FAST FOURIER TRANSFORM ALGORITHMS[1]

S. B. Gashkov, I. S. Sergeev (Moscow)

The paper deals with fast algorithms for discrete Fourier transform in some rings and their application to the multiplication of polynomials. The algorithm's performance measure is its complexity, defined as the number of binary operations of addition, subtraction, multiplication, as well as operations of multiplication by ring constants.

1. Discrete Fourier transform

Let $\mathbf{K}$ be a commutative ring with unity[2]. An element $\zeta \in \mathbf{K}$ is called a *primitive root of order* $N \in \mathbb{N}$ if $\zeta^N = 1$, and none of the elements $\zeta^{N/p} - 1$, where p is a prime divisor of N, is a zero divisor in $\mathbf{K}$. (Recall that an element a is a zero divisor if there exists a nonzero element b such that $ab = 0$.)

The *discrete Fourier transform* (*DFT*) *of order* N is the $(\mathbf{K}^N \to \mathbf{K}^N)$-transform

$$\mathrm{DFT}_{N,\zeta}[\mathbf{K}](\gamma_0, \ldots, \gamma_{N-1}) = (\gamma_0^*, \ldots, \gamma_{N-1}^*), \qquad \gamma_j^* = \sum_{i=0}^{N-1} \gamma_i \zeta^{ij}, \qquad (1)$$

where ζ is a primitive root of order N.

The fundamental property of the DFT is stated as follows:

Lemma 1. *Let elements* γ_j^* *be determined from* (1). *Then*

$$\mathrm{DFT}_{N,\zeta^{-1}}[\mathbf{K}](\gamma_0^*, \ldots, \gamma_{N-1}^*) = (N\gamma_0, \ldots, N\gamma_{N-1}),$$

where N *on the right-hand side of the formula is the sum of* N *units of the ring.*

Before we proceed to the proof of the lemma, we establish several auxiliary facts.

Note that if $a \in \mathbf{K}$ is not a zero divisor, and $a = cd$, then the factors c and d are also not zero divisors. Indeed, if, say, $ce = 0$ and $e \neq 0$, then $ae = (ce)d = 0$, which implies that a is a zero divisor.

[1] **Translated version.** Originally published in: "Discrete mathematics and its applications". Part V. Moscow: Izd. IPM RAN, 2009. P. 3–23. (in Russian) — a few minor typos are corrected

[2] *Note from* 01.11.2010. In the proof of Lemma 2, the associativity of the ring $\mathbf{K}$ is used. Therefore, throughout the text, the ring should also be considered associative.

Lemma 2. *If ζ is a primitive root of order N, then for any $l = 1, \ldots, N-1$,*

$$\sum_{i=0}^{N-1} \zeta^{il} = 0.$$

Proof. Consider the expansion

$$0 = \zeta^{lN} - 1 = (\zeta^l - 1) \sum_{i=0}^{N-1} \zeta^{il}.$$

From the definition of a primitive root it follows that N is the minimal natural exponent n for which $\zeta^n = 1$, therefore $\zeta^l - 1 \neq 0$. Consequently, either $\zeta^l - 1$ is a zero divisor, or $\sum_{i=0}^{N-1} \zeta^{il} = 0$. We will show that the first is impossible.

Let $m = \mathrm{GCD}(l, N)$. As is known, there exist integers q, s such that $m = ql + sN$ (these numbers q, s are called Bezout coefficients), and we can assume that q is positive. In this case, $\zeta^m - 1 = \zeta^{ql} - 1$ is divisible by $\zeta^l - 1$. On the other hand, since $m < N$, there exists a prime p such that $m \mid (N/p)$. Then $(\zeta^m - 1) \mid (\zeta^{N/p} - 1)$. Finally, we have $(\zeta^l - 1) \mid (\zeta^{N/p} - 1)$. Since $\zeta^{N/p} - 1$ is not a zero divisor, $\zeta^l - 1$ cannot be a zero divisor as well. Therefore, $\sum_{i=0}^{N-1} \zeta^{il} = 0$. □

Proof of Lemma 1. In the vector $\mathrm{DFT}_{N,\zeta^{-1}}[\mathbf{K}](\gamma_0^*, \ldots, \gamma_{N-1}^*)$ consider an arbitrary j-th component:

$$\sum_{i=0}^{N-1} \gamma_i^* \zeta^{-ij} = \sum_{i=0}^{N-1} \sum_{k=0}^{N-1} \gamma_k \zeta^{ki} \zeta^{-ij} = \sum_{k=0}^{N-1} \sum_{i=0}^{N-1} \gamma_k \zeta^{i(k-j)} = \sum_{k=0}^{N-1} \gamma_k \sum_{i=0}^{N-1} (\zeta^{k-j})^i.$$

The inner sum, as follows from Lemma 2, is zero in all cases except for the case $k - j = 0$, when this sum is N. Therefore, continuing the calculation, we obtain $N\gamma_j$, as required. □

As a consequence, we obtain that if $N = 1 + \ldots + 1 \in \mathbf{K}$ is invertible, then the inverse DFT transform is defined:

$$\mathrm{DFT}_{N,\zeta}^{-1}[\mathbf{K}] = N^{-1} \mathrm{DFT}_{N,\zeta^{-1}}[\mathbf{K}].$$

2. Polynomial interpretation of the DFT

Consider a polynomial $\Gamma(x) = \gamma_0 + \ldots + \gamma_{N-1} x^{N-1}$. Then, by definition,

$$\mathrm{DFT}_{N,\zeta}[\mathbf{K}](\gamma_0, \ldots, \gamma_{N-1}) = \left(\Gamma(\zeta^0), \ldots, \Gamma(\zeta^{N-1})\right),$$

i.e., the DFT evaluates the polynomial $\Gamma(x)$ at the points ζ^i. The meaning of the inverse transform $\mathrm{DFT}^{-1}_{N,\zeta}[\mathbf{K}]$ is to restore the coefficients of a unique polynomial of degree less than N that has a given set of values at the points $\zeta^0, \ldots, \zeta^{N-1}$.

Formally, the relationship between the DFT and interpolation is described by the following lemma:

Lemma 3. *The transform* $\mathrm{DFT}_{N,\zeta}[\mathbf{K}]$ *defines an isomorphism:* $\mathbf{K}[x]/(x^N - 1) \to \mathbf{K}^N$.

Proof. The bijectivity of the mapping follows from the fact that a polynomial of degree no greater than $N - 1$ is uniquely determined by its values on a set of N distinct points.

Let us verify that the DFT preserves the operations of addition and multiplication: in the ring $\mathbf{K}[x]/(x^N - 1)$ these operations are performed as with ordinary polynomials, only with subsequent reduction modulo $x^N - 1$, in the ring $\mathbf{K}^N$ the operations are performed componentwise.

Indeed, the value of the sum of the polynomials $\Gamma_1(x) + \Gamma_2(x)$ at some point coincides with the sum of the values of each of the polynomials at this point. Representing the product of the polynomials in the form $Q(x)(x^N - 1) + R(x)$, where $R(x)$ is the remainder of division by $x^N - 1$, we see that the product is mapped into a product, since

$$\Gamma_1(\zeta^j)\Gamma_2(\zeta^j) = Q(\zeta^j)(\zeta^{jN} - 1) + R(\zeta^j) = R(\zeta^j) = (\Gamma_1\Gamma_2 \bmod (x^N - 1))(\zeta^j).$$

□

The above isomorphism leads to an efficient way of multiplying polynomials over $\mathbf{K}$.

