Lecture #8 (Quantum Fourier transform) **DRAFT** Notes by Boris Bukh
30 September 2004
Fall 2004 Lecture 8

Fourier transform on $\mathbf{Z}_N$

Let f be a complex-valued function on $\mathbf{Z}_N$. Then its Fourier transform is

$$\hat{f}(t) = \frac{1}{\sqrt{N}} \sum_{x \in \mathbf{Z}_N} f(x) w^{xt}$$

where $w = \exp(2\pi i/N)$. Let B_1 be the standard basis for $\mathscr{C}^{Z_N}$ consisting of vectors $f_i(j) = \delta_{i,j}$. In the standard basis the matrix for the Fourier transform is

$$FT_N = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & w^3 & \cdots & w^{N-1} \\ 1 & w^2 & w^4 & w^6 & \cdots & w^{2N-2} \\ 1 & w^3 & w^6 & w^9 & \cdots & w^{3N-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w^{N-1} & w^{2N-2} & w^{3N-3} & \cdots & w^{(N-1)(N-1)} \end{pmatrix}$$

where i, j'th entry of FT_N is w^{ij}.

Classical fast Fourier transform

Straightforward multiplication of the vector f by FT_N would take $\Omega(N^2)$ steps because multiplication of f by each row requires N multiplications. However, there is an algorithm known as fast Fourier transform (FFT) that performs Fourier transform in $O(N \log N)$ operations.

In our presentation of FFT we shall restrict ourselves to the case $N = 2^n$. Let B_2 be a basis for $\mathscr{C}^{\mathbf{Z}_N}$ consisting of vectors

$$f_i(j) = \begin{cases} \delta_{2i,j}, & i \in \{0, 1, \ldots, N/2 - 1\}, \\ \delta_{2i-N+1,j}, & i \in \{N/2, N/2+1, \ldots, N-1\}, \end{cases}$$

i.e., the vectors of the standard basis sorted by the least-significant bit. Then as a map from B_2 to B_1 the Fourier transform has the matrix representation

$$\begin{array}{c} \text{bit \#} \\ j \\ j+N/2 \end{array} \quad \begin{array}{c} \begin{array}{cc} 2k & 2k+1 \end{array} \\ \left(\begin{array}{c|c} w^{2jk} & w^{2jk} w^j \\ \hline w^{2jk} & w^{2jk} w^j \end{array} \right) \end{array} = \begin{pmatrix} FT_{N/2} & w^j FT_{N/2} \\ FT_{N/2} & -w^j FT_{N/2} \end{pmatrix}.$$

