Advances in Intelligent Systems Research, volume 174
Proceedings of the 8th Scientific Conference on Information Technologies for Intelligent Decision Making Support (ITIDS 2020)

Development of a Fast Algorithm of Number-Theoretic Signal Transformation for OFDM Communication Systems Using UFMC Technology

Igor Kalmykov
Institute of Information Technologies and Telecommunications
North Caucasus Federal University
Stavropol, Russia
kia762@yandex.ru

Maksim Kalmykov
Institute of Information Technologies and Telecommunications
North Caucasus Federal University
Stavropol, Russia
kia762@yandex.ru

Evgeny Voloshin
Institute of Information Technologies and Telecommunications
North Caucasus Federal University
Stavropol, Russia
jec9999@mail.ru

Dmitriy Yurdanov*
Institute of Information Technologies and Telecommunications
North Caucasus Federal University
Stavropol, Russia
stavrodim77@yandex.ru

***Abstract*—Modern OFDM communication systems must have the property of adapting to the changing parameters of the communication channel. Intelligent decision support systems using UFMS technology can effectively solve this problem. The use of UFMS filtering allows you to select the optimal value of the cyclic prefix and increase the spectral efficiency of the OFDM signal. However, this increases the computational cost of performing digital filtering procedures, which leads to an increase in network latency. Therefore, the development of a fast algorithm for performing numerical-theoretical signal transformations for OFDM systems using UFMC technology is an urgent task.**

Keywords—OFDM, orthogonal signal transformations, fast Fourier transform, fast algorithms, number-theoretic transformations

I. INTRODUCTION

The current stage of social development is characterized by the constant growth of the requirements for the multi-service communication quality, which leads to the need for the development of high-speed data transmission systems. A special feature of such systems is the use of the Orthogonal Frequency Division Multiplexing (OFDM) method. The most popular one is the implementation of OFDM using the harmonic Fourier basis [1-4] in systems such as DVB-x, Wi-Fi, WiMAX, LTE, which are the undisputed leaders in the information transmission over channels with limited time-frequency resources [1,5,6]. However, the use of Fast Fourier Transform (FFT) is characterized by a number of shortcomings, due to the presence of two computational paths for processing the real and imaginary part of the signal, as well as rounding errors caused by using the sine and cosine functions as turning coefficients. Therefore, the development of new orthogonal signal transformation algorithms using integer arithmetic, which allows eliminating the mentioned shortcomings, is very urgent.

The main disadvantage of orthogonal signal transformations based on FFT is the use of trigonometric functions as an orthogonal basis. This problem can be solved by using the integer computation. Some works [2,7-9] propose to perform digital signal processing using the number-theoretic transformations (NTT). However, such integral signal transformations have low productivity, since they are similar to a discrete Fourier transform (DFT). Therefore, the purpose of the study is to increase the speed of performing orthogonal signal transformations by developing a fast number-theoretic transformations algorithm.

II. MATERIALS AND METHODS

Currently, Galois fields are applied in digital telecommunication systems mainly in the areas of corrective code development, and the formation of pseudo-random sequences. The use of finite fields for digital signal processing issues is restricted by the lack of existence criteria of fast algorithms for computing the number-theoretic transformations that are alternative to the Fourier transform. This restriction is due to the fact that, the modular arithmetic does not use primitive roots of any degree unit in contrast to the complex case. Therefore, the development of algorithms for NTT fast calculation and their existence criteria will improve the efficiency of info-communication systems.

For many practical DSP (digital signal processing) applications, a fast Fourier transform is used. The implementation of fast Fourier transform gives several options for organizing calculations, depending on how the sequence $x_0, x_1, x_2, \ldots, x_{N-1}$ of length N is divided into parts. In

case N is even it is possible to use the "time-thinning" option, which is defined as the sum of two points discrete Fourier transforms:

$$X(k) = \sum_{n=0}^{N/2-1} x_{2n} W_{N/2}^{nk} + W_N^k \sum_{n=0}^{N/2-1} x_{2n+1} W_{N/2}^{nk}, \qquad (1)$$

where $W_{N/2} = e^{-i\frac{2\pi}{N/2}}$, $i = \sqrt{-1}$, x_{2n}, x_{2n+1}, are subsequences of length $N/2$ with even and odd numbers, respectively.

