CS 170 Homework 3

Due **2/10/2020, at 10:00 pm**

1 Study Group

List the names and SIDs of the members in your study group. If you have no collaborators, you must explicitly write "none".

2 Modular Fourier Transform

Fourier transforms (FT) have to deal with computations involving irrational numbers which can be tricky to implement in practice. Motivated by this, in this problem you will demonstrate how to do a Fourier transform in modular arithmetic, using modulo 5 as an example.

(a) There exists $\omega \in \{0, 1, 2, 3, 4\}$ such that ω are 4^{th} roots of unity (modulo 5), i.e., solutions to $z^4 = 1$. When doing the FT in modulo 5, this ω will serve a similar role to the primitive root of unity in our standard FT. Show that $\{1, 2, 3, 4\}$ are the 4^{th} roots of unity (modulo 5). Also show that $1 + \omega + \omega^2 + \omega^3 = 0 \pmod 5$ for $\omega = 2$.

(b) Using the matrix form of the FT, produce the transform of the sequence $(0, 1, 0, 2)$ modulo 5; that is, multiply this vector by the matrix $M_4(\omega)$, for the value $\omega = 2$. Be sure to explicitly write out the FT matrix you will be using (with specific values, not just powers of ω). In the matrix multiplication, all calculations should be performed modulo 5.

(c) Write down the matrix necessary to perform the inverse FT. Show that multiplying by this matrix returns the original sequence. (Again all arithmetic should be performed modulo 5.)

(d) Now show how to multiply the polynomials $2x^2 + 3$ and $-x + 3$ using the FT modulo 5.

3 Inverse FFT

Recall that in class we defined M_n, the matrix involved in the Fourier Transform, to be the following matrix:

$$M_n = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \dots & \omega^{(n-1)(n-1)} \end{bmatrix},$$

where ω is a primitive n-th root of unity.
For the rest of this problem we will refer to this matrix as $M_n(\omega)$ rather than M_n. In this problem we will examine the inverse of this matrix.

2. (a) $1^4 \equiv 1 \pmod 5$ $\quad 3^4 = 81 \equiv 1 \pmod 5$ → Fermat little theorem

$2^4 = 16 \equiv 1 \pmod 5$ $\quad 4^4 = 256 \equiv 1 \pmod 5$

$1 + 2 + 2^2 + 2^3 = 2^4 - 1 = 15 \equiv 0 \pmod 5$

(b)
$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \\ 1 & 4 & 1 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 2 \end{bmatrix} = \begin{bmatrix} 3 \\ 8 \\ 12 \\ 7 \end{bmatrix} = \begin{bmatrix} 3 \\ 3 \\ 2 \\ 2 \end{bmatrix}$$

$4 * 4 \equiv 1 \pmod 5$.

(c) $w = 2$ $\quad w^{-1} = 3$

4^{-1}
$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 4 & 2 \\ 1 & 4 & 1 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix} \begin{bmatrix} 3 \\ 3 \\ 2 \\ 2 \end{bmatrix}$$

$$\begin{bmatrix} 4 & 4 & 4 & 4 \\ 4 & 2 & 1 & 3 \\ 4 & 1 & 4 & 1 \\ 4 & 3 & 1 & 2 \end{bmatrix} \begin{bmatrix} 3 \\ 3 \\ 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 2 \end{bmatrix}$$

d) $2x^2+3$ $\quad$ $-x+3$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \\ 1 & 4 & 1 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix} \begin{bmatrix} 3 \\ 0 \\ 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \\ 1 & 4 & 1 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix} \begin{bmatrix} 3 \\ 4 \\ 0 \\ 3 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \\ 4 \\ 0 \end{bmatrix} \quad *$$

$$\begin{bmatrix} 4 \\ 2 \\ 1 \\ 3 \end{bmatrix}$$

$3x^3 + x^2 + 2x + 4$

(a) Define

$$M_n(\omega^{-1}) = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \dots & \omega^{-(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{-(n-1)} & \omega^{-2(n-1)} & \dots & \omega^{-(n-1)(n-1)} \end{bmatrix}$$

Recall that $\omega^{-1} = 1/\omega = \bar{\omega} = \exp(-2\pi i/n)$.

Show that $\frac{1}{n}M_n(\omega^{-1})$ is the inverse of $M_n(\omega)$, i.e. show that

$$\frac{1}{n}M_n(\omega^{-1})M_n(\omega) = I$$

where I is the $n \times n$ identity matrix – the matrix with all ones on the diagonal and zeros everywhere else.

(b) Let A be a square matrix with complex entries. The *conjugate transpose* $A^\dagger$ of A is given by taking the complex conjugate of each entry of A^T. A matrix A is called *unitary* if its inverse is equal to its conjugate transpose, i.e. $A^{-1} = A^\dagger$. Show that $\frac{1}{\sqrt{n}}M_n(\omega)$ is unitary.

(c) Suppose we have a polynomial $C(x)$ of degree at most $n-1$ and we know the values of $C(1), C(\omega), \dots, C(\omega^{n-1})$. Explain how we can use $M_n(\omega^{-1})$ to find the coefficients of $C(x)$.