Theorem 1. *Let* $\mathrm{DFT}_{N,\zeta}[\mathbf{K}]$ *and its inverse be defined over a ring* $\mathbf{K}$. *Then the multiplication of two polynomials of total degree at most* $N - 1$ *over* $\mathbf{K}$ *can be performed using two transforms* $\mathrm{DFT}_{N,\zeta}[\mathbf{K}]$, *one* $\mathrm{DFT}^{-1}_{N,\zeta}[\mathbf{K}]$, *and* N *multiplications in* $\mathbf{K}$.

Proof. Denote the polynomials to be multiplied by $A(x) = \sum a_i x^i$ and $B(x) = \sum b_i x^i$. Compute the vectors

$$(a^*_0, \ldots, a^*_{N-1}) = \mathrm{DFT}_{N,\zeta}[\mathbf{K}](a_0, \ldots, a_{N-1}),$$
$$(b^*_0, \ldots, b^*_{N-1}) = \mathrm{DFT}_{N,\zeta}[\mathbf{K}](b_0, \ldots, b_{N-1}).$$

Then the coefficients of the polynomial $C(x) = \sum c_i x^i = A(x)B(x)$ due to $C(x) = C(x) \bmod (x^N - 1)$ can be determined as

$$(c_0, \ldots, c_{N-1}) = \mathrm{DFT}^{-1}_{N,\zeta}[\mathbf{K}](a^*_0 b^*_0, \ldots, a^*_{N-1} b^*_{N-1}),$$

whence the assertion of the theorem follows.

3. DFT computation

Independent calculation of the DFT components by formulas (1) can be performed in $O(N^2)$ operations of addition, subtraction, and multiplication by constants in a ring $\mathbf{K}$. For a composite number N, the following more efficient method can be proposed.

First, note that if ζ is a primitive root of order ST, then ζ^S and ζ^T are primitive roots of order T and S, respectively (this can be easily verified directly from the definition).

Lemma 4 (Cooley, Tukey [5]). *A DFT of order ST is implemented using S DFTs of order T, T DFTs of order S, and $(S-1)(T-1)$ multiplications by powers of ζ — a primitive root of order ST.*

Proof. For $s = 0, \ldots, S-1$ and $t = 0, \ldots, T-1$, write

$$\gamma^*_{sT+t} = \sum_{I=0}^{ST-1} \gamma_I \zeta^{I(sT+t)} = \sum_{i=0}^{T-1} \sum_{j=0}^{S-1} \gamma_{iS+j} \zeta^{(iS+j)(sT+t)} =$$

$$= \sum_{i=0}^{T-1} \sum_{j=0}^{S-1} \gamma_{iS+j} \zeta^{itS+jsT+jt} = \sum_{j=0}^{S-1} (\zeta^T)^{js} \cdot \zeta^{jt} \cdot \gamma_{(j),t}, \quad (2)$$

where

$$\gamma_{(j),t} = \sum_{i=0}^{T-1} \gamma_{iS+j} (\zeta^S)^{it}.$$

The obtained formula allows to perform computations in the following order:
a) For $j = 0, \ldots, S-1$, compute the vectors

$$\left(\gamma_{(j),0}, \gamma_{(j),1}, \ldots, \gamma_{(j),T-1}\right) = \mathrm{DFT}_{T,\zeta^S}[\mathbf{K}](\gamma_j, \gamma_{S+j}, \ldots, \gamma_{(T-1)S+j}).$$

b) Compute the products $\omega_{(t),j} = \zeta^{jt} \cdot \gamma_{(j),t}$, $j = 0, \ldots, S-1$, $t = 0, \ldots, T-1$.
c) Note that

$$\gamma^*_{sT+t} = \sum_{j=0}^{S-1} \omega_{(t),j} (\zeta^T)^{js}.$$

This allows to finally find the components of the DFT by the formulas

$$\left(\gamma^*_t, \gamma^*_{T+t}, \ldots, \gamma^*_{(S-1)T+t}\right) = \mathrm{DFT}_{S,\zeta^T}[\mathbf{K}](\omega_{(t),0}, \omega_{(t),1}, \ldots, \omega_{(t),S-1}),$$

where $t = 0, \ldots, T-1$.

The assertion of the lemma follows immediately from the form of the operations performed at steps *a*–*c*) if we note that among ST multiplications at step *b*) there are $S + T - 1$ multiplications by $\zeta^0 = 1$. □

Remark (Good, Thomas [6]). *If S and T are relatively prime, then to implement the DFT of order ST it is sufficient to perform S DFTs of order T and T DFTs of order S, i.e., no additional multiplications are required.*

Let $F(N) = F_A(N) + F_C(N)$ denote the complexity of an order-N DFT circuit constructed by the method of Lemma 4, where $F_A(N)$ is the number of additive elements (additions and subtractions) in the circuit, and $F_C(N)$ is the number of scalar multiplications (i.e. multiplications by constants of the ring $\mathbf{K}$). In this case, the required circuits implementing DFT of prime orders should be constructed separately.

It is easy to construct a circuit for the DFT of order 2, if it exists. The components of the DFT are determined by the formulas

$$\gamma_0^* = \gamma_0 + \gamma_1, \qquad \gamma_1^* = \gamma_0 - \gamma_1,$$

since -1 can be taken as a primitive root of order 2. Therefore, we set $F(2) = 2$, $F_A(2) = 2$, $F_C(2) = 0$.

To calculate the complexity of an order-2^k DFT circuit, where $k > 1$, we use recurrence relations that follow from Lemma 4 with the choice of parameters $S = 2^{k-1}$ and $T = 2$:

$$F_A(2^k) = 2F_A(2^{k-1}) + 2^{k-1}F_A(2), \quad F_C(2^k) = 2F_C(2^{k-1}) + 2^{k-1}F_C(2) + 2^{k-1} - 1.$$

It is easy to check that these relations are resolved as

$$F_A(2^k) = k2^k, \qquad F_C(2^k) = (k-2)2^{k-1} + 1. \tag{3}$$

So, we proved

Theorem 2. *A DFT of order 2^k can be performed in $k2^k$ addition-subtraction operations and $(k-2)2^{k-1} + 1$ scalar multiplication operations.*

This bound is asymptotically the best known upper bound for the complexity of a DFT of order 2^k.

The complexity of the circuit for the inverse DFT of order 2^k coincides with the complexity of the "forward" DFT up to 2^k multiplications by constants 2^{-k}. For $k \geq 2$, multiplications by 2^{-k} can be combined with multiplications at step *b*).

The given algorithm is an example of the *fast Fourier transform* (*FFT*) algorithm. In general, FFT algorithms are understood as those algorithms that imply reducing a DFT of composite order N to DFTs of orders of factors of N. Sometimes the term FFT is applied to any algorithms of complexity $O(N \log N)$.

4. Real complexity of complex DFT

The situation when additive and multiplicative operations in a ring $\mathbf{K}$ cannot be considered equivalent leads to the creation of special FFT algorithms. Let us illustrate this on the example of the field of complex numbers $\mathbb{C}$.

