Fast Algorithms for Discrete Fourier Transform: Galois Reduction

Vladimir Chernov

The problem of inverse Fourier transform computation is investigated.

$$\hat{y}(m) = \sum_{n=0}^{p-1} y(n) \exp\{\frac{2\pi inm}{p}\}, \quad (m = 0, ..., p-1) \tag{1}$$

p is prime. It is shown, that the problem can be reduced to calculation of full Galois-image for some element in the cyclotomic field. This Galois-image calculation can be implemented recursively, similarly to the recursive DFT of the length equal to some composite number ("Galois analogue" of well-known Cooley-Tukey, Good-Thomas algorithms).

Unlike Vinograd's method, resulting in the lower estimates of the computational complexity of the DFT, the technique proposed provides the explicit formulas for computational complexity in terms of arithmetic operations of in algebraic number fields. If $y(n) \in \mathbf{Q}$, p is a prime, $\omega = \exp\{2\pi i p^{-1}\}$, then $\hat{y}(m) \in \mathbf{Q}(\omega)$, where $\mathbf{Q}(\omega)$ is the cyclotomic field and $[\mathbf{Q}(\omega) : \mathbf{Q}] = p - 1 = d_1 ... d_t$. In this case field $\mathbf{Q}(\omega)$ can be obtained by consecutive expansions of $\mathbf{Q}$:

$$\mathbf{Q} = \mathbf{K}_0 \subset \mathbf{K}_1 \subset ... \subset \mathbf{K}_t = \mathbf{Q}(\omega), \quad [\mathbf{K}_j : \mathbf{K}_{j-1}] = d_j.$$

In presented paper a new kind of DFT reduction is investigated. It is "Galois reduction", that reduced calculation of sums (1) to calculation of sums which have values in subfields $\mathbf{K}_j$.

Theorem 1. Let $M(p)$ be multiplicative complexity of DFT algorithm. Then

$$M(p) \leq d_1 ... d_t \sum_{j=1}^{t-1} d_j^{-1} M_{conv}(d_j;\ \mathbf{K}_j, \mathbf{K}_{j-1}),$$

where $M_{conv}(d_j;\ \mathbf{K}_j, \mathbf{K}_{j-1})$ is multiplicative complexity of a d_j-periodic convolution algorithm for $\mathbf{K}_j-$valued sequence and $\mathbf{K}_{j-1}-$valued sequence.

In this paper there are given the examples of "bad" prime numbers that do not have a corresponding fast DFT algorithm, as well as analytical criteria of their finding based on Erdös' results and the estimates of their density in the natural scale.

Theorem 2. There exist such a constant λ, then for every prime p (excluding $p \in \Re^*$) there exists a fast DFT-algorithm with the complexity

$$M(p) < \lambda p \log_2 p \tag{2}$$

and

$$\mathrm{card}(p < x; \quad p \in \Re^*) < O\left(\frac{x}{\ln^2 x}\right).$$

Note that inequality (2) was typical for Cooley-Tukey FFT of length $N = 2^k$ only.