CS-E4500 Problem Set 2

Jaan Tollander de Balsch - 452056

January 31, 2019

Two books used as a resources in this report are Cormen et al. (2009), Chapter. 30, *Polynomials and FFT* and Gathen and Gerhard (2013), Chapter. 8.2, *The Discrete Fourier Transform and the Fast Fourier Transform.*

Problem 1

Multiplication with the discrete Fourier tranform. Let us multiply $f = 1 + x + x^2 \in \mathbb{Z}_{13}[x]$ and $g = 2 + 12x^3 \in \mathbb{Z}_{13}[x]$ using the dicrete Fourier transform.

Let ω_n^k be the roots of unity for $k = 0, 1, ..., n-1$.

1) Evaluate the polynomials as the roots of unity (DFT)

$$\alpha_k = f(\omega_n^k)$$

$$\beta_k = g(\omega_n^k)$$

2) Multiply the polynomials pointwise

$$\gamma_k = \alpha_k \cdot \beta_k$$

3) Recover the coffiecients of the polynomial using inverse DFT

$$a_j = n^{-1} \sum_{k=0}^{n-1} \gamma_k (\omega_n^{-1})^{kj}$$

The order of the resulting polynomial $n = 6$ and its inverse $n^{-1} = 6^{-1} = 11 \in \mathbb{Z}_{13}$.

The primitive root of unity $\omega_6 = 4$ and its inverse $w_6^{-1} = 4^{-1} = 10 \in \mathbb{Z}_{13}$.

The power of the root of unity of order 6 are $\omega_6^0, ..., \omega_6^5$

$$[1, \quad 4, \quad 3, \quad 12, \quad 9, \quad 10]$$

The values of polynomial f evaluated at w_6^k are $\alpha_0, ..., \alpha_5$

$$[3, \quad 8, \quad 0, \quad 1, \quad 0, \quad 7]$$

The values of polynomial g evaluated at w_6^k are $\beta_0, ..., \beta_5$

$$[1, \quad 3, \quad 1, \quad 3, \quad 1, \quad 3]$$

The values of the pointwise product $\gamma_k = \alpha_k \cdot \beta_k$ for $k = 0, ..., 5$ are

$$[3, \quad 11, \quad 0, \quad 3, \quad 0, \quad 8]$$

The powers of the inverses of the primitive roots of unity are $(\omega_6^{-1})^0, ..., (\omega_6^{-1})^5$

$$[1, \quad 10, \quad 9, \quad 12, \quad 3, \quad 4]$$

Finally, the inverse discrete Fourier tranform gives us the coefficients $a_0, ..., a_5$ of the polynomial

$$[2, \quad 2, \quad 2, \quad 12, \quad 12, \quad 12]$$

We can verify that

$$f \cdot g = 2 + 2x + 2x^2 + 12x^3 + 12x^4 + 12x^5 \in \mathbb{Z}_{13}[x]$$

using for example the naive multiplication algorithm.

Problem 2

The convolution identity. Let $\omega \in R$ be a primitive root of unity of order n in a ring R. Show that for all $f, g \in R[x]/\langle x^n - 1\rangle$ we have $DFT_\omega(fg) = DFT_\omega(f) \cdot DFT_\omega(g)$.

The polynomial $fg \in R[x]/\langle x^n - 1\rangle$ is given by the convolution

$$(f * g) \equiv f \cdot g \mod x^n - 1.$$

The by evaluation $f * g$ in the roots of unity ω^j for $j = 0, 1, ..., n-1$ gives us

$$\begin{aligned}(f * g)(\omega^j) &= f(\omega^j) \cdot g(\omega^j) + q(\omega^j) \cdot (\omega^j - 1), \quad \omega^j - 1 = 0 \\ &= f(\omega^j) \cdot g(\omega^j).\end{aligned}$$

This proves the indentity

$$\begin{aligned}DFT_\omega(f * g) &= [(f * g)(\omega^0), ..., (f * g)(\omega^{n-1})] \\ &= [f(\omega^0) \cdot g(\omega^0), ..., f(\omega^{n-1}) \cdot g(\omega^{n-1})] \\ &= [f(\omega^0), ..., f(\omega^{n-1})] \cdot [g(\omega^0), ..., g(\omega^{n-1})] \\ &= DFT_\omega(f) \cdot DFT_\omega(g).\end{aligned}$$

Problem 3

Input: A polynomial $A(x) = \sum_{j=0}^{n-1} a_j x^j$ in the ring $R[x]$ and roots of unity ω^j for $j = 0, 1, ..., n-1$ where ω is the primitive root of unity in R.

Output: Vector of values of the polynomial evaluated at the roots of unity $[A(\omega^0), A(\omega^1), ..., A(\omega^{n-1})] \in R^n$.

Idea: Recursively evaluate polynomial

$$A(x) = A$$

Algorithm

Problem 4

References

Cormen, T.H., Leiserson, C.E., Rivest, R.L. and Stein, C., 2009. *Introduction to Algorithms, Third Edition*. 3rd ed. The MIT Press.

Gathen, J. von zur and Gerhard, J., 2013. *Modern Computer Algebra*. 3rd ed. New York, NY, USA: Cambridge University Press.