Equation (1) shows that the FFT implementation is characterized by the presence of two computational paths affecting the design efforts and reliability of the DSP special processor. In addition, FFT uses irrational numbers as rotational coefficients, which reduces the accuracy of the calculations. To eliminate these shortcomings, the number-theoretic transformations should be used, defined in an algebraic system with ring or field properties [1,6,10].

Let GF(M) be a finite Galois field, G_N - a cyclic group of order N, $\varepsilon_N \in GF(M)$ - a primitive root of order N (ε_N an element of the field GF(M), that fulfils the condition $(\varepsilon_N)^N = 1 \bmod M$ and $(\varepsilon_N)^L \neq 1 \bmod M$ for any natural $L < N$). Then the number-theoretic transformations of the sequence $x_0, x_1, x_2, \ldots, x_{N-1}$, where $x_i \in G_N$ $k = 0,1,\ldots N-1$ is given as:

$$S(k) = \left(\sum_{n=0}^{N-1} x_n \times \varepsilon_N^{-kn} \right) \bmod M. \qquad (2)$$

The converse number-theoretic transformation is of the form:

$$x(n) = \left(N^{-1} \sum_{k=0}^{N-1} S_k \times \varepsilon_N^{kn} \right) \bmod M. \qquad (3)$$

It is obvious that NTT in its structure is best implemented using a digital element base. For example, if we take ε_N in the form of a power of two, then the multiplication in (2) and (3) by degrees of ε_N in the calculation of number-theoretic transformations are replaced by shifts of the code words and reduction of the shifted code words modulo M [2].

The work [6] showed the possibility of increasing the speed of NTT execution due to the use of the developed algorithm for applying modular codes. If the compound numbers of Mersenne are used as the number M, then expressions (2) and (3) can be reduced to multidimensional parallel processing.

The properties of number-theoretic transformations are isomorphic to the properties of the discrete Fourier transform. Therefore, there must be a possibility to compute number-theoretic transformations using fast algorithms similar to fast Fourier transform. Let us transfer the approaches used in constructing fast Fourier transform with time-thinning out from the field of complex numbers (1) to a Galois field GF(M). Taking into account (1) rewrite (2) in the form:

$$\begin{aligned} S(k) &= \left(\sum_{n=0}^{N/2-1} x_{2n} \times \varepsilon_N^{-2kn} + \sum_{n=0}^{N/2-1} x_{2n+1} \times \right. \\ &\left. \times \varepsilon_N^{-(2n+1)k} \right) \bmod M = \\ &= \left(\left(\sum_{n=0}^{N/2-1} x_{2n} \times \varepsilon_N^{-2kn} \right) \bmod M + \right. \\ &\left. + \left(\varepsilon_N^{-k} \sum_{n=0}^{N/2-1} x_{2n+1} \times \varepsilon_N^{-2nk} \right) \bmod M \right) \bmod M. \end{aligned} \qquad (4)$$

The expression (4) implies the decomposition N of point number-theoretic transformations into a sum of two number-theoretic transformations lengths $N/2$. Consider the following theorem [11].

Theorem. Let GF(M) be a finite Galois field, N - an even number, G_N - a cyclic group of order N, $\varepsilon_N \in GF(M)$ - a primitive root of order N, fulfilling the following condition:

$$(\varepsilon_N)^N = 1 \bmod M, \qquad (5)$$

then number-theoretic transformations of sequence $x_0, x_1, x_2, \ldots, x_{N-1}$, where $x_i \in G_N$ is represented as a sum of NTT subsequences with even x_{2n}, and odd x_{2n+1} numbers.

