<table>
<thead>
<tr>
<th>項目</th>
<th>内容</th>
</tr>
</thead>
<tbody>
<tr>
<td>タイトル</td>
<td>グローバル検索とその応用</td>
</tr>
<tr>
<td>著者</td>
<td>蔡、勇敏</td>
</tr>
<tr>
<td>参照</td>
<td>2010年度科学技術振興機構ERATO構造物解析プロジェクト研究報告書. p.56-66.</td>
</tr>
<tr>
<td>発行日</td>
<td>2011-06</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2115/48476">http://hdl.handle.net/2115/48476</a></td>
</tr>
<tr>
<td>タイプ</td>
<td>学術講演会</td>
</tr>
<tr>
<td>メモ</td>
<td>ハコベラセミナ 2010年8月3日</td>
</tr>
</tbody>
</table>

HOKKAIDO UNIVERSITY
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

- 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

\[ |0\rangle \text{ Basis, logical value ZERO} \]
\[ |1\rangle \text{ Basis, logical value ONE} \]
\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \text{ Unit of Information by two basis} \]

- 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) \( |\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \alpha, \beta \in \text{Complex Number} \), \( |\alpha|^2 + |\beta|^2 = 1 \)

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

\[ |\psi_0\rangle = \frac{1}{4}(1,0) = \frac{1}{2} (|00\rangle + \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) + \frac{1}{\sqrt{2}} (|11\rangle + |00\rangle) \]

\( n \) qubits can represent \( |\psi\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_i |i\rangle \)

Exponential Reduction of Resource for State Space!!!!

Entanglement

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

Example) An Entangled State for two qubits

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

If the state of first qubit is \( |0\rangle \), then the state of second qubit MUST be \( |0\rangle \)

No signaling condition: No way to communicate faster than light !!!!
Basics of Quantum Computation

**Operation on quantum state**
- Unitary Operator for Evolving Quantum State
  \[ U |\psi_0\rangle = |\psi_{\text{out}}\rangle, \text{ where } U^* U = I \]
- Measurement Operator (Projection Operator)
  \[ |\psi\rangle = a |0\rangle + b |1\rangle \quad M = \frac{1}{2}(|0\rangle \langle 0| + |1\rangle \langle 1|) \quad \langle \psi | m \rangle = \begin{cases} 1, & \text{if } k = m \\ 0, & \text{otherwise} \end{cases} \]

If measure \( |\psi\rangle \) by \( M \), we can get the following state with corresponding probability
\[ |\psi\rangle = \begin{cases} |0\rangle, P = |a|^2 \\ |1\rangle, P = |b|^2 \end{cases} \]

**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.

**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
  - \( |x_t| = 2^n = N \)
- 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

\[
G = (2\psi\langle\psi|-I)(I - 2|x_i\rangle\langle x_i|)
\]

Example of Grover Search

Analysis

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

Let \[|\hat{s}\rangle = |x_i\rangle \quad |ns\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq x_i} |x\rangle\]

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

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

Basis Vector:

\[
\begin{bmatrix}
1
\end{bmatrix}
\]

\[
\begin{bmatrix}
0
\end{bmatrix}
\]

\[
\begin{pmatrix}
\cos \theta/2 \\
\sin \theta/2
\end{pmatrix}
\]

\[
G\psi =
\begin{pmatrix}
\cos \theta/2 & -\sin \theta/2 \\
\sin \theta/2 & \cos \theta/2
\end{pmatrix}
\begin{pmatrix}
\cos \theta/2 \\
\sin \theta/2
\end{pmatrix}
\]

\[
\cos (k\theta + \theta/2)
\]

\[
\sin (k\theta + \theta/2)
\]

\[
R(\theta)
\]

Analysis

\[
P_{\text{success}} = |\langle x | G^\dagger | x \rangle|^2 = \sin^2 \left( \frac{k\theta + \theta}{2} \right)
\]

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

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

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

If \( N \) is large, \( \frac{1}{\sqrt{N}} \to 0 \), \( \sin \frac{\theta}{2} \to 0 \), \( \sin \frac{\theta}{2} + \theta \), \( \frac{\theta}{2} \approx \frac{1}{\sqrt{N}} \)

\[
k = \frac{\pi \sqrt{N}}{4} \quad \frac{1}{2} \quad O(\sqrt{N})
\]

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.

