NOTES ON FFT FOR FINITE FIELDS

DANIEL R. BARRERO R.

1

What follows is an overview of Pollard's definition, as found in [1], of the Fourier transform for finite fields.

Let $GF(p^n)$, or F for short, be the Galois field with p^n elements, where p is a prime number and n is a positive integer. Let d be a divisor of $p^n - 1$, and let r be an element of order d in F^*. Then, if (a_i) is a sequence in F of length d, we define its *Fourier transform* via the rule

$$A_i = \sum_{j=0}^{d-1} a_j r^{ij}. \tag{1}$$

It has the following "convolution property": if the sequences (a_i), (b_i) and (c_i) are such that their transforms (A_i), (B_i) and (C_i) satisfy

$$C_i = A_i B_i \tag{2}$$

then

$$c_i = \sum_{j=0}^{d-1} a_j b_{i-j}, \tag{3}$$

where the indices for the terms b_t are taken modulo d.

In equation (3) we see (c_i) as the "convolution" of (a_i) and (b_i), which allows us to rephrase the relationship between equations (2) and (3) as follows:

Lemma 1 (Informal convolution statement)**.** *To compute the convolution of two sequences, one may first transform them, then compute their point-wise product, and then apply the reverse transform.*

2. Comments

2.1. Prove that if $F = GF(p^n)$ then F^* is cyclic of order $p^n - 1$.

2.2. FFT, both in number fields and in $\mathbf{C}$, has complexity $O(d \log d)$ versus the complexity $O(d^2)$ of the naive way to compute.

References

[1] Pollard, J. M. The fast Fourier transform in a finite field. *Math. Comput. 25* (1971), 365–374.

Date: July 6, 2025.