Math 416

Worksheet 10. The Discrete Fourier Transform

We want to interpolate! That is, we still want to be able to take n values of a polynomial $A(x_0)$, $A(x_1)$, ..., $A(x_{n-1})$ and return its coefficients a_0, a_1,..., a_{n-1}. This problem can be thought of in terms of matrices:

$$\begin{bmatrix} A(x_0) \\ A(x_1) \\ \vdots \\ A(x_{n-1}) \end{bmatrix} = \begin{bmatrix} 1 & x_0 & {x_0}^2 & \cdots & {x_0}^{n-1} \\ 1 & x_1 & {x_1}^2 & \cdots & {x_1}^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{n-1} & {x_{n-1}}^2 & \cdots & {x_{n-1}}^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}.$$

The large $n \times n$ matrix M is called a **Vandermonde matrix**; if the x_i are distinct then M is invertible. So interpolation is just multiplication by M^{-1}.

The naïve algorithm (of basic linear algebra) for finding the inverse of an $n \times n$ matrix takes $O(n^3)$ time. Vandermonde matrices are special and their structure can be exploited to improve this to $O(n^2)$ time, but this is still too expensive for our $O(n \log n)$ goal.

But remember that our plan was to interpolate using the roots of unity. If ζ is an n^{th} root of unity and $x_i = \zeta^i$ then that matrix M above, which we now call $M_n(\zeta)$, becomes

$$M_n(\zeta) = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta & \zeta^2 & \cdots & \zeta^{n-1} \\ 1 & \zeta^2 & \zeta^4 & \cdots & \zeta^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{n-1} & \zeta^{2(n-1)} & \cdots & \zeta^{(n-1)(n-1)} \end{bmatrix}.$$

For example,

Problem 1. Write down $M_4(i)$. And $M_4(-i)$ too, while you're at it.

Problem 2. Let $\zeta = e^{2\pi i/n}$.

(a) Show that the $(i, j)^{\text{th}}$ entry of $M_n(\zeta)$ is ζ^{ij} and conclude that $M_n(\zeta)$ is a symmetric matrix.

(b) Establish the following formula for the sum of the powers of ζ^m.

$$\sum_{l=0}^{n-1} \zeta^{ml} = \begin{cases} n & \text{if } m \text{ is a multiple of } n \\ 0 & \text{otherwise} \end{cases}.$$

(c) Prove that $M(\zeta)M(\zeta^{-1}) = nI$, where I is the $n \times n$ identity matrix.

(d) Find a formula for the (matrix) inverse of $M(\zeta)$.

(e) Go back through this problem and make sure that you never actually used the fact that $\zeta = e^{2\pi i/n}$. What you use is that ζ is a **primitive** n^{th} root of unity, meaning that $\zeta^k = 1$ iff n divides k.

Definition. The **discrete Fourier transform** (DFT) of a sequence $z_\bullet = (z_0, \ldots, z_{n-1})$ is the sequence $\text{DFT}(z_\bullet) = (c_0, \ldots, c_{n-1})$ where

$$c_k = \sum_{l=0}^{n-1} z_l e^{-2\pi ikl/n} = \sum_{l=0}^{n-1} z_l \zeta^{-kl}.$$

(In this case we insist that $\zeta = e^{2\pi i/n}$. This distinction is important.)

Problem 3. Thinking of $z_\bullet$ as a column vector, fill in the blank:

$$\mathrm{DFT}(z_\bullet) = M(\boxed{}) \cdot z_\bullet$$

Problem 4. Consider $\zeta = e^{2\pi i/4} = i$.

(a) Find $\mathrm{DFT}(1, 1, 1, 1)$.

(b) Let (z_0, z_1, z_2, z_3) be an arbitrary sequence of length 4. Find a formula for $\mathrm{DFT}(z_\bullet)$.

Definition. The **inverse discrete Fourier transform** sends $c_\bullet = (c_0, \ldots, c_{n-1})$ to $z_\bullet = \mathrm{IFT}(c_\bullet)$. It is given by the formula

$$z_l = \frac{1}{n} \sum_{k=0}^{n-1} c_k \zeta^{kl}.$$

Problem 5. Prove that $\mathrm{IFT}(\mathrm{DFT}(z_\bullet)) = z_\bullet$ and $\mathrm{DFT}(\mathrm{IFT}(c_\bullet)) = c_\bullet$.
(*Hint:* Use matrices and Problem 2; don't do it directly from the formulas.)

Proposition. Suppose that we are given a polynomial $P(x) = a_0 + a_1 x + \cdots + a_n x^n$ and an integer $N \geq n + 1$. Set $\zeta = e^{2\pi i/N}$ and set

$$c_\bullet = \mathrm{DFT}(\underbrace{a_0, \ldots, a_n, 0, \ldots, 0}_{N \text{ terms}}).$$

Then $c_\bullet = (P(1), P(\zeta^{-1}), \ldots, P(\zeta^{-(N-1)}))$.

Problem 6. Make sure you understand what the previous Proposition says, and then prove it.

Problem 7. Explain the assertion, 'DFT gives evaluation, while IFT gives interpolation.'

Problem 8. Let $N = 4$, $\zeta = e^{\pi i/2} = i$. Evaluating a polynomial of degree < 4 at the 4^{th} roots of unity is equivalent to taking the DFT of its coefficient sequence. Suppose we are given that the polynomial $p(x)$ passes through the points

$$(1, -3),\ (-i, 3i - 2),\ (-1, 3),\ (i, -3i - 2).$$

Find the coefficients of $p(x)$.