Proof. Condition (5) implies the existence of a primitive root $\varepsilon_{N/2} = (\varepsilon_N)^2 \bmod M$ of order $N/2$. Transform the expression (4) taking into account the equality (5):

$$\begin{aligned} S(k) == &\left(\left(\sum_{n=0}^{N/2-1} x_{2n} \times \varepsilon_N^{-2kn} \right) \bmod M + \right. \\ &\left. \left(\varepsilon_N^{-k} \sum_{n=0}^{N/2-1} x_{2n+1} \times \varepsilon_N^{-2nk} \right) \bmod M \right) \bmod M = \\ &= \left(\left(\sum_{n=0}^{N/2-1} x_{2n} \times \varepsilon_{N/2}^{-kn} \right) \bmod M + \right. \\ &\left. \left(\varepsilon_N^{-k} \sum_{n=0}^{N/2-1} x_{2n+1} \times \varepsilon_{N/2}^{-nk} \right) \bmod M \right) \bmod M = \\ &= \left(S_{11}(k) + \varepsilon_N^{-k} S_{12}(k) \right) \bmod M, \end{aligned} \qquad (6)$$

where $S_{11}(k)$ and $S_{12}(k)$ – are NTT sequences with even x_{2n}, and odd x_{2n+1} numbers.

Since $S_{11}(k)$ and $S_{12}(k)$ have dimension $N/2$, the formula (6) can only be used to calculate $S(k)$ for $0 \le k < N/2$. For the case, let us use the periodicity of number-theoretic transformations:

$$S_{11}(k+\frac{N}{2}) = S_{11}(k) \text{ and } S_{12}(k+\frac{N}{2}) = S_{12}(k). \qquad (7)$$

Taking (7) into account, for $N/2 \le k < N$ the formula (6) can be rewritten in the form:

$$S(k) = \left(S_{11}(k-\frac{N}{2}) + \left(\varepsilon_N^{-k} S_{12}(k-\frac{N}{2}) \right) \right) \bmod M. \qquad (8)$$

The theorem is proved.

Unlike fast Fourier transform in the field of complex numbers, in which the roots of any degree unit exist ($\sqrt[N]{1} = e^{i\frac{2\pi}{N}}$, $i = \sqrt{-1}$), the condition for representing the dimension of number-theoretic transformations in the form of a power of two is not sufficient for the existence of fast NTT with "time-thinning" because there are no roots in the finite fields of any degree unit. Let us consider the examples of the use of the proved theorem.

III. RESULTS AND DISCUSSION

Use the finite fields GF(17), GF(29) to calculate the number-theoretic transformations signal. Where the length of the input sequence of the field GF(17) is 16 samples, and in the final Galois field GF(29) the length of the input vector will be 28 samples.

A. Example 1.

Let us perform a number-theoretic transformation of a vector in the Galois field GF(17):

$$(x_0, x_1, x_2, \ldots, x_{15}) = (0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15).$$

Therefore prepare a chain of primitive roots: $\varepsilon_{16} = 3, \varepsilon_8 = 9, \varepsilon_4 = 13, \varepsilon_2 = 16$. Note that the given numbers fulfil the condition:

$$(\varepsilon_{16}^{-2}) \bmod 17 = (\varepsilon_8^{-1}) \bmod 17 = 2,$$
$$(\varepsilon_8^{-2}) \bmod 17 = (\varepsilon_4^{-1}) \bmod 17 = 4,$$
$$(\varepsilon_4^{-2}) \bmod 17 = (\varepsilon_2^{-1}) \bmod 17 = 16.$$

Let us imagine the developed fast algorithm of number-theoretic transformations modulo 17. At the first stage of the developed fast PPPS algorithm modulo 17 we obtain