A complex number is usually represented by a pair of real numbers — real and imaginary parts: $z = x + \mathbf{i}y$. Let's recalculate operations with complex numbers into operations with real numbers. Complex addition (subtraction) is equivalent to two real additions (subtractions). Complex multiplication can be performed via four real multiplications and two addition-subtractions. In addition, to multiply by a constant, three real multiplications and three addition-subtractions are sufficient.

For the above-described circuit for the complex DFT of order 2^k, we obtain the estimates $F_A^{\mathbb{R}}(2^k) < 3.5k2^k$ for the number of real additions-subtractions and $F_C^{\mathbb{R}}(2^k) < 1.5k2^k$ for the number of real scalar multiplications, and in total $F^{\mathbb{R}}(2^k) < 5k2^k$.

However, a better estimate can be derived if we note that it is advantageous not to perform some multiplications in the algorithm of Lemma 4 immediately, but to postpone them for the next stage of computations (implementation of DFTs of order S). The well-known "split-radix" FFT algorithm is based on such observation.

Theorem 3. *A DFT of order 2^k over $\mathbb{C}$ can be implemented via at most $3k2^k$ additions-subtractions and at most $k2^k$ multiplications in the field $\mathbb{R}$.*

Proof. By formula (2), in which $S = 2^{k-1}$ and $T = 2$, compute only even components of the DFT of order 2^k, i.e., for $t = 0$. To do this, it is sufficient to calculate one component $\gamma_{(j),0} = \gamma_j + \gamma_{S+j}$ of each of the 2^{k-1} internal order-2 DFTs and implement the external DFT of order 2^{k-1}.

To calculate the components with odd indices, set $S = 2^{k-2}$ and $T = 4$ and again apply formula (2). For each of 2^{k-2} inner DFTs of order 4, we need to compute two components $\gamma_{(j),1}$ and $\gamma_{(j),3}$. Each such pair, due to $\zeta^S = \mathbf{i}$, can be obtained by the formulas

$$\gamma_{(j),1} = (\gamma_j - \gamma_{2S+j}) + \mathbf{i}(\gamma_{S+j} - \gamma_{3S+j}),$$
$$\gamma_{(j),3} = (\gamma_j - \gamma_{2S+j}) - \mathbf{i}(\gamma_{S+j} - \gamma_{3S+j}).$$

Since multiplication by $\pm\mathbf{i}$ is reduced to permutation of the real and imaginary parts with a sign change for one of them, the calculation of one pair $\gamma_{(j),1}$, $\gamma_{(j),3}$ by these formulas is performed in 8 real additions-subtractions. Finally, 2^{k-1} multiplications by powers of ζ^{jt} and two DFTs of order 2^{k-2} are performed.

For the number $F_A^{\mathbb{R}}(2^k)$ of additions-subtractions and the number $F_C^{\mathbb{R}}(2^k)$ of scalar multiplications in the constructed circuit we have the recurrence relations:

$$F_A^{\mathbb{R}}(2^k) \le F_A^{\mathbb{R}}(2^{k-1}) + 2F_A^{\mathbb{R}}(2^{k-2}) + 4.5 \cdot 2^k,$$
$$F_C^{\mathbb{R}}(2^k) \le F_C^{\mathbb{R}}(2^{k-1}) + 2F_C^{\mathbb{R}}(2^{k-2}) + 1.5 \cdot 2^k,$$

which, taking into account the initial data

$$F_A^{\mathbb{R}}(2) = 4,\ F_C^{\mathbb{R}}(2) = 0,\ F_A^{\mathbb{R}}(4) = 16,\ F_C^{\mathbb{R}}(4) = 0,$$

are resolved as promised. □

A more careful counting allows to obtain the complexity of the method in the form: $3k2^k - 3 \cdot 2^k + 4$ additions-subtractions and $k2^k - 3 \cdot 2^k + 4$ scalar multiplications over $\mathbb{R}$. This estimate was established no later than 1968, but it was only in 2004 that van Buskirk discovered that it could be improved (see the survey [3]). His method takes into account that multiplication by constants of the form $\pm 1 + a\mathbf{i}$ or $a \pm \mathbf{i}$ can be performed in two real additions-subtractions and two real multiplications.

Theorem 4. *A DFT of order 2^k over $\mathbb{C}$ can be implemented using at most $(8/3)k2^k$ additions-subtractions and at most $(10/9)k2^k + 2^{k+1}$ multiplications in $\mathbb{R}$.*

Proof. For $k \in \mathbb{N}$ and $j \in \mathbb{Z}$ we define real coefficients

$$\sigma_{k,j} = \prod_{l \ge 0} \max\left\{ \left|\cos \frac{4^l 2\pi j}{2^k}\right|, \left|\sin \frac{4^l 2\pi j}{2^k}\right| \right\}.$$

These coefficients satisfy the properties of symmetry $\sigma_{k,j} = \sigma_{k,-j}$ and periodicity $\sigma_{k,j} = \sigma_{k,j+2^{k-2}}$, which follows from the known relations

$$\sin x = -\sin(-x), \quad \cos x = \cos(-x),$$
$$\left\{ \left|\sin\left(x + \frac{\pi n}{2}\right)\right|, \left|\cos\left(x + \frac{\pi n}{2}\right)\right| \right\} = \{|\sin x|, |\cos x|\},$$

where $x \in \mathbb{R}$, $n \in \mathbb{Z}$. Moreover, for a primitive root $\zeta = e^{\frac{2\pi\mathbf{i}}{2^k}}$ of order 2^k, $(\sigma_{k-2,j}/\sigma_{k,j})\zeta^j$ has the form $\pm 1 + a\mathbf{i}$ or $a \pm \mathbf{i}$, since

$$\zeta^j = \cos\frac{2\pi j}{2^k} + \mathbf{i}\sin\frac{2\pi j}{2^k}, \qquad \frac{\sigma_{k,j}}{\sigma_{k-2,j}} = \max\left\{ \left|\cos\frac{2\pi j}{2^k}\right|, \left|\sin\frac{2\pi j}{2^k}\right| \right\}.$$

We will construct circuits for transforms

$$\Phi_{2^k}(\gamma_0,\dots,\gamma_{2^k-1}) = \mathrm{DFT}_{2^k,\zeta}[\mathbb{C}](\sigma_{k,0}^{-1}\gamma_0,\, \sigma_{k,1}^{-1}\gamma_1,\dots,\sigma_{k,2^k-1}^{-1}\gamma_{2^k-1}).$$

According to formula (2) with the choice of parameters $S = 2^{k-2}$ and $T = 4$ and the periodicity property of the coefficients $\sigma_{k,j}$, for the components φ_i of the transform Φ_{2^k} the following holds:

$$\varphi_{4s+t} = \sum_{j=0}^{S-1} (\zeta^4)^{js} \cdot \zeta^{jt} \cdot \sigma_{k,j}^{-1}\gamma_{(j),t}, \qquad \gamma_{(j),t} = \sum_{l=0}^{3} \gamma_{lS+j} \cdot \mathbf{i}^{lt}.$$

The components $\gamma_{(j),t}$, $t = 0,\dots,3$, of each of 2^{k-2} order-4 DFTs can be computed via 16 real additions-subtractions. Subsequent calculations for $t = 0,\ 1,\ 3$ are performed by the formulas

$$\begin{aligned}
\varphi_{4s} &= \sum_{j=0}^{S-1} (\zeta^4)^{js}\sigma_{k-2,j}^{-1} \cdot (\sigma_{k-2,j}/\sigma_{k,j}) \cdot \gamma_{(j),0},\\
\varphi_{4s+1} &= \sum_{j=0}^{S-1} (\zeta^4)^{js}\sigma_{k-2,j}^{-1} \cdot (\sigma_{k-2,j}/\sigma_{k,j})\zeta^j \cdot \gamma_{(j),1},\\
\varphi_{4s+3} &= \sum_{j=0}^{S-1} (\zeta^4)^{j(s+1)}\sigma_{k-2,j}^{-1} \cdot (\sigma_{k-2,j}/\sigma_{k,j})\zeta^{-j} \cdot \gamma_{(j),3}.
\end{aligned}$$

These calculations involve 2^{k-2} multiplications by real constants, 2^{k-1} multiplications by constants of the form $\pm 1 + a\mathbf{i}$ or $a \pm \mathbf{i}$, and three $\Phi_{2^{k-2}}$ transforms.