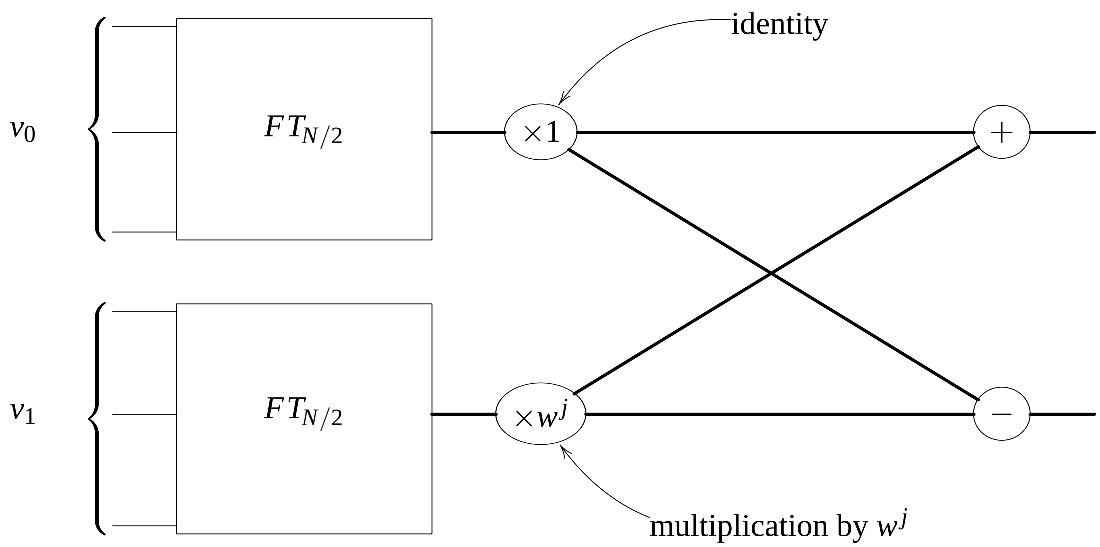

Figure 1: A circuit for classical fast Fourier transform

Hence,

$$\left(\begin{array}{c|c} w^{2jk} & w^{2jk}w^j \\ \hline w^{2jk} & w^{2jk}w^j \end{array}\right)\left(\begin{array}{c} v_0 \\ \hline v_1 \end{array}\right) = \begin{pmatrix} FT_{N/2}v_0 + w^j FT_{N/2}v_1 \\ FT_{N/2}v_0 - w^j FT_{N/2}v_1 \end{pmatrix}.$$

This representation gives a recursive algorithm for computing the Fourier transform in time $T(N) = 2T(N/2) + O(N) = O(N \log N)$. As a circuit the algorithm can be implemented as

Quantum Fourier transform

Let $N = 2^n$. Suppose a quantum state α on n qubits is given as $\sum_{j=0}^{N-1} \alpha_j \left|j\right\rangle$. Let the Fourier transform of ϕ be $FT_N\left|\phi\right\rangle = \sum_{j=0}^{N-1} \beta_j \left|j\right\rangle$ where

$$FT_N \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1} \end{pmatrix}.$$

The map $FT_N = \left|\alpha\right\rangle \mapsto \left|\beta\right\rangle$ is unitary (see the proof below), and is called the quantum Fourier transform (QFT). A natural question arises whether it can be efficiently implemented quantumly. The answer is that it can be implemented by circuit of size $O(\log^2 N)$. However, this does not constitute an exponential speed-up over the classical algorithm because the result of quantum Fourier transform is a superposition of states which can be observed, and any measurement can extract at most $n = \log N$ bits of information.

A quantum circuit for quantum Fourier transform is where R_K is the controlled phase shift by angle

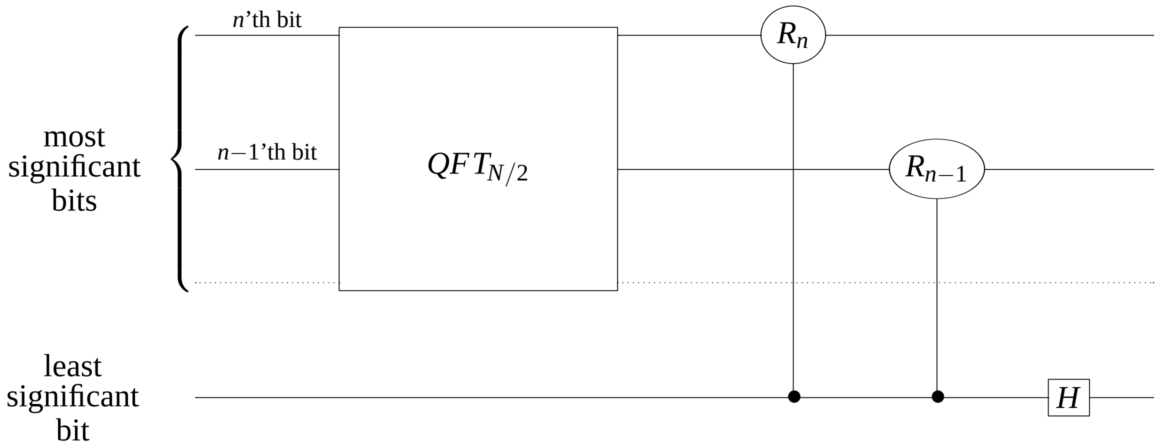

Figure 2: Circuit for quantum Fourier transform

$2\pi/2^K$ whose matrix is

$$R_K = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{2\pi/2^K} \end{pmatrix}.$$

In the circuity above the quantum Fourier transform on $n-1$ bits corresponds to two Fourier transforms on $n-1$ bits in the figure 1. The controlled phase shifts correspond to multiplications by w^j in classical circuit. Finally, the Hadamard gate at the very end corresponds to the summation.

