Quantum Computing

Dr. Andrés Gómez
Andres.gomez.tato@cesga.es
Apr. 2019
Lecture 3: Basic algorithms

- Quantum Parallelism
- Quantum Fourier Transform
- Amplitude amplification
- Phase estimation
Quantum Paralelism

- The idea behind quantum paralelism is that you can apply a function to all the states in a superposition in just one step

- Let \( U_f \) an operator that implements the function \( f \) such that:

\[
U_f |x, y> = |x, f(x) \oplus y>
\]

- If we choose \( y=|0> \):

\[
U_f |x, 0> = |x, f(x)>
\]

- And because \( U_f \) is linear, we can apply to any superposition. For example, to the result states of Walsh-Hadamard operator:

\[
W = H^\otimes n \Rightarrow \\
U_f(W|0> \otimes |0>) = U_f\left(\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i> \otimes |0>\right) = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i> |f(i)>
\]

- BUT. All the solutions are entangled and we can get only one for each measurement
Toffoli gate implement the classical AND operation on 2 bits

\[
\begin{array}{ccc}
\ket{x} & \ket{y} & \ket{x \& y} \\
0 & 0 & 0 \\
1 & 0 & 0 \\
0 & 1 & 0 \\
1 & 1 & 1 \\
\end{array}
\]

So, \( Toffoli(W|00 \rangle \otimes |0 \rangle) = \frac{1}{2} (|000 \rangle + |010 \rangle + |100 \rangle + |111 \rangle) \)
Quantum Subroutines

\[ |0 \rangle \xrightarrow{W} |\psi_x \rangle \]

\[ |0 \rangle \xrightarrow{X \ H} \]

Ancilla or temporary qubit.
Exercise: Quantum Parallel Programming
When on a state $|\psi > = \sum_{i=0}^{N-1} a_i |i >$, a superposition, one unitary gate is applied to only a one single qubit, all the amplitudes of state $|\psi >$ can be affected.

For example:

\[
(I \otimes H) \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 \\ a_1 - a_2 \\ a_3 + a_4 \\ a_3 - a_4 \end{pmatrix}
\]
Exercise: Applying Quantum Parallelism

OPEN QISKIT/FIND_EDGE NOTEBOOK
Discrete Fourier Transform of \( a: [0, \ldots, N-1] \): 
\[
A(x) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} a(k)e^{2\pi i \frac{kx}{N}}
\]

Classical Fast Fourier Transform assumes that \( N = 2^n \)

Quantum Fourier Transform (QFT):
- Amplitudes \( a(x) \) of state \( |x> \) is a function of \( x \)
- So \( \text{QFT}(\sum_x a(x) |x>) = \sum_x A(x) |x> \)
- If \( a(x) \) is a function of period \( r \) (\( r \) power of 2), \( A(x) \) are zero except for states multiple of \( N/r \)
Quantum Fourier Transform

- \[ \text{QFT}(|k>) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{i\frac{2\pi k x}{N}} |x> \]

- The way of calculate QFT is recursive as in classical FFT.

- If \( R_m = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^m}} \end{bmatrix} \)
Exercise: Programming QFT

OPEN QISKIT/QFT NOTEBOOK
Quantum computing is probabilistic.

Want to maximize the opportunity of measuring the right answer in one shot.

This means increase probability of the solutions. If possible, to 1.

Solution: Amplitude amplification.

If $U_g$ is the transformation on $n$ qubits ($N=2^n$ states) that solve the problem, apply $k$ times the transformation $DU_g$

- What is $U_g$?
- What is $D$?
- How large is $k$?
U_g is a transformation that changes the sign to the solutions when applied to the superposition of all states.

\[ U_g(\ldots) = \ldots \]

D is the Grover’s operator (or difusor operator) that inverts about the average.

\[ D(\ldots) = \ldots \]

If \(|G|\) is the probability of \(|x>\) if being a Good result, the number of time to apply the algorithm is:

\[ k \approx \frac{\pi}{4} \sqrt{\frac{N}{|G|}} \]
Grover’s operator

\[
D = \begin{bmatrix}
\frac{2}{N} - 1 & \frac{2}{N} & \frac{2}{N} \\
\frac{2}{N} & \frac{2}{N} - 1 & \frac{2}{N} \\
\vdots & \vdots & \ddots & \vdots \\
\frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} - 1
\end{bmatrix} = -WS_0^\pi W
\]

\(W\) is the \textbf{Walsh-Hadamard} transform:

\[
H \otimes^n = H \otimes H \otimes ... \otimes H \otimes H
\]

\(S_0^\pi\) is the phase shit by \(\pi\) of the baseis vector \(|0\rangle\):

\[
S_0^\pi = \begin{bmatrix}
-1 & 0 & \cdots & 0 \\
0 & 1 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 1
\end{bmatrix} = X \otimes^n C_n^{[0,n-1]}(Z) X \otimes^n
Exercise: Grover’s algorithm
Phase estimation

- Let $U$ an unitary operation.

- Let $|u\rangle$ an eigenvector of $U$ such that (which $0 < \phi < 1$):
  \[ U|u\rangle = e^{i2\pi\phi}|u\rangle \]

- Phase algorithm tray to estimate $\phi$ applying controled unitaries gates $U^{2n}$, $n \in \{0,1,...,t\}$, being $\frac{1}{2^t}$ the precission of the approximation.

- The algorithm use $t$ qubits to calculate the phase and $m$ qubits to represent $|u\rangle$. 

![Diagram](image.png)
Phase Kickback

\[ \frac{1}{\sqrt{2}} (|0\rangle + e^{i\varphi} |1\rangle) \]
Phase estimation

Steps:
- Allocate quantum register for n qubits ($q_n$).
- Allocate a second quantum register for m qubits ($q_m$).
- Initialize $q_m$ to $|u\rangle$.
- Apply Walsh-Hadamard to $q_n$.
- Apply Controlled($U^{2n}, n$) on $|u\rangle$ for all n qubit in $q_n$.
- Make QFT$^{-1}$ on $q_n$.
- Measure $q_n$.
- From the measurements (as integers) calculate $\phi$.

\[
\begin{align*}
|0\rangle & \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + e^{i2\pi 0\phi}|1\rangle) \\
|0\rangle & \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + e^{i2\pi 1\phi}|1\rangle) \\
|0\rangle & \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + e^{i2\pi 2\phi}|1\rangle) \\
|0\rangle & \xrightarrow{X R_{z\phi}^{20} R_{z\phi}^{21} R_{z\phi}^{22}} |1\rangle
\end{align*}
\]
Exercise: Phase Estimation

OPEN PROJECTQ/PHERE_ESTIMATION NOTEBOOK
Shor’s Factoring Algorithm

AC: Abstract Concurrent Architecture. Supports ccNOT, concurrency and gate operands any distance apart
NTC: Neighbor-only, Two-qubit-gate, Concurrent architecture. Qbits in a line. Not ccNOT. Only two-qubits gates. Only neighbor qubits can operate
BCDP: Beckman, Chari, Devabhaktuni, and Preskill’s algorithm

Exercise: Shor’s algorithm
Thanks!
Questions?