To compute the remaining components φ_{4s+2}, apply formula (2) with parameters $S' = 2^{k-3}$ and $T' = 8$:

$$\begin{aligned}
\varphi_{8s+2} &= \sum_{j=0}^{S'-1} (\zeta^8)^{js}\sigma_{k-3,j}^{-1} \cdot (\sigma_{k-3,j}/\sigma_{k-1,j})(\zeta^2)^j \cdot \gamma'_{(j),2},\\
\varphi_{8s+6} &= \sum_{j=0}^{S'-1} (\zeta^8)^{j(s+1)}\sigma_{k-3,j}^{-1} \cdot (\sigma_{k-3,j}/\sigma_{k-1,j})(\zeta^2)^{-j} \cdot \gamma'_{(j),6},
\end{aligned}$$

where

$$\begin{aligned}
\gamma'_{(j),2} &= (\sigma_{k-1,j}/\sigma_{k,j})\gamma_{(j),2} + (\sigma_{k-1,j+S'}/\sigma_{k,j+S'})\mathbf{i}\gamma_{(j+S'),2},\\
\gamma'_{(j),6} &= (\sigma_{k-1,j}/\sigma_{k,j})\gamma_{(j),2} - (\sigma_{k-1,j+S'}/\sigma_{k,j+S'})\mathbf{i}\gamma_{(j+S'),2}.
\end{aligned}$$

Note that $\sigma_{k-1,j} = \sigma_{k-1,j+S'}$. These calculations are performed via 2^{k-2} multiplications by real or imaginary constants, 2^{k-2} multiplications by constants of the form $\pm 1 + a\mathbf{i}$ or $a \pm \mathbf{i}$, and two $\Phi_{2^{k-3}}$ transforms.

Thus, for the numbers $\hat{F}_A^{\mathbb{R}}(2^k)$ of additive real operations and $\hat{F}_C^{\mathbb{R}}(2^k)$ of real scalar multiplications, we have the following recurrence relations:

$$\hat{F}_A^{\mathbb{R}}(2^k) \le 3\hat{F}_A^{\mathbb{R}}(2^{k-2}) + 2\hat{F}_A^{\mathbb{R}}(2^{k-3}) + 6 \cdot 2^k,$$
$$\hat{F}_C^{\mathbb{R}}(2^k) \le 3\hat{F}_C^{\mathbb{R}}(2^{k-2}) + 2\hat{F}_C^{\mathbb{R}}(2^{k-3}) + 2.5 \cdot 2^k,$$

which, in agreement with the initial data for $k \le 3$ obtained by the previous method, are resolved as

$$\hat{F}_A^{\mathbb{R}}(2^k) \le (8/3)k2^k, \qquad \hat{F}_C^{\mathbb{R}}(2^k) \le (10/9)k2^k.$$

It remains to notice that a circuit for the DFT of order 2^k is completed from a circuit for Φ_{2^k} via 2^k multiplications by real constants $\sigma_{k,j}$. □

A more accurate account of the operations allows to refine the estimates of Theorem 4 in the remainder term (see, e.g., [2]).

The complexity of the inverse DFT (up to multiplications by 2^{-k}, which can be combined with internal multiplications) in both considered algorithms is estimated in the same way as the complexity of the "forward" one, since a primitive root ζ^{-1} is the complex conjugate of ζ.

Let us consider the case when a DFT is applied to a vector with real components γ_j — this case is of interest when multiplying polynomials over $\mathbb{R}$. It turns out that the complexity of such DFT (we will call it *real-input DFT*) in this case can be reduced by approximately half compared to the general case.

Note that if all $\gamma_j \in \mathbb{R}$, then $\gamma^*_{N-j} = \overline{\gamma^*_j}$ for any j, where γ^*_j are determined from (1) and $^-$ denotes the complex conjugation operation.

Lemma 5. *A real-input DFT of order $4N$ can be implemented via a real-input DFT of order $2N$, a complex DFT of order N, $7N$ addition-subtraction operations, and $3N$ scalar multiplication operations in $\mathbb{R}$.*

Proof. To determine the components γ^*_k with even indices $k = 2s$, apply formula (2), assuming $S = 2N$ and $T = 2$:

$$\gamma^*_{2s} = \sum_{j=0}^{2N-1} (\zeta^2)^{js} \cdot (\gamma_j + \gamma_{2N+j}).$$

These calculations are reduced to the computation of an order-$2N$ real-input DFT and $2N$ additions in $\mathbb{R}$.

Among the components with odd indices, it is sufficient to compute only γ^*_{4s+1}, since $\gamma^*_{4s+3} = \overline{\gamma^*_{4(N-s-1)+1}}$. For this, apply (2) with parameters $S = N$ and $T = 4$:

$$\gamma^*_{4s+1} = \sum_{j=0}^{N-1} (\zeta^4)^{js} \cdot \zeta^j \cdot (\gamma_j - \gamma_{2N+j} + \mathbf{i}(\gamma_{N+j} - \gamma_{3N+j})).$$

To calculate the above components, it is sufficient to employ a DFT of order N, at most $2N$ subtractions in $\mathbb{R}$, and N scalar multiplications in $\mathbb{C}$. □

Another way to reduce a real-input DFT to a complex DFT of half the order can be found in [1].

An analogous statement can be proved about the complexity of the inverse real-input DFT — its input is a vector $(\gamma_0, \ldots, \gamma_{N-1})$ such that $\gamma_0 \in \mathbb{R}$ and $\gamma_{N-j} = \overline{\gamma_j}$ for any $j = 1, \ldots, N-1$. We call such a transform a *real-valued DFT*. A result similar to the one proved above holds for this DFT.

Lemma 6. *A real-valued DFT of order $4N$ can be implemented via a real-valued DFT of order $2N$, a complex DFT of order N, $7N$ addition-subtraction operations, and $3N$ scalar multiplication operations in $\mathbb{R}$.*

Proof. Applying formula (2) and the notation from Lemma 4 with the choice of parameters $S = 2$ and $T = 2N$, write

$$\gamma^*_{2Ns+t} = \omega_{(t),0} + (-1)^s \omega_{(t),1} = \gamma_{(0),t} + (-1)^s \zeta^t \gamma_{(1),t},$$

where $s = 0$, 1 and $t = 0, \ldots, 2N-1$,

$$\gamma_{(0),t} = \sum_{i=0}^{2N-1} \gamma_{2i} (\zeta^2)^{it}, \qquad \gamma_{(1),t} = \sum_{i=0}^{2N-1} \gamma_{2i+1} (\zeta^2)^{it}.$$

Given that the components $\omega_{(t),i}$ are already computed, all γ^*_j may be determined in $4N$ real additions and subtractions.

