Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley

Lecture 9: Quantum Fourier Transform

Overview

$$H^{\otimes 3} = \frac{1}{\sqrt{8}}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

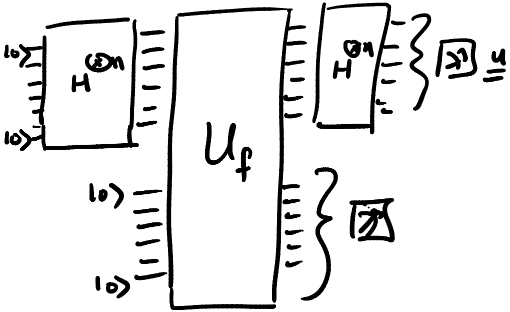
$$QFT_8 = \frac{1}{\sqrt{8}}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix}$$

$x^8 = 1 \qquad \omega = \cos\frac{2\pi}{8} + i\sin\frac{2\pi}{8} = e^{\frac{2\pi}{8}i}$

$1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6, \omega^7.$

Simon's Algorithm:

$f(x) = f(x \oplus \underline{s})$

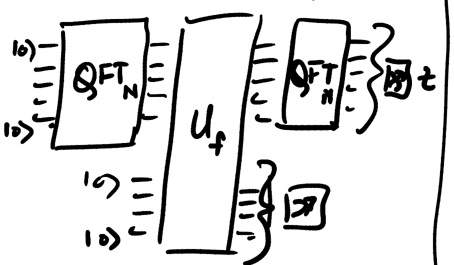


$u \cdot s = 0$

Period Finding:

$f(x) = f(x + \underline{r})$

$N = 2^n$



t allows us to reconstruct r.

1. QFT_N
2. Properties of QFT_N
3. Quantum ckt.

* Period finding.
* Factoring.

* Course Notes.
* Reference books.

- “Algorithms” by Dasgupta, Papadimitriou, Vazirani

  www.cs.berkeley.edu/~vazirani/algorithms.html

  ✓Chapter 1: Modular Arithmetic
  ✓Chapter 2 (2nd half): Fast fourier transform
  ✓Chapter 10: Quantum factoring.

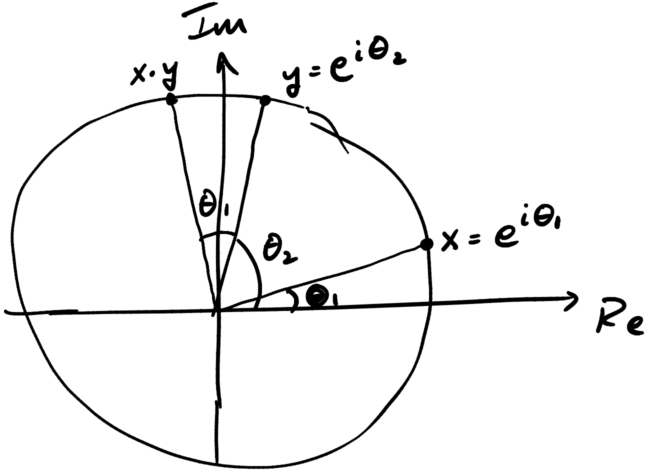
Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley

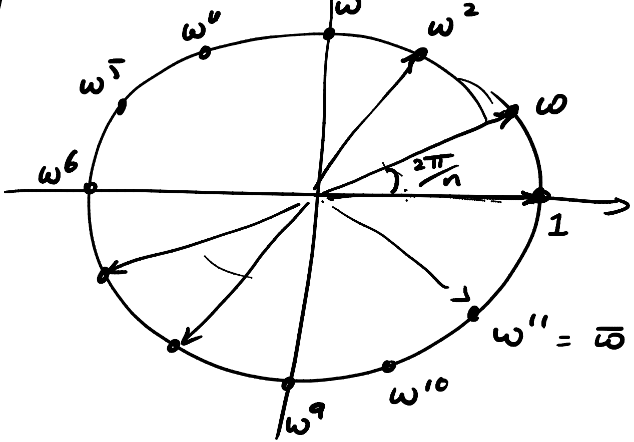
Lecture 9: Quantum Fourier Transform

n-th roots of unity

$$x = \cos\theta_1 + i\sin\theta_1 = e^{i\theta_1}$$
$$y = \cos\theta_2 + i\sin\theta_2 = e^{i\theta_2}$$
$$x \cdot y = (\cos\theta_1 + i\sin\theta_1)(\cos\theta_2 + i\sin\theta_2)$$
$$= \cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2) = e^{i(\theta_1+\theta_2)}$$



