Quantum Computing - Grover’s Algorithm

Programming Quantum Computers: A Primer with IBM Q and D-Wave Exercises

Patrick Dreher
NC State University
Chief Scientist - NCSU IBM Q Hub
Demo of the Grover Algorithm
Using the Quirk Simulator
Grover Algorithm

• Classically, searching an unsorted database requires a linear search that is of $O(N)$ in time.

• Grover’s quantum search algorithm finds the unique input to a black box function that produces a particular output value, with only $\mathcal{O}(N^{1/2})$ evaluations of the function with high probability.

• It is the fastest possible quantum algorithm for searching an unsorted database and provides a quadratic speedup.

• Reference:
  • Quantum Algorithm Implementation for Beginners https://arxiv.org/pdf/1804.03719
Grover Algorithm

• Find a unique item in an unstructured search among N items
• Classically worst case requires check of N boxes
• In quantum computer
  • Prepare of superposition of initial states that are
    \[ |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \]
  • Oracle on \(|-\rangle\) reverses the amplitude of that state

\[
0|x^*\rangle \frac{|f(x^*)\oplus 0\rangle - |f(x^*)\oplus 1\rangle}{\sqrt{2}} = |x^*\rangle \frac{|1\rangle - |0\rangle}{\sqrt{2}} = -|x^*\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}
\]
Grover Algorithm

- Define Grover operator $G$ and initial uniform superposition of states $|\psi\rangle$ and $G = [2|\psi\rangle\langle\psi| - I] \otimes$
- The amplitude of each state is flipped about the mean

$$G = [2|\psi\rangle\langle\psi| - I] \sum_i a_i |i\rangle = \sum_i [2 < a > - a_i] |i\rangle$$

- Applying $G = [2|\psi\rangle\langle\psi| - I]$ makes $|x^*\rangle$ have amplitude above the mean while all other states have an amplitude below the mean
Implementation of the Algorithm

1. Use the Quirk simulator (https://algassert.com/quirk)

2. Initialization
   • Initialize the qubits in a superposition with $N^{-1/2}$ normalization (.25 for N=4)

3. Oracle
   • Implement the Oracle function

4. Amplification
   • Phase flip the amplitude about the average amplitude
   • Inverting the target state amplitude while keeping all other amplitudes unchanged causes the target amplitude to increase while all other states decrease

5. Measurement
   • Perform a readout of the final qubit states
Initialization of 4 Qubit System

• Quantum computing platforms are normally initialized as $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

• The procedure is to apply Hadamard gates to each qubit

\[
\begin{align*}
|q_0\rangle & \quad \text{H} \\
|q_1\rangle & \quad \text{H} \\
|q_2\rangle & \quad \text{H} \\
|q_3\rangle & \quad \text{H}
\end{align*}
\]
Possible Oracle Configurations with 4 Qubits

• With 4 qubits there are 16 possible oracle configurations

• States are initialized on QC platforms in the $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ state

• Recall that the Z gate has the matrix representation $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

• Recall that the T gate has the matrix representation $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$
The Toffoli gate is a 3-bit gate, which is universal for classical computation. If the first two bits are in the state $|1\rangle$, it applies a Pauli-X (NOT) on the third bit, otherwise the state is left unchanged.
Properties of Toffoli Gates

• Toffoli Gate is a reversible gate (i.e. $U_T^{-1}U_T=I$) or

• Toffoli gate is used to replace a classical circuit with the equivalent reversible gate

• Two bits are control bits (|a> and |b>) and target bit |c> is flipped as per the truth table

  $$(a, b, c) \rightarrow (a, b, c \oplus ab) \rightarrow (a, b, c)$$

• Toffoli gate and be used to simulate a NAND Gate
Toffoli Gate Truth Table and Matrix

<table>
<thead>
<tr>
<th>INPUT</th>
<th>OUTPUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 
\end{pmatrix}$$

X Gate
Pauli $$\sigma_x$$ rotation matrix
4 Qubit Control-Z Gate

• Within the Oracle there is multi-connected gate that as similar characteristics to the Toffoli Gate
CCC-Not Gate Construction

• It should be possible to construct a CCC-Not gate using an array of CC-Not gates combined with a sequence of 1 bit gates

• Any 4-bit gate that has 3 controlled and one unitary transformation can be represented* as where V is tuned such that $V^4 = U$

Amplification

• This stage performs an inversion of the amplitudes about the average

• From the initialization step the amplitude is .25 (N^{-1/2} where N=4)

• \( \text{Avg}_{\text{amp}} = [(15)(0.25)+(-0.25)]/16 = 0.21875 \)

• \( \text{Ind}_{\text{amp}} = 0.21875-(-0.25) = 0.46875 \)

• The inversion of the \( \text{Ind}_{\text{amp}} \) about the average is

  \[ 0.21875 + 0.46875 = 0.6875 \]

• The amplitudes of the other states are 0.21875 - 0.25 = -0.03125

• The other states have a value 0.21875 - 0.03125 = 0.1875
Amplification Gate Structure
Quantum Computing Circuits for |0000> Oracle

CCC-Not Gate Structure

Amplification
Final Measurement
Final Measurement
Final Measurement

Amplitude of $|0010\rangle$
val: $-0.68750 - 0.00000i$
mag$: 47.2655\%, phase: -180.00°

Local wire states (Chance/Bloch)

Final amplitudes
Final Measurement