The vector with components $\omega_{(t),0} = \gamma_{(0),t}$ is the image of the real-valued DFT of order $2N$, since it is applied to the vector $(\gamma_0, \gamma_2, \ldots, \gamma_{2(2N-1)})$. To compute $\omega_{(t),1}$, represent $\gamma_{(1),t}$ in form (2) with the choice of parameters $S = 2$ and $T = N$:

$$\gamma_{(1),Ns'+t'} = \gamma'_{(0),t'} + (-1)^{s'} \zeta^{2t'} \gamma'_{(1),t'},$$

where $s' = 0$, 1 and $t' = 0, \ldots, N-1$,

$$\gamma'_{(0),t'} = \sum_{i=0}^{N-1} \gamma_{4i+1} (\zeta^4)^{it'}, \qquad \gamma'_{(1),t'} = \sum_{i=0}^{N-1} \gamma_{4i+3} (\zeta^4)^{it'}.$$

Due to $\gamma_{4N-j} = \overline{\gamma_j}$ we have

$$\gamma'_{(1),t'} = \sum_{i=0}^{N-1} \overline{\gamma_{4(N-i-1)+1}}(\zeta^4)^{it'} = \sum_{i'=0}^{N-1} \overline{\gamma_{4i'+1}}(\zeta^4)^{(N-1-i')t'} =$$

$$= \zeta^{-4t'} \overline{\sum_{i'=0}^{N-1} \gamma_{4i'+1}(\zeta^4)^{i't'}} = \zeta^{-4t'}\overline{\gamma'_{(0),t'}}.$$

Thus, the components $\omega_{(t),1}$ can be determined by the formulas:

$$\omega_{(Ns'+t'),1} = \mathbf{i}^{s'} \left(\zeta^{t'}\gamma'_{(0),t'} + (-1)^{s'}\zeta^{-t'}\overline{\gamma'_{(0),t'}}\right),$$

i.e.[3],

$$\omega_{(t'),1} = \mathrm{Re}(2\zeta^{t'}\gamma'_{(0),t'}), \qquad \omega_{(N+t'),1} = -\mathrm{Im}(2\zeta^{t'}\gamma'_{(0),t'}).$$

To compute all $\omega_{(t),1}$, one DFT of order N and N multiplications in $\mathbb{C}$ are sufficient. □

Resolving the recurrence relations following from the proved lemmas, using Theorem 4 we conclude:

Corollary 1. *Any of real-input and real-valued DFTs of order 2^k can be performed in $(4/3)k2^k+O(2^k)$ addition-subtraction operations and $(5/9)k2^k+O(2^k)$ scalar multiplication operations in $\mathbb{R}$.*

5. DFT in extension ring

If a ring $\mathbf{K}$ does not contain roots of unity of an appropriate order, then it is impossible to directly apply the method of Theorem 1 to multiply polynomials over $\mathbf{K}$. In the Schönhage—Strassen algorithm [7, 8] and similar ones, in such a case it is proposed to use an extension $\mathbf{K}_{2,n}(x) = \mathbf{K}[x]/(x^{2^n}+1)$, provided two is invertible in $\mathbf{K}$.

In the ring $\mathbf{K}_{2,n}(x)$, the DFT of order 2^{n+1} with primitive root x is defined (here and below, instead of elements of the factor ring $\mathbf{K}_{2,n}(x)$, which are classes of equivalent polynomials modulo $x^{2^n}+1$, we will use polynomials that are representatives of their classes).

Lemma 7. *A DFT of order 2^k over the ring $\mathbf{K}_{2,n}(x)$, $k \le n+1$, can be performed in $k2^{k+n}$ addition-subtraction operations in $\mathbf{K}$.*

[3] As usual, $\mathrm{Re}\, z$ and $\mathrm{Im}\, z$ denote the real and imaginary parts of $z \in \mathbb{C}$, respectively.

Proof. Representing elements of the ring $\mathbf{K}_{2,n}(x)$ by polynomials of degree at most 2^n-1, it is easy to see that addition or subtraction in $\mathbf{K}_{2,n}(x)$ corresponds to 2^n additions-subtractions in the ring $\mathbf{K}$, and multiplication by x^m — to a cyclic shift of coefficients with a change of sign for some of them. Thus, if the change of sign can be taken into account in subsequent calculations, multiplication by powers of the primitive root x is implemented "free of charge". To complete the proof, it now remains to apply (3). □

To implement multiplication in $\mathbf{K}_{2,n}(x)$, it is convenient to consider this ring as an extension of some ring $\mathbf{K}_{2,m}(y)$:

Lemma 8. *Let $m < n$. There is an isomorphism*

$$\mathbf{K}_{2,n}(x) \cong \mathbf{K}_{2,m}(y)[x]/(x^{2^{n-m}} - y), \tag{4}$$

generated by the substitution $x^{2^{n-m}} = y$.

Proof. The polynomial $f(x) \in \mathbf{K}_{2,n}(x)$ can be written as $f(x) = \sum_{i=0}^{2^{n-m}-1} f_i(x^{2^{n-m}})x^i$, where $\deg f_i < 2^m$. The substitution $x^{2^{n-m}} = y$ maps $f(x)$ to the polynomial $\sum_{i=0}^{2^{n-m}-1} f_i(y)x^i$. Assume $f_i(y) \in \mathbf{K}_{2,m}(y)$.

Obviously, the substitution generates a linear one-to-one mapping. It remains to verify that this mapping preserves the product, and due to linearity, the verification can be restricted to monic monomials. In the ring $\mathbf{K}_{2,n}(x)$,

$$x^{j_1 2^{n-m}+i_1} \cdot x^{j_2 2^{n-m}+i_2} = x^{j_3 2^{n-m}+i_3} = (-1)^k x^{j_4 2^{n-m}+i_3},$$

where

$$i_3 = (i_1 + i_2) \bmod 2^{n-m}, \qquad j_3 = j_1 + j_2 + (i_1 + i_2 - i_3)/2^{n-m},$$
$$j_4 = j_3 \bmod 2^m, \qquad k = (j_3 - j_4)/2^m.$$

On the other hand, in the ring $\mathbf{K}_{2,m}(y)[x]/(x^{2^{n-m}} - y)$ it is also true that

$$y^{j_1} x^{i_1} \cdot y^{j_2} x^{i_2} = y^{j_3} x^{i_3} = (-1)^k y^{j_4} x^{i_3}.$$

Evidently, the results of both multiplications turn into each other upon substitution $y = x^{2^{n-m}}$. □

It is important to note that the considered mapping is performed by a simple permutation of the coefficients. For example, the polynomial $x^3 + 2x^2 - 1 \in \mathbf{K}_{2,2}(x)$ corresponds to the polynomial $yx + (2y - 1) \in \mathbf{K}_{2,1}(y)[x]/(x^2 - y)$. Other isomorphisms can also be used to implement multiplication, see [3].

Theorem 5. *Multiplication in the ring* $\mathbf{K}_{2,n}(x)$ *can be performed using* $3 \cdot 2^n n(\log_2 n + O(1))$ *addition-subtraction operations,* $3 \cdot 2^{n+\lceil \log_2 n \rceil - 1}$ *multiplication operations, and* 2^n *scalar multiplication operations in* $\mathbf{K}$.