$$S_{31}(0) = (x_0 + 16^0 x_8) \bmod 17 = 8;$$
$$S_{31}(1) = (x_0 + 16^{-1} x_8) \bmod 17 = 9;$$
$$S_{32}(0) = (x_4 + 16^0 x_{12}) \bmod 17 = 16;$$
$$S_{32}(1) = (x_4 + 16^{-1} x_{12}) \bmod 17 = 9;$$
$$S_{33}(0) = (x_2 + 16^0 x_{10}) \bmod 17 = 12;$$
$$S_{33}(1) = (x_2 + 16^{-1} x_{10}) \bmod 17 = 9;$$
$$S_{34}(0) = (x_6 + 16^0 x_{14}) \bmod 17 = 3;$$
$$S_{34}(1) = (x_6 + 16^{-1} x_{14}) \bmod 17 = 9;$$
$$S_{35}(0) = (x_1 + 16^0 x_9) \bmod 17 = 10;$$
$$S_{35}(1) = (x_1 + 16^{-1} x_9) \bmod 17 = 9;$$
$$S_{36}(0) = (x_5 + 16^0 x_{13}) \bmod 17 = 1;$$
$$S_{36}(1) = (x_5 + 16^{-1} x_{13}) \bmod 17 = 9;$$
$$S_{37}(0) = (x_3 + 16^0 x_{11}) \bmod 17 = 14;$$
$$S_{37}(1) = (x_3 + 16^{-1} x_{11}) \bmod 17 = 9;$$
$$S_{38}(0) = (x_7 + 16^0 x_{15}) \bmod 17 = 5;$$
$$S_{38}(1) = (x_7 + 16^{-1} x_{15}) \bmod 17 = 9.$$

At the second stage of the developed fast number-theoretic transformations algorithm modulo 17 we obtain

$$S_{21}(0) = (S_{31}(0) + 13^0 S_{32}(0)) \bmod 17 = 7;$$
$$S_{21}(1) = (S_{31}(1) + 13^{-1} S_{32}(1)) \bmod 17 = 11;$$
$$S_{21}(2) = (S_{31}(0) + 13^{-2} S_{32}(0)) \bmod 17 = 9;$$
$$S_{21}(3) = (S_{31}(1) + 13^{-3} S_{32}(1)) \bmod 17 = 7;$$
$$S_{22}(0) = (S_{33}(0) + 13^0 S_{34}(0)) \bmod 17 = 15;$$
$$S_{22}(1) = (S_{33}(1) + 13^{-1} S_{34}(1)) \bmod 17 = 11;$$
$$S_{22}(2) = (S_{33}(0) + 13^{-2} S_{34}(0)) \bmod 17 = 9;$$
$$S_{22}(3) = (S_{33}(1) + 13^{-3} S_{34}(1)) \bmod 17 = 7;$$
$$S_{23}(0) = (S_{35}(0) + 13^0 S_{36}(0)) \bmod 17 = 11;$$
$$S_{23}(1) = (S_{35}(1) + 13^{-1} S_{36}(1)) \bmod 17 = 11;$$
$$S_{23}(2) = (S_{35}(0) + 13^{-2} S_{36}(0)) \bmod 17 = 9;$$
$$S_{23}(3) = (S_{35}(1) + 13^{-3} S_{36}(1)) \bmod 17 = 7;$$
$$S_{24}(0) = (S_{37}(0) + 13^0 S_{38}(0)) \bmod 17 = 2;$$
$$S_{24}(1) = (S_{37}(1) + 13^{-1} S_{38}(1)) \bmod 17 = 11;$$
$$S_{24}(2) = (S_{37}(0) + 13^{-2} S_{38}(0)) \bmod 17 = 9;$$
$$S_{24}(3) = (S_{37}(1) + 13^{-3} S_{38}(1)) \bmod 17 = 7.$$

At the third stage of the developed fast number-theoretic transformations algorithm modulo 17, we get

$$S_{11}(0) = (S_{21}(0) + 9^0 S_{22}(0)) \bmod 17 = 5;$$
$$S_{11}(1) = (S_{21}(1) + 9^{-1} S_{22}(1)) \bmod 17 = 16;$$
$$S_{11}(2) = (S_{21}(2) + 9^{-2} S_{22}(2)) \bmod 17 = 11;$$
$$S_{11}(3) = (S_{21}(3) + 9^{-3} S_{22}(3)) \bmod 17 = 12;$$
$$S_{11}(4) = (S_{21}(0) + 9^{-4} S_{22}(0)) \bmod 17 = 9;$$
$$S_{11}(5) = (S_{21}(1) + 9^{-5} S_{22}(1)) \bmod 17 = 6;$$
$$S_{11}(6) = (S_{21}(2) + 9^{-6} S_{22}(2)) \bmod 17 = 7;$$
$$S_{11}(7) = (S_{21}(3) + 9^{-7} S_{22}(3)) \bmod 17 = 2;$$
$$S_{12}(0) = (S_{23}(0) + 9^0 S_{24}(0)) \bmod 17 = 13;$$
$$S_{12}(1) = (S_{23}(1) + 9^{-1} S_{24}(1)) \bmod 17 = 16;$$
$$S_{12}(2) = (S_{23}(2) + 9^{-2} S_{24}(2)) \bmod 17 = 11;$$
$$S_{12}(3) = (S_{23}(3) + 9^{-3} S_{24}(3)) \bmod 17 = 12;$$
$$S_{12}(4) = (S_{23}(0) + 9^{-4} S_{24}(0)) \bmod 17 = 9;$$
$$S_{12}(5) = (S_{23}(1) + 9^{-5} S_{24}(1)) \bmod 17 = 6;$$