$x^n = 1.$



$$1 + \omega + \omega^2 + \cdots + \omega^{n-1} = 0$$

$$1 + \omega^j + \omega^{2j} + \cdots + \omega^{(n-1)j} = \begin{cases} 0 & j \neq 0 \\ n & j = 0 \end{cases}$$

"

$$\frac{\omega^{nj} - 1}{\omega^j - 1} = 0$$

$$\bar{\omega} = \cos\frac{2\pi}{n} - i\sin\frac{2\pi}{n} = \cos\frac{-2\pi}{n} + i\sin\frac{-2\pi}{n}$$
$$= \omega^{n-1} = \frac{1}{\omega} = \omega^{-1}$$

Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley

Lecture 9: Quantum Fourier Transform

QFT_N

Discrete Fourier transform

$$QFT_N = \frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix}$$

$\omega = e^{2\pi i/N} = \cos\frac{2\pi}{N} + i\sin\frac{2\pi}{N}$. eg $N=8$ $\omega = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$

$$QFT_N = \frac{1}{\sqrt{N}} \begin{array}{c} 0 \\ 1 \\ \vdots \\ j \\ \vdots \\ N-1 \end{array} \overset{\begin{array}{cccccc} 0 & 1 & \cdots & k & \cdot & N-1 \end{array}}{\begin{pmatrix} & & & & & \\ & & & & & \\ & & & & & \\ & & & \omega^{jk} & & \\ & & & & & \\ & & & & & \end{pmatrix}}$$

$\boxed{QFT_2}$

$\underline{\underline{QFT_4}}$

$\omega = e^{\frac{2\pi i}{4}} = i$

$1, i, i^2, i^3$

$i^2 = -1$, $i^3 = -i$

$$QFT_4 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix}$$

$\alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle + \alpha_3|3\rangle.$

$|2\rangle \xrightarrow{QFT_4} \frac{1}{2}|0\rangle - \frac{1}{2}|1\rangle + \frac{1}{2}|2\rangle - \frac{1}{2}|3\rangle$

$\omega = e^{2\pi i/N}$ $\quad \omega^N = 1.$

ω^M $\quad M = Q\cdot N + \underline{R}.$

$= \omega^{QN+R}$ $\quad 0 \le R \le N-1$

$= \underline{\underline{\omega^{QN}}} \cdot \omega^R = \omega^R.$

$R \equiv M \pmod N$

$|00\rangle, |01\rangle, |10\rangle, |11\rangle$

$= |0\rangle, |1\rangle, |2\rangle, |3\rangle$

Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley

Lecture 9: Quantum Fourier Transform

QFT_N

Discrete Fourier transform

$O(N^2)$ time.

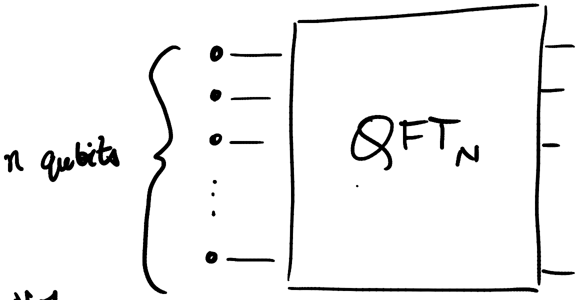
FFT $O(N \log N)$ time.

$$QFT_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1} \end{pmatrix}$$

exponential improvement!!

$N = 2^n \qquad n = \log N$

$O(n^2) = O(\log^2 N)$



$\sum_{i=0}^{N-1} \alpha_j |i\rangle \qquad \sum \beta_j |j\rangle$

Measure: j w.p. $|\beta_j|^2$.

Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley

Lecture 9: Quantum Fourier Transform

Properties

Convolution - Multiplication.

$$QFT_N = \frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1} \end{pmatrix}$$

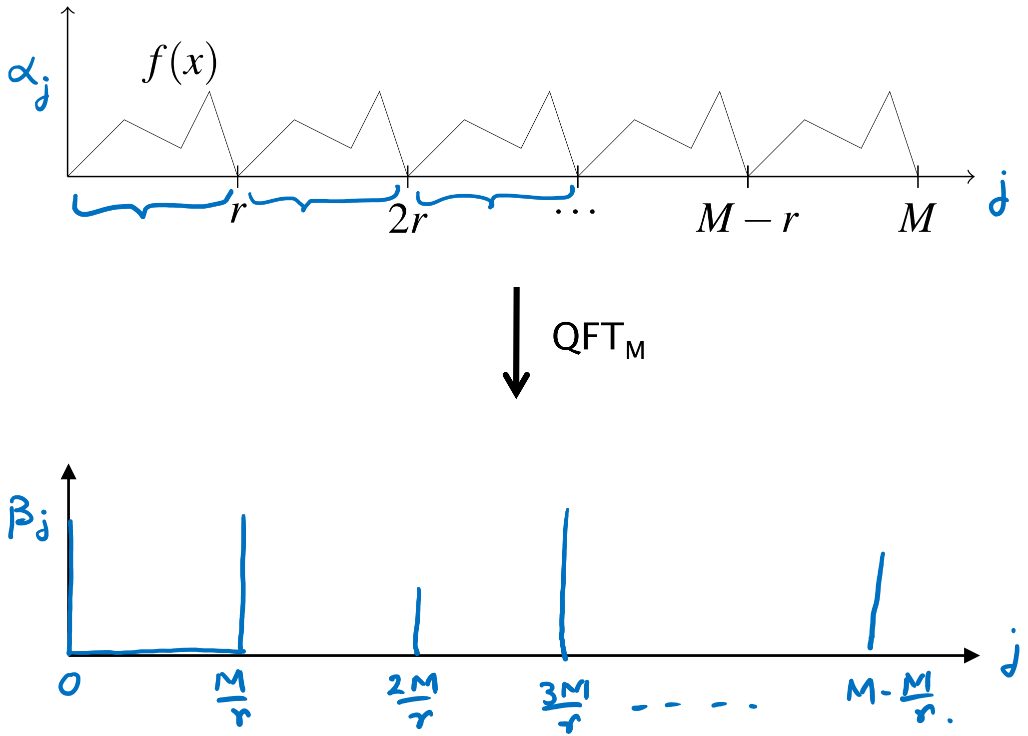
see j w.p. $|\beta_j|^2$

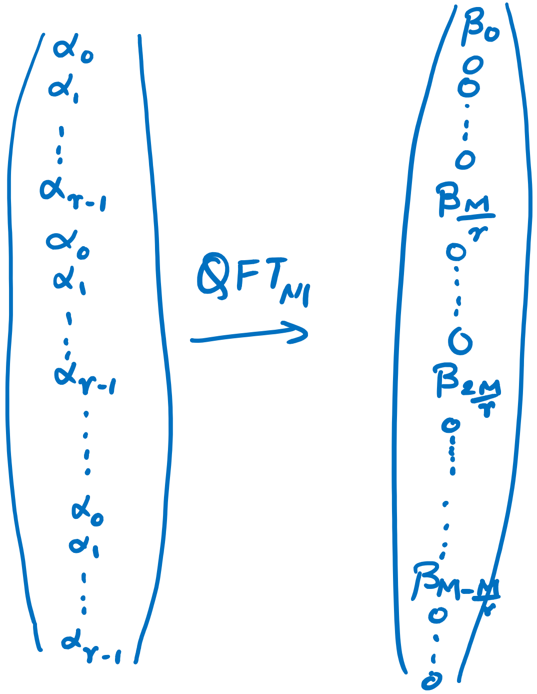
$$\alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{N-1}|N-1\rangle \xrightarrow{QFT_N} \beta_0|0\rangle + \beta_1|1\rangle + \cdots + \beta_{N-1}|N-1\rangle$$