Proof. We apply (4) with the choice of parameter $m = \lceil n/2 \rceil$. The multiplication of polynomials over $\mathbf{K}_{2,m}(y)$ modulo $x^{2^{n-m}} - y$ is performed as the usual multiplication of polynomials of degree at most $2^{n-m} - 1$ with subsequent modulo reduction.

The multiplication is performed via three DFTs of order $2^{n-m+1} = 2^{\lfloor n/2 \rfloor + 1}$ and $2^{\lfloor n/2 \rfloor + 1}$ multiplications in the ring $\mathbf{K}_{2,m}(y)$, where the inverse DFT is computed up to a normalizing constant factor. The modulo reduction $x^{2^{n-m}} - y$ is implemented in 2^n additions-subtractions in $\mathbf{K}$. Finally, the result is multiplied by an appropriate power of 2^{-1}.

For the numbers $\mu_A(n)$ of additions and subtractions and $\mu_M(n)$ of non-scalar multiplications in the proposed circuit for $n \geq 2$ we obtain the recurrence relations:

$$\mu_A(n) \leq 2^{\lfloor n/2 \rfloor + 1} \mu_A(\lceil n/2 \rceil) + 3(\lfloor n/2 \rfloor + 1)2^{n+1} + 2^n,$$
$$\mu_M(n) \leq 2^{\lfloor n/2 \rfloor + 1} \mu_M(\lceil n/2 \rceil),$$

which are resolved exactly as promised if for $n = 1$ we apply the estimates $\mu_A(1) = 5$ and $\mu_M(1) = 3$. Otherwise, we can take $\mu_A(1) = 2$ and $\mu_M(1) = 4$. In the latter case the circuit will contain $2^{n+\lceil \log_2 n \rceil + 1}$ multiplications, but the total number of operations will be somewhat smaller. □

These complexity bound is asymptotically the best known. Multiplication of polynomials over $\mathbf{K}$ can now be performed by a circuit for multiplication in a suitable ring $\mathbf{K}_{2,n}(x)$.

6. Application of DFT of order 3^k

In a ring of characteristic 2, it is impossible to define a DFT of even order, so the problem of constructing and efficiently implementing (in the ring itself or in an extension) a DFT of odd order, preferably of order 3^k, is relevant. This problem is also actual for rings in which either there are primitive roots of order 3^k, or two is irreversible.

The components of the DFT of order 3 may be calculated by the formulas

$$\gamma_0^* = \gamma_0 + \gamma_1 + \gamma_2, \quad \gamma_1^* = \gamma_0 - \gamma_2 + \zeta(\gamma_1 - \gamma_2), \quad \gamma_2^* = \gamma_0 - \gamma_1 - \zeta(\gamma_1 - \gamma_2), \quad (5)$$

where ζ is a primitive root of order 3 in $\mathbf{K}$. These calculations can be performed in seven addition-subtraction operations and one scalar multiplication

(or six additions-subtractions and two multiplications). If char $\mathbf{K} = 2$, then five additions and one multiplication are sufficient.

From Lemma 4 it follows

Theorem 6. *A DFT of order 3^k can be implemented using at most $(7/3)k3^k$ addition-subtraction operations and $(k-1)3^k+1$ scalar multiplication operations. In a ring of characteristic 2, the number of additive operations is estimated as $(5/3)k3^k$.*

Proof. The stated estimates follow from the recurrence relations on the numbers $F_A(3^k)$ of additive operations and $F_C(3^k)$ of scalar multiplication operations in the method of Lemma 4:

$$F_A(3^k) = 3F_A(3^{k-1}) + 3^{k-1}F_A(3),$$
$$F_C(3^k) = 3F_C(3^{k-1}) + 3^{k-1}F_C(3) + 2 \cdot 3^{k-1} - 2$$

and the initial conditions: $F_C(3) = 1$, $F_A(3) = 7$ in the general case or $F_A(3) = 5$ for a ring of characteristic 2. □

If a ring $\mathbf{K}$ does not contain primitive roots of sufficiently large order 3^k, but 3 is invertible, then we can consider the extension $\mathbf{K}_{3,n}(x) = \mathbf{K}[x]/(x^{2\cdot 3^n} + x^{3^n} + 1)$, in which x is a primitive root of order 3^{n+1}.

In the ring $\mathbf{K}_{3,n}(x)$, addition (subtraction) is performed in $2 \cdot 3^n$ addition (subtraction) operations in $\mathbf{K}$, and the complexity of multiplication by x^m depends on m:

Lemma 9. *The complexity of multiplication by x^m up to a factor of ± 1 in the ring $\mathbf{K}_{3,n}(x)$ is $|m|$ subtraction operations in $\mathbf{K}$ if $-3^n \le m \le 3^n$, and 3^n subtraction operations, otherwise (i.e., if $3^n < m < 2 \cdot 3^n$).*

Proof. Let $0 \le m \le 3^n$. Write a polynomial $f(x) \in \mathbf{K}_{3,n}(x)$ as $a(x)x^{2\cdot 3^n - m} + b(x)$, where $\deg a < m$ and $\deg b < 2 \cdot 3^n - m$. In the ring $\mathbf{K}_{3,n}(x)$, the equality

$$f(x)x^m = b(x)x^m - a(x) - a(x)x^{3^n}$$

holds, from which it is clear that, not counting multiplications by -1, computing the coefficients of the product requires m subtractions in $\mathbf{K}$.

In the case $-3^n \le m < 0$, write $f(x) = b(x)x^{-m} + a(x)$. Then, due to

$$f(x)x^m = b(x) - a(x)x^{2\cdot 3^n} - a(x)x^{3^n}$$

computing the coefficients of the polynomial also requires $|m|$ subtractions.

Suppose $3^n < m < 2 \cdot 3^n$. Represent $f(x)$ as $a(x) + b(x)x^{2\cdot 3^n - m} + c(x)x^{-m}$, where $\deg a < 2 \cdot 3^n - m$, $\deg b < 3^n$, and $\deg c < m - 3^n$. Then computing $f(x)x^m$ requires 3^n subtractions, since

$$f(x)x^m = a(x)x^m - b(x)x^{3^n} + c(x) - b(x).$$

□

Lemma 10. *Any of the transforms* $\mathrm{DFT}_{3,\zeta}[\mathbf{K}_{3,n}(x)](\gamma_0, \zeta^{c_1}\gamma_1, \zeta^{c_2}\gamma_2)$*, where* $\zeta = x^{3^n}$*,* $c_1, c_2 \in \{0, 1, 2\}$*, can be performed in* $13 \cdot 3^n$ *addition-subtraction operations in* $\mathbf{K}$ *or in* $10 \cdot 3^n$ *addition operations if* $\operatorname{char} \mathbf{K} = 2$*.*

Proof. Despite the nine possibilities for choosing the parameters c_1, c_2, actually it is sufficient to consider three cases, for example, $(c_1, c_2) \in \{(0, 0), (0, 1), (1, 1)\}$. The components of any other transform are obtained by permuting the components of one of the three listed.

