Lecture 23: Fast Fourier Transform II

Recap:

Def: Let $\{a_j\}_{j=0}^{n}$ and $\{b_k\}_{k=0}^{n}$ be two sequences of real numbers. We define their convolution $a*b$ as the new sequence $\{c_\ell\}_{\ell=0}^{n+m}$ given by:

$$c_\ell = (a*b)_\ell = \sum_{j=0}^{\ell} a_j b_{\ell-j}$$

The Strategy

Input: Coefficient vectors

Compute evaluations

$x_j \mapsto p(x_j)$, $x_j \mapsto q(x_j)$

for $j = 0 \dots n+m$

Find good choice of $x_0 \dots x_{n+m} \in \mathbb{C}$ using DaC to get $O((n+m)\log(n+m))$ time

$\Longrightarrow$

$O(n+m)$ time

· #evaluations

evaluations

Interpolate back

Output: Coefficient vec $a*b$ of $r(x) = p(x) \cdot q(x)$

Discrete Fourier Transform: Given $\{a_j\}_{j=0}^{n-1}$ specifying a poly $p(x) = \sum_{j=0}^{n-1} a_j x^j$, complete all the evaluations

$$\omega_n^k \longmapsto p(\omega_n^k) \quad \forall \; k = 0, \dots, n-1$$

where ω_n is the primitive n-th root of unity.

FFT for computing DFT:

Input: $a_0, \ldots a_{n-1}$; Assume n is power of 2

$\left.\begin{array}{l} \text{If } n=1: \\ \quad \text{Return}[a_0] \\ \text{Build } a_{even} := (a_0, a_2 \ldots a_{n-2}),\ a_{odd} := (a_1, a_3 \ldots a_{n-1}) \end{array}\right\} O(n)$

$\left.\text{Recurse}\quad F_{even} = FFT(a_{even}),\ F_{odd} = FFT(a_{odd})\right\} 2\,T(n/2)$

$\left.\begin{array}{l} \text{For } k \in \{0, 1, \ldots n/2 - 1\}: \\ \quad \text{Set } F[k] := F_{even}[k] + \omega_n^{k} \cdot F_{odd}[k] \\ \quad \text{Set } F[k+\frac{n}{2}] = F_{even}[k] + \omega_n^{k+n/2} \cdot F_{odd}[k] \end{array}\right\} O(n)$

Return F

$T(n) = O(n \log n)$!!

Claim: FFT computes DFT correctly for degree $2^{\ell}-1$ poly

Proof: Induction on ℓ. Base case $\ell=0$ is obvious.

Recall $p(x) = a_0 + a_1 x + a_2 x^2 \dots$

$$P_{even}(x) = a_0 + a_2 x + a_4 x^2 \dots = \sum_{k=0}^{\frac{n}{2}-1} a_{2k} x^k$$

$$P_{odd}(x) = a_1 + a_3 x + a_5 x^2 \dots = \sum_{k=0}^{\frac{n}{2}-1} a_{2k+1} x^k$$

$$p(x) = P_{even}(x^2) + x \cdot P_{odd}(x^2)$$

$$p(x) = P_{even}(x^2) - x P_{odd}(x^2)$$

Inductive step:

$$F[k] = F_{even}[k] + \omega_{2^{\ell+1}}^{k} \cdot F_{odd}[k]$$

$$= p_{even}(\omega_{2^{\ell}}^{k}) + \omega_{2^{\ell+1}}^{k} \, p_{odd}[\omega_{2^{\ell}}^{k}]$$

$$= p(\omega_{2^{\ell+1}}^{k})$$

Obs: $\omega_{n/2}^{k} = \exp\left(\frac{2\pi i}{n/2} k\right)$

$$= \exp\left(\frac{2\pi i}{n} 2k\right) = (\omega_n^{k})^2$$

Interpolation

Fact: Any degree-n polynomial p is uniquely determined by its evaluations on any set of $n+1$ distinct points.

$$
\begin{array}{c}
F \\
\begin{bmatrix} p(x_0) \\ p(x_1) \\ p(x_2) \\ \vdots \\ p(x_n) \end{bmatrix}
\end{array}
=
\begin{array}{c}
V \\
\begin{bmatrix}
1 & x_0 & x_0^2 & \cdots & x_0^n \\
1 & x_1 & x_1^2 & \cdots & x_1^n \\
1 & x_2 & x_2^2 & \cdots & x_2^n \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & x_n & x_n^2 & \cdots & x_n^n
\end{bmatrix}
\end{array}
\cdot
\begin{array}{c}
C \\
\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}
\end{array}
$$

Inversion in $O(n^2)$ with lagrange

Fact: the matrix above is invertible iff $x_i \neq x_j$.