$$S_{12}(6) = \left(S_{23}(2) + 9^{-6} S_{24}(2)\right) \bmod 17 = 7;$$
$$S_{12}(7) = \left(S_{23}(3) + 9^{-7} S_{24}(3)\right) \bmod 17 = 2.$$

In the fourth stage of the developed fast number-theoretic transformations algorithm modulo 17, we get

$$S(0) = \left(S_{11}(0) + 3^{0} S_{12}(0)\right) \bmod 17 = 1;$$
$$S(1) = \left(S_{11}(1) + 3^{-1} S_{12}(1)\right) \bmod 17 = 10;$$
$$S(2) = \left(S_{11}(2) + 3^{-2} S_{12}(2)\right) \bmod 17 = 16;$$
$$S(3) = \left(S_{11}(3) + 3^{-3} S_{12}(3)\right) \bmod 17 = 3;$$
$$S(4) = \left(S_{11}(4) + 3^{-4} S_{12}(4)\right) \bmod 17 = 11;$$
$$S(5) = \left(S_{11}(5) + 3^{-5} S_{12}(5)\right) \bmod 17 = 14;$$
$$S(6) = \left(S_{11}(6) + 3^{-6} S_{12}(6)\right) \bmod 17 = 12;$$
$$S(7) = \left(S_{11}(7) + 3^{-7} S_{12}(7)\right) \bmod 17 = 13;$$
$$S(8) = \left(S_{11}(0) + 3^{-8} S_{12}(0)\right) \bmod 17 = 9;$$
$$S(9) = \left(S_{11}(1) + 3^{-9} S_{12}(1)\right) \bmod 17 = 5;$$
$$S(10) = \left(S_{11}(2) + 3^{-10} S_{12}(2)\right) \bmod 17 = 6;$$
$$S(11) = \left(S_{11}(3) + 3^{-11} S_{12}(3)\right) \bmod 17 = 4;$$
$$S(12) = \left(S_{11}(4) + 3^{-12} S_{12}(4)\right) \bmod 17 = 7;$$
$$S(13) = \left(S_{11}(5) + 3^{-13} S_{12}(5)\right) \bmod 17 = 15;$$
$$S(14) = \left(S_{11}(6) + 3^{-14} S_{12}(6)\right) \bmod 17 = 2;$$
$$S(15) = \left(S_{11}(7) + 3^{-15} S_{12}(7)\right) \bmod 17 = 8.$$

B. Example 2.

Let us calculate the number-theoretic transformations of the input sample vector $\left(x_0,\ x_1,\ x_2,\ x_3 \ldots,\ x_{25},,\ x_{26},\ x_{27}\right) =$ $(0,\ 1,\ 2,\ 3, \ldots,\ 25,\ 26,\ 27)$ in the finite Galois field $GF(29)$. Therefore it is necessary to calculate the following chain of primitive roots:

$$\varepsilon_{28} = 2, \varepsilon_{14} = 4, \varepsilon_7 = 16.$$

To obtain specific values of the 28-point number-theoretic transformations, it is necessary to prepare the elements $S_{21}, S_{22}, S_{23}, S_{24}, S_{11}$ and S_{12}:

$$S_{21}(0) = (x_0 + x_4 + x_8 + x_{12} + x_{16} + $$
$$+ x_{20} + x_{24}) \bmod 29 = 26;$$
$$S_{21}(1) = (x_0\varepsilon_7^{-1\cdot 0} + x_4\varepsilon_7^{-1\cdot 1} + x_8\varepsilon_7^{-1\cdot 2} + x_{12}\varepsilon_7^{-1\cdot 3} + x_{16}\varepsilon_7^{-1\cdot 4} +$$
$$+ x_{20}\varepsilon_7^{-1\cdot 5} + x_{24}\varepsilon_7^{-1\cdot 6}) \bmod 29 = 3;$$
$$S_{21}(2) = (x_0\varepsilon_7^{-2\cdot 0} + x_4\varepsilon_7^{-2\cdot 1} + x_8\varepsilon_7^{-2\cdot 2} + x_{12}\varepsilon_7^{-2\cdot 3} + x_{16}\varepsilon_7^{-2\cdot 4} +$$
$$+ x_{20}\varepsilon_7^{-2\cdot 5} + x_{24}\varepsilon_7^{-2\cdot 6}) \bmod 29 = 25;$$
$$S_{21}(3) = (x_0\varepsilon_7^{-3\cdot 0} + x_4\varepsilon_7^{-3\cdot 1} + x_8\varepsilon_7^{-3\cdot 2} + x_{12}\varepsilon_7^{-3\cdot 3} + x_{16}\varepsilon_7^{-3\cdot 4} +$$
$$+ x_{20}\varepsilon_7^{-3\cdot 5} + x_{24}\varepsilon_7^{-3\cdot 6}) \bmod 29 = 6;$$
$$S_{21}(4) = (x_0\varepsilon_7^{-4\cdot 0} + x_4\varepsilon_7^{-4\cdot 1} + x_8\varepsilon_7^{-4\cdot 2} + x_{12}\varepsilon_7^{-4\cdot 3} + x_{16}\varepsilon_7^{-4\cdot 4} +$$
$$+ x_{20}\varepsilon_7^{-4\cdot 5} + x_{24}\varepsilon_7^{-4\cdot 6}) \bmod 29 = 24;$$
$$S_{21}(5) = (x_0\varepsilon_7^{-5\cdot 0} + x_4\varepsilon_7^{-5\cdot 1} + x_8\varepsilon_7^{-5\cdot 2} + x_{12}\varepsilon_7^{-5\cdot 3} + x_{16}\varepsilon_7^{-5\cdot 4} +$$
$$+ x_{20}\varepsilon_7^{-5\cdot 5} + x_{24}\varepsilon_7^{-5\cdot 6}) \bmod 29 = 5;$$
$$S_{21}(6) = (x_0\varepsilon_7^{-6\cdot 0} + x_4\varepsilon_7^{-6\cdot 1} + x_8\varepsilon_7^{-6\cdot 2} + x_{12}\varepsilon_7^{-6\cdot 3} + x_{16}\varepsilon_7^{-6\cdot 4} +$$
$$+ x_{20}\varepsilon_7^{-6\cdot 5} + x_{24}\varepsilon_7^{-6\cdot 6}) \bmod 29 = 27.$$

Similarly, we calculate 7-point number-theoretic transformations $S_{22} = (11, 3, 25, 6, 24, 5, 27)$,

$S_{23} = (4, 3, 25, 6, 24, 5, 27)$ and
$S_{24} = (18, 3, 25, 6, 24, 5, 27)$ for subsequences:
$(x_2, x_6, x_{10}, x_{14}, x_{18}, x_{22}, x_{26})$,
$(x_1, x_5, x_9, x_{13}, x_{17}, x_{21}, x_{25})$ and
$(x_3, x_7, x_{11}, x_{15}, x_{19}, x_{23}, x_{27})$.

