Lecture 39

Quantum Algorithms Again!
Where We Are

- Doing our projects!
- Using problem sets to solidify our knowledge base
- Following class lectures
- Seeing examples in class illustrate how to apply QM (the QM postulates) to problems
A set of quantum postulates

- There is a (normalized) state vector
- Unitary evolution of the state vector is generated by a Hamiltonian
- Measurements give eigenvalues of Hermitian operators and place the system in the associated eigenstate with its probability
- A composite state vector is represented in a basis that is an outer product of the basis sets of its component state vectors
The Five December Lectures

• Shor’s algorithm with all the trimmings
• The Q beamsplitter and teleportation using an interferometer
• Problems Set 6
• Factoring $15=5$ times 3 using Q interference
• HW problems and exam review
Last Monday’s Topics

• Quick review thru Q computing model
• Quick review of last week through the Deutsch Jozsa algorithm
• The quantum FFT
• Quantum phase estimation
Single Qubit Quantum Logic

X → S
Y → T
Z → H
1 and N Qubit Quantum Logic

\[ |00...0> \xrightarrow{H^n} \frac{|00...0> + |11...1>}{\sqrt{2^n}} \]

Computational basis

\[ |j_1j_2...j_n> / \sqrt{2^n} \]
Two Qubit Quantum Logic

\[ \text{CNOT} \quad |x,x \ (XOR) \ y> \]

\[ x \quad y> \]

\[ y \quad |x,y> \]

\[ |x,x \ (XOR) \ y> \quad \text{control} \]

\[ x \quad y \]

\[ |x,y> \quad \text{XOR} \quad |x,x \ (XOR) \ y> \]
A Usual Q computer Model

Unitarily Evolve Data Registers

Target Registers

Control "Interference"
$1+1$ and $n+1$ Qubit Quantum Logic

$|x,x(XOR)y\rangle$
Topics from Two Monday’s Ago

- The $U_f$ gate for 1+1 and n+1 inputs
- Quantum parallelism and quantum interference
- Deutsch’s algorithm
- The Deutsch-Jozsa algorithm
- The quantum FFT
- Quantum phase estimation
Uf Quantum Logic Gates

\begin{align*}
\text{Uf} & \quad |x,y (\text{XOR}) f(x)> \\
\langle x \rangle \quad \text{Uf} & \quad ||x>,y (\text{XOR}) f(|x>)>
\end{align*}
Quantum Parallelism on 1+1 Qubits

2 functional evaluations, sort of
Quantum Parallelism on $n+1$ Qubits

$H^n |0\rangle$ $\rightarrow$ $\langle x|, 0 \rangle$ $\rightarrow$ $\langle x|, 0 \rangle (\text{XOR}) f(|x\rangle)$ $\rightarrow$ $\langle x|, f(|x\rangle)$

$2^n$ functional evaluations, sort of
Quantum Interference on 1+1 Qubits: Deutsch Algorithm

Interference tells us if $f$ changes sign
Quantum Interference on n+1 Qubits: Deutsch-Jozsa Algorithm

\[ U_f \]

Qubit |0…0> is zero or one depending on edge in \( f(|x>) \) telling us if \( f \) changes sign
Today’s Topics

- Shor’s Algorithm
- The discrete FFT
- The quantum FFT and $R_k$ gate
- $n+m$ logic and $U^{(2^i)}$ gate
- Quantum phase estimation
Shor’s Algorithm with $n+m$ bits

$|0\rangle$'s

$H^\text{n}$

Bit by bit targeting

$n$ Oracle queries

$m$

$|u\rangle$

$U^{(2^i)}$

$n$ bit IQFT

$|\phi\rangle$

$U|u\rangle = \exp[2\pi i \phi]|u\rangle$
The Quantum DFT (QFT)

\[ |j_1j_2...j_n\rangle ----> \]
\[ |0\rangle + \exp[2 \pi i 0.j_n]|1\rangle \]
\[ (|0\rangle + \exp[2 \pi i 0.j_{(n-1)}j_n]|1\rangle) \]
\[ .................................................. \]
\[ ..(|0\rangle + \exp[2 \pi i 0.j_1j_2...j_n]|1\rangle)/2^{(n/2)} \]

Subdefinitions:
1) \( j = j_1 2^n + j_{(2)} 2^{(n-1)} + ... + j_n 2^0 \)
2) \( 0.j_1j_2 = j_1/2^1 + j_2/2^4 \)
3) \( 0.j_1j_2...j_n = j/2^{(n+1)} \)
A Three bit QFT
Some Identities

\[ |j_1\rangle = \exp[2 \pi i j_1/2^1]|1\rangle \]

\[ |j_2\rangle = \exp[2 \pi i j_2/2^1]|1\rangle \]

\[ |j_1/2^1+j_2/2^2\rangle = \exp[2 \pi i (j_1/2^1+j_2/2^2)]|1\rangle \]

Using \[ j = j_{12}^n + j_{22}^{(n-1)} + \ldots + j_{nn} \]
$R_k$ Gates

where $|in\rangle = |j\rangle = |j_1j_2\ldots j_n\rangle$

$|j_{k-1}\rangle = |0\rangle$  $\xrightarrow{H} |0\rangle + \exp[\text{phase}] |1\rangle$

Phase = $2\pi i j_k/2^k$

$|j_k\rangle$

where $j = j_1 2^n + j_2 2^{(n-1)} + \ldots + j_n 2^0$
$U^{(2^k)}$ Gates

$|j_k> + \exp[\text{phase}] |1> \quad \text{phase}=2 \pi i 2^k \phi$

where $|\text{in}> = |j_1 j_2 \ldots j_n>$
Phase Generation

\[ |0> \text{'s} \rightarrow H^n \rightarrow \text{Bit by bit targeting} \rightarrow |\exp[2 \pi i \phi]\rangle \]

where

\[ \phi = \phi_1 2^n + \phi_2 2^{(n-1)} + \ldots + \phi_1 2^0 \]

\[ U|u> = \exp[2 \pi i \phi]|u> \]
IQFT

|exp[2 pi i phi]> → n bit IQFT → |phi>
Shor’s Algorithm with $n+m$ bits

- $n$-bit $|u>$
- $m$-bit $|u>$
- $H^n$
- Bit by bit targeting
- $U^{(2^i)}$
- $n$ Oracle queries
- $U|u> = \exp[2\pi i \phi]|u>$
- $|\phi>$
- $n$ bit IQFT