4 Polynomial from roots

Given a polynomial with exactly n distinct roots at $r_1, \dots, r_n$, compute the coefficient representation of this polynomial. Your runtime should be $\mathcal{O}(n \log^c n)$ for some constant $c > 0$ (you should specify what c is in your runtime analysis). There may be multiple possible answers, but your algorithm should return the polynomial where the coefficient of the highest degree term is 1.

You can give only the algorithm description and runtime analysis, a three-part solution is not required.

Hint: A root of a polynomial p is a number r such that $p(r) = 0$. One polynomial with roots $r_1, ..., r_k$ is

$$p(x) = \prod_{i=1}^{k}(x - r_i)$$

.

3. (a) $M_n(w^{-1}) M_n(w) = \begin{bmatrix} n & & \\ & \ddots & \\ & & n \end{bmatrix} = A$

$1 + w + w^2 + \dots + w^{n-1} = \frac{w^n - 1}{} = 0$

$A_{ij} =$

$[\,1,\ w^{-(i-1)},\ w^{-2(i-1)} \dots w^{-(j-1)(n-1)}]$

$\begin{bmatrix} 1 \\ w^{j-1} \\ \vdots \\ w^{(j-1)(n-1)} \end{bmatrix}$

$1 + w^{j-i} + w^{(j-1)^2} + \dots w^{(n-1)(j-i)}$

$w^{(j-i)} = \begin{cases} j = i & n \\ j \neq i & w^{n(j-i)} - 1 = 0 \end{cases}$

(b) $\frac{1}{\sqrt{n}} M_n(w) = A$

$A^+ = \frac{1}{\sqrt{n}} M_n(-w)$

$M_n(-w) * M_n(w) = n * I$

$\frac{1}{\sqrt{n}} M_n(-w) * \underbrace{\frac{1}{\sqrt{n}} M_n(w)}_{A} = I.$

$A^{-1} = \frac{1}{\sqrt{n}} M_n(-w)$

(c)

$$\frac{1}{n} M_n(w^{-1}) \begin{bmatrix} c(1) \\ c(w) \\ \vdots \\ c(w^{n-1}) \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix}$$

$$\frac{1}{n} \underbrace{M_n(w) * M_n(w^{-1})}_{\| \; I} \begin{bmatrix} c(1) \\ c(w) \\ \vdots \\ c(w^{n-1}) \end{bmatrix} = M_n(w) \begin{bmatrix} c_0 \\ \vdots \\ c_{n-1} \end{bmatrix}$$

4. $P(x) = \prod_{i=1}^{k} (x - r_i)$

$\downarrow$

$\frac{n}{2}$ root

$\frac{n}{2}$ root

$T(n) = 2T(\frac{n}{2}) + O(n \log n)$

$O(n \log n)$ X

$x - r_i$ $(x - r_i)$

$2^i * \frac{n}{2^i} * \log(\frac{n}{2^i})$ every level.

$n[\log(n) - i] = O(n \log(n))$

$\log n$ level $n \log^2 n$

5 Triple sum

We are given an array $A[0..n-1]$ with n elements, where each element of A is an integer in the range $0 \leq A[i] \leq n$ (the elements are not necessarily distinct). We would like to know if there exist indices i, j, k (not necessarily distinct) such that

$$A[i] + A[j] + A[k] = n$$

Design an $\mathcal{O}(n \log n)$ time algorithm for this problem. Note that you do not need to actually return the indices; just yes or no is enough.

Please give a 3-part solution to this problem.

6 Searching for Viruses

Sherlock Holmes is trying to write a computer antivirus program. He thinks of computer RAM as being a binary string s_2 of length m, and a virus as being a binary string s_1 of length $n < m$. His program needs to find all occurrences of s_1 in s_2 in order to get rid of the virus. Even worse, though, these viruses are still damaging if they differ slightly from s_1. So he wants to find all copies of s_1 in s_2 that differ in at most k locations for arbitrary $k \leq n$.

(a) Give a $O(nm)$ time algorithm for this problem.

(b) Give a $O(m \log m)$ time algorithm for any k.

You do not need a 3-part solution for either part. Instead, describe the algorithms clearly and give an analysis of the running time.

7 Vertex Cut

Let $G = (V, E)$ be an undirected, unweighted graph with $n = |V|$ vertices. The *distance* between two vertices $u, v \in G$ is the length of the shortest path between them. A *vertex cut* of G is a subset $S \subseteq V$ such that removing the vertices in S (as well as incident edges) disconnects G.

Show that if there exist $u, v \in G$ of distance $d > 1$ from each other, that there exists a vertex cut of size at most $\frac{n-2}{d-1}$. Assume G is connected.

5. sort first $O(n \log n)$

for i in [0, n-3].

$O(n^2)$

j = i+1 k = n-1

s = A[i] + A[j] + A[k]

if s == n

$O(n^2)$

return yes.

if s > n

main idea

pseudo code

6. (a) m call n: viruses

pseudo code:

$O(nm)$

for i in range(len(m))

for j in range(len(n))

if(m[i+j] ≠ n[j])

break

else:

viruses at i

(b) add count in (a) can solve in $O(mn)$

binary string ???

7. ??? ???