Consider the case $c_1 = c_2 = 0$, in which the transform is a usual DFT of order 3. Represent $\gamma_i \in \mathbf{K}_{3,n}(x)$ as $a_i(x) + x^{3^n} b_i(x)$, where a_i, b_i are polynomials of degree less than 3^n, $i = 0, 1, 2$. Then formulas (5) can be rewritten as

$$\begin{aligned}
\gamma_0^* &= (a_0 + a_1 + a_2) + x^{3^n}(b_0 + b_1 + b_2),\\
\gamma_1^* &= (a_0 - a_2 - (b_1 - b_2)) + x^{3^n}(b_0 - b_1 + a_1 - a_2),\\
\gamma_2^* &= (a_0 - a_1 + b_1 - b_2) + x^{3^n}(b_0 - b_2 - (a_1 - a_2)).
\end{aligned}$$

If we represent γ_2^* as

$$\gamma_2^* = a_0 - a_2 + ((b_1 - b_2) - (a_1 - a_2)) + x^{3^n}(b_0 - b_1 + ((b_1 - b_2) - (a_1 - a_2))),$$

then it becomes clear that all three components of γ_i^* can be calculated in 13 addition-subtraction operations with polynomials of degree at most $3^n - 1$.

In a ring of characteristic 2, the formulas for γ_i^* take the form

$$\begin{aligned}
\gamma_0^* &= (a_0 + a_1 + a_2) + x^{3^n}(b_0 + b_1 + b_2),\\
\gamma_1^* &= (a_0 + a_2 + b_1 + b_2) + x^{3^n}(b_0 + b_1 + a_1 + a_2),\\
\gamma_2^* &= (a_0 + a_1 + b_1 + b_2) + x^{3^n}(b_0 + b_2 + a_1 + a_2).
\end{aligned}$$

If we write

$$\gamma_2^* = \gamma_1^* + (a_1 + a_2) + x^{3^n}(b_1 + b_2),$$

then it is easy to verify that to compute the components γ_i^* we can do with 10 additions of polynomials of degree at most $3^n - 1$.

The other two cases are treated similarly. For example, the components of the transform parameterized by $c_1 = c_2 = 1$ have the form

$$(a_0 - b_1 - b_2) + x^{3^n}(b_0 - (b_1 - a_2 + b_2 - a_1)),$$
$$(a_0 - a_1 + b_1 - a_2) + x^{3^n}(b_0 + b_2 - a_1),$$
$$(a_0 + a_1 - a_2 + b_2) + x^{3^n}(b_0 + b_1 - a_2),$$

from which it is clear that they can be calculated in 13 addition-subtraction operations of polynomials of degree at most $3^n - 1$. The remaining cases for verification are left to the reader. □

Lemma 11. *A DFT of order 3^k over the ring $\mathbf{K}_{3,n}(x)$, where $k \le n+1$, can be implemented using at most $4.5k3^{n+k}$ addition-subtraction operations in $\mathbf{K}$, and in the case* $\operatorname{char}\mathbf{K} = 2$ *— at most $3.5k3^{n+k}$ addition operations.*

Proof. The implementation of a DFT of order 3^{k+1}, if we apply Lemma 4 with the choice of parameters $S = 3$ and $T = 3^k$, is reduced to performing 3^k DFTs of order 3, three DFTs of order 3^k and multiplications by $x^{3^{n-k}jt}$, where $j = 1, 2$ and $t = 1, \ldots, 3^k - 1$.

Let $m = c3^n + m'$, where $c \in \mathbb{Z}$ and $|m'| < 3^n/2$. Then, instead of multiplying by x^m, we will multiply by $x^{m'}$, transferring the multiplication by x^{c3^n} inside an outer DFT of order 3. Since the inputs of any of the outer DFTs are of the form $\gamma_{(0),t}$, $x^l\gamma_{(1),t}$, $x^{2l}\gamma_{(2),t}$, where $l = 3^{n-k}t < 3^n$, then when reducing to multiplications by $x^{m'}$, the outer DFT is replaced by one of the transforms of Lemma 10.

In the group of multiplications under consideration, multiplications by each of the powers $x^{m'}$, $m' = 3^{n-k}t$, $t = -(3^k - 1)/2, \ldots, (3^k - 1)/2$, are performed twice, since

$$\{2t \bmod 3^k \mid t = 1, \ldots, 3^k - 1\} = \{1, \ldots, 3^k - 1\}.$$

Counting the complexity of each such multiplication as $|m'|$, the complexity of all these multiplications is estimated as

$$4 \cdot 3^{n-k} \sum_{t=1}^{\frac{3^k-1}{2}} t = 3^{n-k} \cdot \frac{3^{2k} - 1}{2}$$

addition-subtraction operations in $\mathbf{K}$.

Thus, for the complexity $F_n(3^{k+1})$ of the constructed circuit, we have the recurrence relation

$$F_n(3^{k+1}) \le 3F_n(3^k) + 3^k F_n(3) + 3^{n+k}/2,$$

which, under the initial conditions $F_n(3) = 13 \cdot 3^n$ (or $F_n(3) = 10 \cdot 3^n$ for a ring of characteristic 2), is resolved as stated in the assertion of the lemma. $\square$

Lemma 12. *Multiplication in the ring* $\mathbf{K}_{3,1}(x)$ *can be accomplished in* 30 *addition-subtraction operations and* 27 *multiplication operations in* $\mathbf{K}$.

Proof. Represent polynomials $A(x), B(x) \in \mathbf{K}_{3,1}(x)$ to be multiplied as $A(x) = A_1(x)x^3 + A_0$, $B(x) = B_1(x)x^3 + B_0$, where $\deg A_i, B_i \le 2$. Compute their product via the Karatsuba method:

$$AB = A_1B_1x^6 + ((A_1 - A_0)(B_0 - B_1) + A_1B_1 + A_0B_0)x^3 + A_0B_0.$$

We denote $C = (A_1 - A_0)(B_0 - B_1) = C_1x^3 + C_0$, $D = A_0B_0 = D_1x^3 + D_0$, $E = A_1B_1 = E_1x^3 + E_0$, where $\deg C_0, D_0, E_0 \le 2$ and $\deg C_1, D_1, E_1 \le 1$. Then in the ring $\mathbf{K}_{3,1}(x)$, i.e. modulo $x^6 + x^3 + 1$, the following relation takes place:

$$\begin{aligned} AB &= Ex^6 + (C + D + E)x^3 + D = (C + D)x^3 + (D - E) = \\ &= ((D_0 - C_1) + C_0 - E_1)x^3 + ((D_0 - C_1) - E_0 - D_1) = G_1x^3 + G_0. \end{aligned}$$

The products C, D, E of polynomials of degree at most 2 are performed in a straightforward manner in 9 multiplications and 4 additions each. The remaining calculations are performed in 18 addition-subtraction operations: six of them are used to compute $A_1 - A_0$, $B_0 - B_1$, and 12 — to compute the linear combinations G_0, G_1. $\square$

Theorem 7. *Multiplication in the ring* $\mathbf{K}_{3,n}(x)$ *can be performed using* $13.5 \cdot 3^n n(\log_2 n + O(1))$ *addition-subtraction operations, at most* $3^{n+2} \cdot 2^{\lceil \log_2 n \rceil}$ *multiplication operations, and* $O(3^n)$ *scalar multiplication operations in* $\mathbf{K}$. *In the case of a ring of characteristic* 2, *the additive complexity is at most* $10.5 \cdot 3^n n(\log_2 n + O(1))$.

