Math 342 Tutorial

July 23, 2025

Fast Fourier Transform. Let $n = 2^m$, $a(x) = \sum_{j=0}^{n-1} a_j x^j$, and $\omega = e^{2\pi\sqrt{-1}/n}$. The Fourier transform of of $a(x)$ is the vector $(\hat{a}_0, \dots, \hat{a}_{n-1})$ where $\hat{a}_i = \sum_j a_j \omega^{ij}$. Given $a(x) = \sum_{j=0}^{n-1} a_j x^j$, define $A(x) = \sum_{j=0}^{2n-1} a_j x^j$. Show the following.

- **(a)** Given two polynomials a and b of degree $n = 2^k$, show that the Fourier transform of $c(x) = a(x)b(x)$ is $(\hat{c}_0, \dots, \hat{c}_{2n-1})$ where $\hat{c}_i = \hat{A}_i \hat{B}_i$.
- **(b)** Show that $(a_0, \dots, a_{n-1}) \mapsto (\bar{a}_0, \dots, \bar{a}_{n-1})$ where $\bar{a}_i = n^{-1} \sum_{j=0}^{n-1} a_i \omega^{-ij}$ is an inverse of the Fourier transform.
- **(c)** Show that we can use the Fourier transform to multiply two polynomials in $O(n \log n)$ time. [Hint: Decompose a polynomial $a(x)$ of degree $n = 2^k$ as $a(x) = b(x^2) + xc(x^2)$ where $b(x)$ and $c(x)$ are the terms of even and odd exponent, respectively. Use the fact that $\{1, \omega, \dots, \omega^{n-1}\}$ are symmetric in the sense that $\omega^{n/2+i} = -\omega^i$.]

Fast Matrix Multiplication.

- **(a)** Show that standard matrix multiplication is $O(n^3)$.
- **(b)** Show that it is possible to multiply two 2×2 matrices using only 7 multiplications. Use the identity

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = C$$

with

$$\begin{aligned} c_{11} &= a_{11}b_{11} + a_{12}b_{21}, \\ c_{12} &= x + (a_{21} + a_{22})(b_{12} - b_{11}) + (a_{11} + a_{12} - a_{21} - a_{22})b_{22}, \\ c_{21} &= x + (a_{11} - a_{21})(b_{22} - b_{12}) - a_{22}(b_{11} - b_{21} - b_{12} + b_{22}), \\ c_{22} &= x + (a_{11} - a_{21})(b_{22} - b_{12}) + (a_{21} + a_{22})(b_{12} - b_{11}). \end{aligned}$$

- **(c)** Use an inductive argument to show that one may multiply $2^k \times 2^k$ matrices using only 7^k multiplications and fewer than 7^{k+1} additions. Conclude that two $n \times n$ matrices can be multiplied using $O(n^{\log_2 7})$ bit operations when all entries of the matrix a less than a constant c number of bits.