Properties of Fourier transform

- FT_N is unitary. Proof: the inner product of the i'th and j'th column of FT_N where $i \neq j$ is

$$\frac{1}{N}\sum_{k\in\mathbf{Z}_N} w^{ik}\overline{w^{jk}} = \frac{1}{N}\sum_{k\in\mathbf{Z}_N} w^{ik-jk} = \frac{1}{N}\sum_{k\in\mathbf{Z}_N} (w^{i-j})^k = \frac{1}{N}\frac{w^{N(i-j)}-1}{w^{i-j}-1} = \frac{1}{N}\frac{1-1}{w^{i-j}-1}$$

  which is zero because $w^{i-j} \neq 1$ due to $i \neq j$. The norm of i'th column is

$$\sqrt{\frac{1}{N}\sum_{k\in\mathbf{Z}_N} w^{ik}\overline{w^{ik}}} = \sqrt{\frac{1}{N}\sum_{k\in\mathbf{Z}_N} 1} = 1.$$

- FT_N^{-1} is FT_N with w replaced by w^{-1}. Proof: since FT is unitary we have $F_N^{-1} = FT_N^*$. Since FT_N is symmetric and $\bar{w} = w^{-1}$, the result follows.

- Fourier transform sends translation into phase rotation, and vice versa. More precisely, if we let the translation be $T_l \colon |x\rangle \mapsto |x+l \pmod N\rangle$ and rotation by $P_k \colon |x\rangle \mapsto w^{kx}|x\rangle$, then $FT_N P_l P_k = P_l T_{-k} FT_N$. Proof: by linearity it suffices to prove this for a vector of the form $|x\rangle$. We have

$$FT_N T_l P_k|x\rangle = FT_N w^{kx}|x+l \pmod N\rangle = \frac{1}{\sqrt{N}} w^{kx} \sum_{y\in\mathbf{Z}_N} w^{y(x+l)}|y\rangle$$

and by making the substitution $y = y' - k$

$$= \frac{1}{\sqrt{N}} w^{y'x} \sum_{y' \in \mathbf{Z}_N} w^{(y'-k)l} \left| y' - k \right\rangle = \frac{1}{\sqrt{N}} P_l T_{-k} \sum_{y' \in \mathbf{Z}_N} w^{xy} \left| y' \right\rangle$$
$$= P_l T_{-k} FT_N \left| x \right\rangle.$$

Corollary: FT_N followed by Fourier sampling is equivalent to $T_l FT_N$ followed by Fourier sampling.

- Suppose $r \mid N$. Let $\left|\phi\right\rangle = \frac{1}{\sqrt{N/r}} \sum_{j=0}^{N/r-1} \left| jr \right\rangle$. Then $FT_N \left|\phi\right\rangle = \frac{1}{\sqrt{r}} \sum_{i=0}^{r-1} \left| i\frac{N}{r} \right\rangle$. Proof: the amplitude of $\left| i\frac{N}{r} \right\rangle$ is

$$\frac{1}{\sqrt{N}} \frac{1}{\sqrt{N/r}} \sum_{j=0}^{N/r-1} w^{(jr)(iN/r)} = \frac{\sqrt{r}}{N} \sum_{j=0}^{N/r-1} 1 = \frac{1}{\sqrt{r}}$$

Since FT_N is unitary, the norm of $FT_N \left|\phi\right\rangle$ has to be equal to the norm of $\left|\phi\right\rangle$ which is 1. However the orthogonal projection of $FT_N \left|\phi\right\rangle$ on the space spanned by vectors of the form $\left| i\frac{N}{r} \right\rangle$ has norm 1. Therefore $FT_N \left|\phi\right\rangle$ lies in that space.

If we apply the corollary above to $\left|\phi\right\rangle$ we conclude that the result of Fourier sampling of $T_l \left|\phi\right\rangle = \frac{\sqrt{r}}{\sqrt{N}} \sum_{j=0}^{N/r-1} \left| jr + l \right\rangle$ is a random multiples of N/r.