We want to compute $F = Wc \Rightarrow c = W^{-1}F$

Lemma: $W^{-1} = \frac{1}{n+1}\overline{W}$, where $\overline{W}$ is entry wise complex conjugate of W.

Corollary: We can compute $c = W^{-1}F$ in $O(n\log n)$ again using FFT.

Proof: Goal is to verify $\frac{1}{n+1}\overline{W}\cdot W = I$

Diagonal Entries: Fix $k \in \{0, \dots, n\}$

$$\left(\frac{1}{n+1}\overline{W}\cdot W\right)(k,k) = \frac{1}{n+1}\sum_{j=0}^{n}\overline{W}(k,j)\cdot W(j,k) = \frac{1}{n+1}\sum_{j=0}^{n}\underbrace{\overline{\left(\omega_{n+1}^{j\cdot k}\right)}\left(\omega_{n+1}^{j\cdot k}\right)}_{=1}$$

$=1$

Off-Diagonal Entries: Fix $k \neq l$ in $\{0, \dots, n\}$.

$$\left(\frac{1}{n+1}\overline{W}\cdot W\right)(k,l) = \frac{1}{n+1}\sum_{j=0}^{n}\overline{\left(\omega_{n+1}^{jk}\right)}\,\omega_{n+1}^{j\cdot l}$$

$$= \frac{1}{n+1}\sum_{j=0}^{n}\left(\omega_{n+1}^{l-k}\right)^{j}$$

$$= \frac{1}{n+1}\sum_{j=0}^{n}\left(\omega^{*}_{n+1}\right)^{j}$$

$$= 0$$

ω^{*} is another primitive root of unity.

Convolution:

Input: $a, b \in \mathbb{R}^n$; Assume n is power of 2

Compute $F = DFT(a)$, $G = DFT(b)$

Compute $H = F \cdot G \in \mathbb{C}^n$ entrywise

Return $InverseDFT(H)$

Inverse DFT:

Input: $F_0 \ldots F_{n-1}$ Assume $n = 2^\ell$

Compute $y = FFT(\overline{F}_0, \ldots, \overline{F}_{n-1})$

Return $\overline{y}/n$

$$\boxed{\begin{aligned} W^{-1}F &= \frac{1}{n+1}\overline{W}F \\ &= \frac{1}{n+1}\overline{(W\overline{F})} \end{aligned}}$$

Bonus! Revisiting Sketching

Median Trick:

Goal: Unknown Y want to estimate. Let X r.v. satisfying

$$\mathbb{E}[X] = Y \;\&\; \mathrm{Var}(X) \leq C Y^2$$

Want: Design a new estimator $\hat{X}$ based on copies of X s.t. $\forall \varepsilon, \delta$, $\Pr[(1-\varepsilon)Y \leq \hat{X} \leq (1+\varepsilon)Y] \geq 1-\delta$

Naive Approach: $\hat{X} = \frac{1}{T}\sum_{i=1}^{T} X_i$ where X_i is indep. copy of X.

$$\mathrm{Var}(\hat{X}) = \frac{1}{T}\mathrm{Var}(X)$$

Median-of-means Estimator:

Let $\tilde{X}_j = \frac{1}{T}\sum_{i=1}^{T} X_{ij}$ for copies X_{ij} of X.

For $j=1,\dots,L$ (Set $T=\frac{100C}{\varepsilon^2}$, $L=\Theta(\log(1/\delta))$)

Theorem: Let $\hat{X} = \text{median}(\tilde{X}_1,\dots,\tilde{X}_L)$, then $\Pr[|\hat{X}-Y|>\varepsilon Y] \le \delta$

Proof: Define $Z_j = \mathbb{1}[|\tilde{X}_j - Y| \le \varepsilon Y]$

By earlier analysis, if $T=\frac{100C}{\varepsilon^2}$, then $\Pr[Z_j=1] = \frac{99}{100}$

$$\Pr[|\hat{X}-Y|>\varepsilon Y] = \Pr[|\hat{X}-Y|>\varepsilon Y \text{ for more than half of } j=1\dots L]$$

$$= \Pr\left[\sum_{j=1}^{L} Z_j < \frac{1}{2}L\right] \le \Pr\left[\sum_{j=1}^{L} Z_j \le \frac{3}{4}\underbrace{\mathbb{E}\left[\sum_{j=1}^{L} Z_j\right]}_{=\mu}\right] \le \exp\Big(-\overbrace{\frac{\mu}{32}}^{\mu=.99L}\Big) \le \underbrace{\delta}_{L=\Theta(\log\frac{1}{\delta})}$$