COL 351 : Analysis and Design of Algorithms

Tutorial Sheet - 7

Question 1 Applications of FFT:

(i) Let $A = \{a_1, a_2, \ldots, a_n\}$ be a set of positive integers in range $[1, M]$. Prove that the set $S = \{x + y + z \mid x, y, z \in A\}$ $\cancel{S = \{x^2 + y^3 + z \mid x, y, z \in A\}}$ is computable in $O(M \log M)$ time.

(ii) The hamming distance of two n-length arrays A, B is the number of positions where they mismatch, that is,

$$Ham\text{-}Dist(A, B) = \sum_{\substack{i \in [1,n] \\ A[i] \neq B[i]}} 1.$$

The cyclic shift M^i of an array M by a value $i < n$ is defined to be the concatenated array

$$M^i := M[i+1, n] \cdot M[1, i].$$

Device an $O(n \log n)$ time algorithm that given two n-length binary arrays A, B, finds an i in range $[0, n-1]$ for which $Ham\text{-}Dist(A, B^i)$ is minimized.

Question 2 Prove the following:

(i) If ω is N^{th} primitive root of unity then $\{1, \omega, \omega^2, \ldots, \omega^{N-1}\}$ are distinct roots of $x^N - 1 = 0$.

(ii) If ω is N^{th} primitive root of unity then for every $1 \leq i \lneq N$, we have

$$1 + \omega^i + \omega^{2i} + \cdots + \omega^{i(N-1)} = 0.$$

(iii) If ω is a non-primitive N^{th} root of unity then there exists an $1 \leq i \lneq N$ satisfying

$$1 + \omega^i + \omega^{2i} + \cdots + \omega^{i(N-1)} \neq 0.$$

(iv) If ω is N^{th} primitive root of unity and N is power of two, then for any $1 \leq i \lneq N$, ω^i is N^{th} primitive root of unity if and only if i is odd. Use this to argue that ω^{-1} is also N^{th} primitive root of unity.

Question 3 Consider the Vandermonde matrix below of size $N \times N$.

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^j & \cdots & \omega^{N-1} \\ 1 & & & & & & \\ \vdots & & & & & & \\ 1 & \omega^i & (\omega^i)^2 & \cdots & (\omega^i)^{\,j} & \cdots & (\omega^i)^{\,N-1} \\ \vdots & & & & & & \\ 1 & & & & & & \end{bmatrix}$$

In the lecture, we computed the inverse of this matrix when ω is N^{th} primitive root of unity. Prove that the matrix will be non-invertible if ω was a non-primitive N^{th} root of unity.

Question 4 Compute the DFT of polynomial $x^3 + x^2 + 2x + 1$ using both FFT algorithm and by pre-multiplying the associated vector by Vandermonde matrix. Verify that the results are identical. (You should take ω to be $0 + i$).

Question 5 Let $\mathcal{U} = \{u_1, \ldots, u_n\}$ be a universe of n elements, and $\mathcal{A}, \mathcal{B}$ be family whose elements are non-empty subsets of $\mathcal{U}$. Thus, $|\mathcal{A}|, |\mathcal{B}| \leq 2^n - 1$.

Use FFT to device an $O(2^n \cdot n)$ time algorithm to compute the number of pairs $(A, B) \in (\mathcal{A} \times \mathcal{B})$ for which $A \cap B = \emptyset$ and $A \cup B = \mathcal{U}$.

Hint: Compute two polynomials $P_{\mathcal{A}}(x)$ and $P_{\mathcal{B}}(x)$ corresponding to $\mathcal{A}$ and $\mathcal{B}$, and look for coefficient of x^{2^n-1} in $P_{\mathcal{A}}(x) \cdot P_{\mathcal{B}}(x)$.

Remark: Note that there are other simpler approaches to solve this problem that don't use FFT.