Proof. The proof of the theorem is similar to that of Theorem 5. For $n \ge 2$, represent the ring $\mathbf{K}_{3,n}(x)$ as an extension of the ring $\mathbf{K}_{3,m}(y)$ (an analogue of Lemma 8 holds):

$$\mathbf{K}_{3,n}(x) \cong \mathbf{K}_{3,m}(y)[x]/(x^{3^{n-m}} - y)$$

and choose $m = \lceil n/2 \rceil$. As in the binary case, the multiplication of polynomials over $\mathbf{K}_{3,m}(y)$ modulo $x^{3^{n-m}} - y$ may be performed as the usual multiplication of polynomials of degree at most $3^{n-m} - 1$ with subsequent modulo reduction.

Unlike the binary case (due to the absence of a DFT of order $2 \cdot 3^{n-m}$), six DFTs of order $3^{n-m} = 3^{\lfloor n/2 \rfloor}$ are employed for multiplication: three DFTs

are used in the usual way to compute the product modulo $x^{3^{n-m}} - 1$, and the other three are used to compute the product modulo $x^{3^{n-m}} - \alpha^{3^{n-m}}$, where $\alpha = y^{3^{n \bmod 2}}$, which reduces to the substitution $x = \alpha z$ and computing the product modulo $z^{3^{n-m}} - 1$. Indeed,

$$\big(f(x) \bmod (x^N - \alpha^N)\big) \mid_{x=\alpha z} = f(\alpha z) \bmod (z^N - 1).$$

The execution of any of the transforms $x = \alpha z$ and $z = x/\alpha$ is performed in the ring $\mathbf{K}_{3,n}(x)$ by $O(3^{n-m})$ operations of multiplication by powers of y in the ring $\mathbf{K}_{3,m}(y)$, i.e., in just $O(3^n)$ additive operations in $\mathbf{K}$, if we perform computations up to a factor of ± 1.

The reconstruction of a polynomial $f(x) \in \mathbf{K}_{3,m}(y)[x]$ of degree no greater than $2N-2$ from its remainders f_1 and f_α from division by $x^N - 1$ and $x^N - \alpha^N$, respectively, can be performed by the formula

$$f(x) = \frac{1}{\alpha^N - 1}\left((x^N - 1)f_\alpha - (x^N - \alpha^N)f_1\right).$$

Moreover, for $N = 3^{n-m}$, due to $\alpha^{2N} + \alpha^N + 1 = 0$, the factor $(\alpha^N - 1)^{-1}$ is equal to $-3^{-1}(\alpha^N + 2)$. It is clear that the described procedure for recovering a polynomial can also be performed in $O(3^{n-m})$ additions-subtractions and multiplications by powers of y in the ring $\mathbf{K}_{3,m}(y)$, i.e., in just $O(3^n)$ additions-subtractions in $\mathbf{K}$.

Reduction of a polynomial of degree less than $2 \cdot 3^{n-m}$ modulo $x^{3^{n-m}} - y$ also costs $O(3^{n-m})$ addition-subtraction operations and multiplications by powers of y in the ring $\mathbf{K}_{3,m}(y)$, that is, $O(3^n)$ additive operations in $\mathbf{K}$.

For the numbers $\mu_A(n)$ of additions-subtractions and $\mu_M(n)$ of nonscalar multiplications in this circuit for $n \geq 2$ we obtain the following recurrence relations:

$$\mu_A(n) \leq 2 \cdot 3^{\lfloor n/2 \rfloor}\mu_A(\lceil n/2 \rceil) + 6F_{\lceil n/2 \rceil}(3^{\lfloor n/2 \rfloor}) + O(3^n),$$
$$\mu_M(n) \leq 2 \cdot 3^{\lfloor n/2 \rfloor}\mu_M(\lceil n/2 \rceil),$$

where the value $F_{\lceil n/2 \rceil}$ is determined from Lemma 11. These relations are resolved as promised in the statement of the theorem if for $n = 1$ we apply the estimates of Lemma 12. □

Note that the method of Theorem 5 provides an asymptotic estimate $3N \log_2 N \log_2 \log_2 N$ for the complexity of polynomial multiplication of total degree at most $N - 1$, where $N = 2^k$, and the method of Theorem 7 in the case of a ring of characteristic 2 and $N = 2 \cdot 3^k$ — a close estimate $3.32N \log_2 N \log_2 \log_2 N$.

Remark. *Multiplication of binary trinomials can be performed via* 6 *multiplications and* 12 *additions-subtractions. Therefore, the estimates for the number of multiplications in Lemma* 12 *and, consequently, in Theorem* 7 *can be reduced by* 1.5 *times at the cost of some increase in the number of additive operations.*

7. Conclusion

The multiplication strategy in the case $2^{-1}, 3^{-1} \notin \mathbf{K}$ is indicated by the Cantor—Kaltofen method [4]. By the method of Theorems 5 and 7, only replacing the inverse transforms $\mathrm{DFT}_{N,\zeta}^{-1}$ with non-normalized transforms $\mathrm{DFT}_{N,\zeta^{-1}}$, compute the "almost products"

$$2^{N_1} fg = 2^{N_1} fg \bmod (x^{2^{n_1}} + 1), \quad 3^{N_2} fg = 3^{N_2} fg \bmod (x^{2 \cdot 3^{n_2}} + x^{3^{n_2}} + 1)$$

for suitable $n_i, N_i \in \mathbb{N}$, where f, g are polynomials being multiplied. Then, the product fg can be obtained as $q2^{N_1} fg + s3^{N_2} fg$, where q, s are Bezout coefficients from the equality $q2^{N_1} + s3^{N_2} = 1$.

However, the relevance of developing fast multiplication algorithms over such rather exotic rings seems insignificant for now.

The work was supported by RFBR, projects 08–01–00863 and 08–01–00632–a, program "Leading scientific schools", project NSh–4470.2008.1, and the fundamental research program of the Department of Mathematical Sciences of the Russian Academy of Sciences "Algebraic and combinatorial methods of mathematical cybernetics" (project "Synthesis and complexity of control systems").

References

1. Gashkov S. B. Remarks on the fast multiplication of polynomials, and Fourier and Hartley transforms // Discrete Math. and Appl. — 2000. — V. 10, no. 5. — P. 499–528.

2. Bernstein D. J. The tangent FFT // Proc. AAECC. LNCS. — 2007. — V. 4851. — P. 291–300.

3. Bernstein D. J. Fast multiplication and its applications // Algorithmic Number Theory, MSRI Publ. — 2008. — V. 44. — P. 325–384.

4. Cantor D., Kaltofen E. On fast multiplication of polynomials over arbitrary algebras // Acta Inf. — 1991. — V. 28, no. 7. — P. 693–701.

5. Cooley J., Tukew J. An algorithm for the machine calculation of complex Fourier series // Math. Comp. — 1965. — V. 19. — P. 297–301.

6. Good I. J. The interaction algorithm and practical Fourier analysis // J. R. Statist. Soc. B. — 1958. — V. 20, no. 2. — 361–372; 1960. — V. 22, no. 2. — 372–375.

7. Schönhage A. Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2 // Acta Inf. — 1977. — V. 7. — P. 395–398.

8. Schönhage A., Strassen V. Schnelle Multiplikation großer Zahlen // Computing. — 1971. — V. 7. — P. 271–282.