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 $f$
  $w = \# \text{ of solutions} / \# \text{ of all inputs}$
- 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
  \[ w_1 = \sin\left(\frac{k\pi}{22k+1}\right), \quad w_2 = \cos\left(\frac{k\pi}{22k+1}\right) \]

Grover Search in Hilbert Space

- \[ |\psi_{w_1}\rangle = \sin\beta|\psi\rangle + \cos\beta|\psi\rangle_{\text{ms}} \]
- \[ G = -i|\psi\rangle\langle\psi| (-\theta) |\psi\rangle\langle\psi| (-\phi) \]
- \[ |\psi_{w_2}\rangle = \sin((2k+1)\beta)|\psi\rangle + \cos((2k+1)\beta)|\psi\rangle_{\text{ms}} \]

Grover Search in Bloch Sphere

- $w_1 + w_2 = 1$
- $w_1 = 1/4$
- $w_2 = 3/4$
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, $w=w_2$

Limited Weight-Decision Algorithm

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

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

When Two Steps are Sufficient
$R_{f_1}(\pi)|\psi_{in}\rangle$

When Two Steps are Sufficient
$R_{f_1}^{(1)}(\theta)R_{f_1}(\pi)|\psi_{in}\rangle$
When Two Steps are Sufficient

Even K

Odd K

Phase Conditions for $\theta_1$

$|\psi_{\psi,1,2}\rangle \rightarrow A$

Based on Even K

$R_{\psi,\pi/2}(\theta)R_{\psi,0}(\pi) \left( \begin{array}{c}
\sin(2k-3)\beta_v \\
0
\end{array} \right) \left( \begin{array}{c}
\cos(2k-2)\beta_v - (-1)^k \cos \beta_v \\
2 \sin \beta_v \\
\end{array} \right) = y$

$y = \sin \theta_1 \sin(2k-2)\beta_v$

$\cos \theta_1 = (-1)^k \cos \beta_v - 2 \cos \beta_v \cos(2k-2)\beta_v$

$\sin 2\beta_v \sin(2k-2)\beta_v$

Phase Conditions for $\theta_2$

$R_{\psi,\pi/2}(\theta)R_{\psi,0}(\pi) \left( \begin{array}{c}
\sin(2k-3)\beta_v \\
0
\end{array} \right) \left( \begin{array}{c}
-\cos(2k-2)\beta_v + (-1)^k \cos \beta_v \\
2 \sin \beta_v \\
\end{array} \right) = y$

$y = \sin \theta_2 \sin(2k-2)\beta_v$

$\cos \theta_2 = (-1)^k \sin 2\beta_v \sin(2k-2)\beta_v$

$\sin \beta_v \cos 2\beta_v - (-1)^k (2k-2)\beta_v$
Symmetric Weight Decision Algorithm

\[ |\psi_{-}\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \]

If \( k \equiv 0 \mod 2 \),
Otherwise \( k \) satisfies \( 2^{\frac{k-1}{2}} \leq n < 2^{\frac{k}{2}} \)

\[ \frac{1}{\sqrt{2^{\frac{k+1}{2}}}} \beta_0 + \beta_n = \pi \]

While \( i \leq k-2 \) do
\[ |\psi_{-i}\rangle = -\frac{1}{\sqrt{2^{\frac{i+1}{2}}}} |\psi_{-(i-1)}\rangle \]

\[ |\psi_{-}\rangle = -\frac{1}{\sqrt{2}} (-i)^i |\psi_{0}\rangle \]

Measure \( |\psi_{-}\rangle \) in the computational basis
Let the result be \( \hat{i} \)
If \( k \) is odd and \( /i\equiv 1 \) then \( w = w_i \) else \( w = w_{\bar{i}} \)
If \( k \) is even and \( /i\equiv 1 \) then \( w = w_i \) else \( w = w_{\bar{i}} \)

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?

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

Performance

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

Contents

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

Motivation

- Extend the Symmetric Case to Asymmetric Case
- Problem
  - \( 0 < w_1 + w_2 < 2 \)
Modify the Oracle Function by Adding two qubits more to reduce the problem into the symmetric case

- \( w_1 = \frac{n_1}{N}, \ w_2 = \frac{n_2}{N} \)
- To satisfy \( w_1 + w_2 = 1 \), we modify the Oracle as

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

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

### Conclusion
- 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
- Let \( S = \{w_1, w_2, \ldots, w_m\} \).
  While \(|S| = 1\)
  \[
  \begin{align*}
    w_{\text{min}} &= \text{smallest weight from } S. \\
    w_{\text{max}} &= \text{largest weight from } S. \\
    \text{Asymmetric Weight Decision Algorithm}(w_{\text{min}}, w_{\text{max}}). \\
    S &= S - \text{non-selected weight}.
  \end{align*}
  \]
  Return the exact weight as \( S \).
### Analysis
- Classical Query Complexity is $O(N)$
- Overall Complexity is $O(m\sqrt{N})$
- 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

---

### 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.