In accordance with the theorem, summing the elements S_{21}, S_{22} and S_{23}, S_{24} obtaining 14-point NTT S_{11} and S_{12}:

$$S_{11}(0) = \left(S_{21}(0) + 4^{0} S_{22}(0)\right) \bmod 29 = 8;$$
$$S_{11}(1) = \left(S_{21}(1) + 4^{-1} S_{22}(1)\right) \bmod 29 = 11;$$
$$S_{11}(2) = \left(S_{21}(2) + 4^{-2} S_{22}(2)\right) \bmod 29 = 3;$$
$$S_{11}(3) = \left(S_{21}(3) + 4^{-3} S_{22}(3)\right) \bmod 29 = 7;$$
$$S_{11}(4) = \left(S_{21}(4) + 4^{-4} S_{22}(4)\right) \bmod 29 = 25;$$
$$S_{11}(5) = \left(S_{21}(5) + 4^{-5} S_{22}(5)\right) \bmod 29 = 12;$$
$$S_{11}(6) = \left(S_{21}(6) + 4^{-6} S_{22}(6)\right) \bmod 29 = 6;$$
$$S_{11}(7) = \left(S_{21}(7) + 4^{-7} S_{22}(7)\right) \bmod 29 = 15;$$
$$S_{11}(8) = \left(S_{21}(8) + 4^{-8} S_{22}(8)\right) \bmod 29 = 24;$$
$$S_{11}(9) = \left(S_{21}(9) + 4^{-9} S_{22}(9)\right) \bmod 29 = 18;$$
$$S_{11}(10) = \left(S_{21}(10) + 4^{-10} S_{22}(10)\right) \bmod 29 = 5;$$
$$S_{11}(11) = \left(S_{21}(11) + 4^{-11} S_{22}(11)\right) \bmod 29 = 23;$$
$$S_{11}(12) = \left(S_{21}(12) + 4^{-12} S_{22}(12)\right) \bmod 29 = 27;$$
$$S_{11}(13) = \left(S_{21}(13) + 4^{-13} S_{22}(13)\right) \bmod 29 = 19;$$
$$S_{12}(0) = \left(S_{23}(0) + 4^{0} S_{24}(0)\right) \bmod 29 = 22;$$
$$S_{12}(1) = \left(S_{23}(1) + 4^{-1} S_{24}(1)\right) \bmod 29 = 11;$$
$$S_{12}(2) = \left(S_{23}(2) + 4^{-2} S_{24}(2)\right) \bmod 29 = 3;$$
$$S_{12}(3) = \left(S_{23}(3) + 4^{-3} S_{24}(3)\right) \bmod 29 = 7;$$
$$S_{12}(4) = \left(S_{23}(4) + 4^{-4} S_{24}(4)\right) \bmod 29 = 25;$$
$$S_{12}(5) = \left(S_{23}(5) + 4^{-5} S_{24}(5)\right) \bmod 29 = 12;$$
$$S_{12}(6) = \left(S_{23}(6) + 4^{-6} S_{24}(6)\right) \bmod 29 = 6;$$
$$S_{12}(7) = \left(S_{23}(7) + 4^{-7} S_{24}(7)\right) \bmod 29 = 15;$$
$$S_{12}(8) = \left(S_{23}(8) + 4^{-8} S_{24}(8)\right) \bmod 29 = 24;$$
$$S_{12}(9) = \left(S_{23}(9) + 4^{-9} S_{24}(9)\right) \bmod 29 = 18;$$
$$S_{12}(10) = \left(S_{23}(10) + 4^{-10} S_{24}(10)\right) \bmod 29 = 5;$$
$$S_{12}(11) = \left(S_{23}(11) + 4^{-11} S_{24}(11)\right) \bmod 29 = 23;$$
$$S_{12}(12) = \left(S_{23}(12) + 4^{-12} S_{24}(12)\right) \bmod 29 = 27;$$
$$S_{12}(13) = \left(S_{23}(13) + 4^{-13} S_{24}(13)\right) \bmod 29 = 19.$$

Summarizing the elements S_{11} and S_{12} obtaining a 28-point number-theoretic transformations:

$S(k) = \left(S_{11}(k) + 2^{-k} S_{12}(k)\right) \bmod 29 = (1, 2, 11, 26, 3, 16, 7, 9, 25, 22, 12, 13, 6, 10, 15, 20, 24, 17, 18, 8, 5, 21, 23, 14, 27, 4, 19, 28),$

where $0 \le k \le 27$.

The formulated conditions for decomposability of the N-point NTT into transforms of a smaller dimension and the proof of the theorem allow us to develop fast algorithms for calculating orthogonal signal transformations in finite fields. It was demonstrated in examples 1 and 2.