$$QFT_N = \frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix} \begin{pmatrix} \alpha_N \\ \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \omega \beta_1 \\ \omega^2 \beta_2 \\ \vdots \\ \omega^{N-1} \beta_{N-1} \end{pmatrix}$$

see j w.p. $|\beta_j|^2$

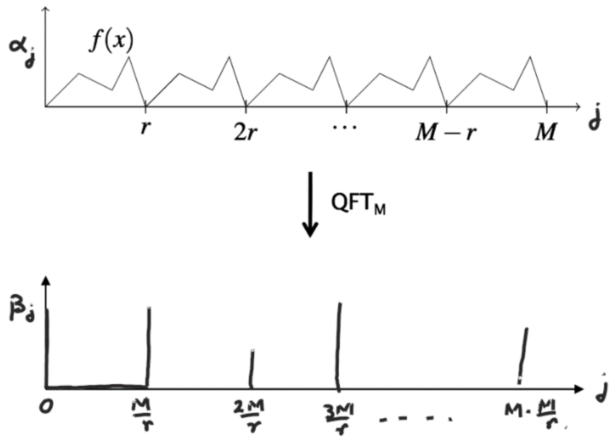
Fourier transform





r divides M

Fourier transform

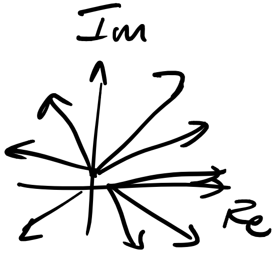


$$\sqrt{\frac{r}{M}}\sum_{j=0}^{\frac{M}{r}-1}|jr\rangle \xrightarrow{QFT} \sum_{j=0}^{M-1}\underline{\underline{\beta_j}}\,|j\rangle$$

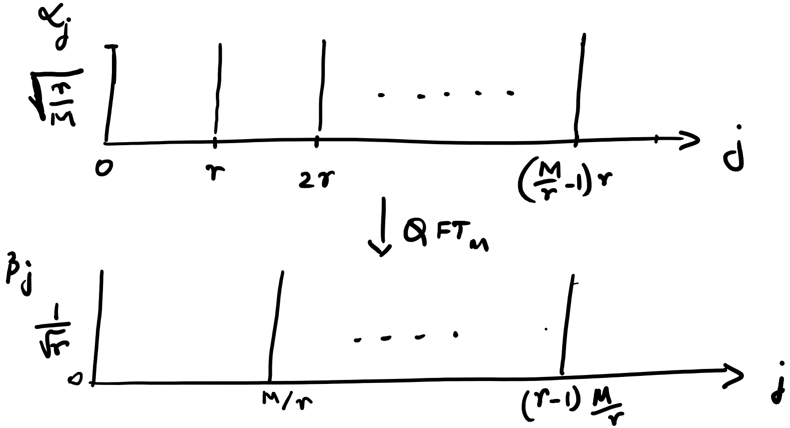
$$\beta_{k\frac{M}{r}} = ?$$

$$\beta_{\frac{kM}{r}} = \sum_{j=0}^{\frac{M}{r}-1}\sqrt{\frac{r}{M}}\times\frac{1}{\sqrt{M}}\times\underline{\underline{\omega^{j\cancel{r}\times\frac{kM}{\cancel{r}}}}} = 1.$$

$$= \frac{\cancel{M}}{r}\times\frac{\sqrt{r}}{\cancel{M}} = \frac{1}{\sqrt{r}}$$



$$\beta_j = ? \qquad j \neq \frac{kM}{r}$$
$$= 0$$



$$\sqrt{\frac{r}{M}}\begin{pmatrix}1\\0\\\vdots\\0\\1\\0\\\vdots\\0\\1\\\vdots\\0\end{pmatrix}\begin{matrix}\uparrow\\r\\\downarrow\end{matrix} \xrightarrow{QFT_M} \frac{1}{\sqrt{r}}\begin{pmatrix}1\\0\\\vdots\\0\\1\\0\\\vdots\\1\\0\\\vdots\end{pmatrix}\begin{matrix}\uparrow\\M/r\\\downarrow\end{matrix}$$