rangle = R_{|S\rangle}(\pi) |\psi_{w_1,0}\rangle \]

\[ |B_1\rangle = R_{|\psi_{w_2,0}\rangle}(\theta_1) R_{|S\rangle}(\pi) |\psi_{w_2,0}\rangle \]

\[ |A_2\rangle = R_{|\psi_{w_1,0}\rangle}(\theta_1) R_{|S\rangle}(\pi) |\psi_{w_1,0}\rangle \]
Even K

\[ Z = X \tan \beta_{w_i} - \frac{\cos(2k - 2) \beta_{w_i}}{\cos \beta_{w_i}} \]

\[ Z = X \tan \beta_{w_i} - 1 \]

\[ Z = -X \tan \beta_{w_i} - 1 \]

\[ |A\rangle = |\psi_{w_i,k-1}\rangle = R_{|\psi_{w_i,0}\rangle} (\theta_1) R_Z (\pi) |\psi_{w_i,k-2}\rangle \]

\[ = \begin{pmatrix} \cos(2k - 2) \beta_{w_i} - \cos \beta_{w_i} \\ 2 \sin \beta_{w_i} \\ -y \\ -\cos(2k - 2) \beta_{w_i} - \cos \beta_{w_i} \end{pmatrix} \frac{2 \cos \beta_{w_i}}{2 \cos \beta_{w_i}} \]

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

\[ |\psi_{w_1,0}\rangle = \begin{pmatrix} \sin \beta_{w_i} \\ 0 \\ -\cos \beta_{w_i} \end{pmatrix} \]

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

\[ \text{non-solution} \]
Odd K

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

\[ |\psi_{w_1,0}\rangle = \begin{pmatrix} \sin\beta_{w_1} \\ 0 \\ -\cos\beta_{w_1} \end{pmatrix} \]

\[ Z = -X \tan \beta_{w_1} + 1 \]

\[ Z = X \tan \beta_{w_1} - \frac{\cos(2k-2)\beta_{w_1}}{\cos \beta_{w_1}} \]

\[ |A\rangle = \frac{\sin(2k-3)\beta_{w_1}}{2\sin\beta_{w_1}} \left( \cos\beta_{w_1} + \cos(2k-2)\beta_{w_1} \right) \]

\[ + \frac{-\cos\beta_{w_1} - \cos(2k-2)\beta_{w_1}}{2\cos\beta_{w_1}} \]

\[ |B\rangle = R_z(\pi) |A\rangle \]

\[ = \begin{pmatrix} \cos\beta_{w_1} + \cos(2k-2)\beta_{w_1} \\ 2\sin\beta_{w_1} \cos\beta_{w_1} \\ y \cos\beta_{w_1} - \cos(2k-2)\beta_{w_1} \end{pmatrix} \]
Phase Conditions for $\theta_1$

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

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

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

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

Based on Even $K$
Phase Conditions for $\theta_2$

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

$$= \begin{pmatrix}
0 \\
0
\end{pmatrix}$$

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

If $w_i \leq \sin^2 \frac{\pi}{5}, k = 2$,
Otherwise $k$ satisfies $\sin^2 \left( \frac{k-1}{2k-1} \frac{\pi}{2} \right) < w_i \leq \sin^2 \left( \frac{k}{2k+1} \frac{\pi}{2} \right)$

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

While $i < (k - 2)$ do
{ $$|\psi_{w,i+1}\rangle = -I_{|\psi_{w,0}\rangle} (\pi) I_{|s\rangle} (\pi) |\psi_{w,i}\rangle, i = i + 1$$ }

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

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 $w = w_1$
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?
  - $w_1, w_2, w_3, ...$

- 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

\[
f'(x) = \begin{cases} 
  f(x), & 0 \leq x < N, \\
  f(x), & N \leq x < 2N, \\
  1, & 2N \leq x < 2N + l, \\
  0, & 2N + l \leq x < 4N 
\end{cases}
\]
Basic Idea

\[ w_1' = \frac{2n_1 + l}{4N} \quad w_2' = \frac{2n_2 + l}{4N} \]

\[ w_1' + w_1' = 1 \Rightarrow l = 2N - (n_1 + n_2) \]
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 $S = \{w_1, w_2, \ldots, w_m\}$.
WHILE ($|S| = 1$) {
\{$
  w_{\text{min}} = \text{smallest weight from } S.
  w_{\text{max}} = \text{largest weight from } S.
  \text{Asymmetric Weight Decision Algorithm}(w_{\text{min}}, w_{\text{max}}).
  S = S - \text{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 $m \leq \sqrt{N}$, 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
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.

Conclusion