October 11, 2002
CS 294-4 Quantum Computing
Professor Umesh Vazirani
Scribe Eugene Shvets

Quantum Fourier Transform (QFT)

Quantum Computation is all about QFT. Why? Need unitary transformations that can be decomposed efficiently (MEANING?). There only a few types of such non-trivial transformations, and FT is an important class of them.
FT lie in the heart of mathematical apparatus of quantum mechanics.

We will discuss Fourier transforms over group Z_m. Note $w = e^{\frac{2pi}{m}}$.
Classically, Fourier Transform is given by the following equation:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \dots & w^{jk} & \vdots \\ 1 & & \ddots & \vdots \\ 1 & \cdots & \cdots & w^{(m-1)(m-1)} \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ \vdots \\ a_{m-1} \end{pmatrix} = \begin{pmatrix} \hat{a}_0 \\ \vdots \\ \vdots \\ \hat{a}_{m-1} \end{pmatrix}$$

, where $j,k = 0 \ldots m-1$.

Normally matrix-vector multiply involves $O(m^2)$ operations. However, exploiting the structure of the Vandermonde matrix, we can cut the complexity to $O(m \log m)$. The algorithm is called Fast Fourier Transform and is discussed below.

Quantumly, the m-dimensional complex vector is the state of $\log m$ qubits. The QFT is the mapping

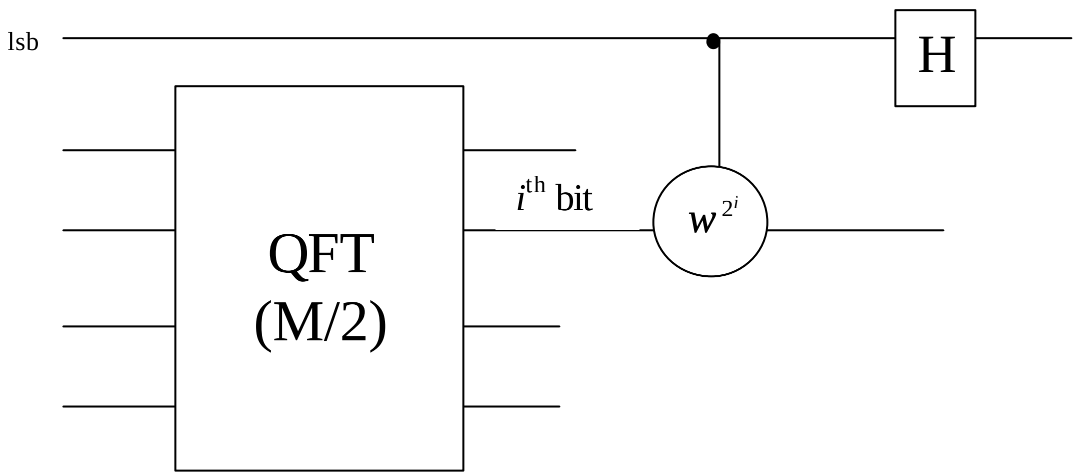
$$\sum_j^{m-1} a_j \left| j \right\rangle \xrightarrow{QFT} \sum_j^{m-1} \hat{a}_j \left| j \right\rangle$$

Advantage: QFT can be realized with a circuit of size $O(\log^{O(1)} m)$, a speedup over FFT's $O(m \log m)$.

Disadvantage: Coefficients $\hat{a}_j$ are quantum states and thus are not readily accessible. All we get is **Fourier Sampling**. If we measure, we get $\left| j \right\rangle$ with probability $\left| \hat{a}_j \right|^2$.

Building QFT circuit of polylog size

Describe QFT's divide and conquer idea here



Properties of Quantum Fourier Transforms

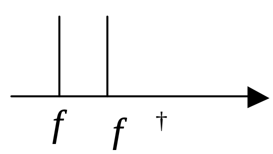
1. F **is unitary**: $FF^\dagger = F^\dagger F = I$.
Proof. Note that $(j,k)^{\text{th}}$ entry of $FF^\dagger$ is

$$\frac{1}{m}\sum_l w^{jl} w^{-jk} = \frac{1}{m}\sum_l w^{l(j-k)} = \begin{cases} 1 \text{ if } j = k \\ 0 \text{ if } j \neq k \end{cases}$$

(geometric series with $a = w^{j-k}$

sums to $\frac{a^m - 1}{a-1} = \frac{1-1}{a-1} = 0$, since $w = \sqrt[m]{1}$.

2. **Pick out similarities**
Consider $|f\rangle = \sum_j a_j |j\rangle$ and $|f^+\rangle = \sum_j a_j | j+1\rangle$. How do $|f\rangle$ and $|f^+\rangle$ differ? Of course, there could be no overlap. So it's hard for us to know that $f \approx f^\dagger$.



Consider the respective QFTs:
$|f\rangle \to \sum_j \hat{a}_j |j\rangle$ and $|f^\dagger\rangle \to \sum_j \hat{b}_j |j\rangle$. The beauty of QFT is that $|\hat{a}_j| \approx |\hat{b}_j|$!

3. **Pick out symmetries**

talk how FT is concentrated for uniform initial superposition and how it can be used for period finding.