The number-theoretic transformations algorithms are most effective at the length of the input data vector equal a power of two and when the condition (5) is satisfied. In this case, the division of the sequences into two parts can be continued until the two-element sequences are obtained, which was shown in Example 1.

Let us estimate the efficiency of the fast NTT algorithm with time-thinning due to the decomposition of the N-point transformation into several small ones. To calculate the N -point number-theoretic transformations according to formula (2) the N^2 operations is required. The highest acceleration of computations can be achieved at $N = 2^k$ and with the existence of a primitive order root N. The number of operations required can be estimated as $N \cdot \log_2(N)$. Thus, the computational efforts are reduced by $N/\log_2(N)$ in comparison with the direct use of formula (2).

IV. CONCLUSION

The main advantage of number-theoretic transformations in comparison with discrete Fourier transform is that the roots of one have a prime representation, which makes it possible to replace complex arithmetic in integer arithmetic in calculations. The use of fast number-theoretic transformations with time-thinning is relevant if the number of elements in the analyzed sequence is a power of two and only if there is a primitive root of the order of the length of the analyzed sequence in the finite Galois field GF(M). In this case, the developed algorithm of fast NTT signal is not an approximate algorithm, and the acceleration is achieved solely due to the optimal computing organization.

The developed algorithm for fast execution of number-theoretic transformations signal with time-thinning is intended for simultaneous calculation of all spectral coefficients S(k). If it is necessary to obtain the coefficient values for any k, it is preferable to use the direct number-theoretic transformations formula.

ACKNOWLEDGMENT

This work was supported by the Russian Foundation for Basic Research, project No. 18-07-01020.

REFERENCES

[1] Vlasov E.G. Finite fields in telecommunication applications. Theory and application of FEC, CRC, and M-sequences. Practical manual. Moscow: Infa-M, 2016. 285 p.

[2] McClellan J. H., Rader C. M. Number Theory in Digital Signal Processing; translated from English; edited by Yu.I. Manin. Moscow: Radio i svyaz', 1993. 356 p.

[3] Chernov V.M. A quasi-parallel algorithm for error-free convolution calculation in reduced Mersenne-Lucas codes. Komp'yuternaya optika. 2015. №2. pp. 241-248.

[4] LMS_W.K. Jenkins, B.A. Schnaufer, "Fault Tolerant Adaptive Filters Based on the Block LMS Algorithm", IEEE International Symposium on Circuits and Systems, 3-6 May 1993, Page(s):862 - 865.

[5] Jörg Arndt Matters Computational. Ideas, Algorithms, Source Code. - Springer Berlin Heidelberg 2011 – 731 p.

[6] Steven G. Johnson and Matteo Frigo, A modified split-radix FFT with fewer arithmetic operations, IEEE Transactions on Signal Processing 55 (2007), no. 1, - p.111-119.

[7] Arslan Kh., Chen Shi Ning. Ultra-wideband wireless communication. Moscow: Tekhnosfera, 2012. 550 p.

[8] Shaposhnikov A.V. Fast algorithm for calculating the number-theoretic transformation. Aktual'nye problemy sovremennoy nauki. 2013. №2. pp. 204-207.

[9] Anne O'Donnell, Chris J. Bleakley, Efficient Concurrent Error Detection and Correction of Soft Errors in NTT-based Convolutions. Published in: Signals and Systems Conference (ISSC 2009), IET Irish. Date Added to IEEE Xplore: 12 August 2010. Electronic ISBN: 978-1-84919-213-2. INSPEC Accession Number: 11260190. DOI: 10.1049/cp.2009.1724.

[10] Yurdanov D.V., Kalmykov M.I., Zhuravlev K.M., Kalmykov I.A. Use of number-theoretic transformations for communication systems with OFDM. Mezhdunarodnyy zhurnal prikladnykh i fundamental'nykh issledovaniy. 2017. № 3, Part 2. pp. 178-182.

[11] Yurdanov, D., Kalmykov, M., Gostev, D. The implementation of information and communication technologies with the use of modular codes. CEUR Workshop Proceedings 1837, 2017, pp. 206-212.