ТЕХНИЧЕСКИЕ НАУКИ

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

М. И. Калмыков [M. I. Kalmykov]
Д. В. Юрданов [D. V. Yurdanov]
И. А. Калмыков [I. A. Kalmykov]
И. Д. Ефременков [I. D. Efremenkov]

УДК 004.052.2

РАЗРАБОТКА АЛГОРИТМОВ ВЫЧИСЛЕНИЯ ТЕОРЕТИКО-ЧИСЛОВЫХ ПРЕОБРАЗОВАНИЙ СИГНАЛОВ С НАИМЕНЬШИМ ЧИСЛОМ УМНОЖЕНИЙ

THE DEVELOPMENT OF ALGORITHMS FOR CALCULATING THEORETICAL-NUMERICAL SIGNAL TRANSFORMATIONS WITH THE LEAST NUMBER OF MULTIPLICATIONS

ФГАОУ ВО Северо-Кавказский федеральный университет,
г. Ставрополь, Россия, e-mail: oleg_military@inbox.ru
North Caucasus Federal University, Stavropol, Russia, e-mail: oleg_military@inbox.ru

Аннотация. *При использовании дискретного преобразования Фурье (ДПФ) для решения задач цифровой обработки сигналов (ЦОС) возникают ошибки округления или усечения результатов операций до используемой специализированными процессорами (СП) длины слова. Указанные ошибки возникают в трактах вычисления действительной и мнимой частей сигнала. В конечных кольцах и полях Галуа может быть определено преобразование, свойства которого изоморфны свойствам ДПФ и лишенное указанных недостатков Поиск новых путей повышения эффективности цифровой обработки сигналов привел к активизации разработки математических моделей, обладающих свойствами конечных алгебраических структур.*

Материалы и методы. *Предлагаемый в данной работе подход построения алгоритмов вычисления теоретико-числовых преобразований (ТЧП) сигналов с минимальным количеством умножений, реализованный на основе идей Винограда и впервые описанный в работе, позволяет повысить скорость выполнения ТЧП.*

Результаты и обсуждения. *Алгоритмы разделяли на пять основных частей: переупорядочивание обрабатываемых данных, входные «модулярные» сложения, выходные «модулярные» умножения, переупорядочивание полученных данных. Для переупорядочивания обрабатываемых и полученных данных на подготовительном этапе выполняли «модулярные» операций сложения и умножения, исключив их из этапа выполнения. Также на подготовительном этапе проводили вычисление степеней элемента ε (порядка N) конечного кольца или поля Галуа.*

Заключение. *В ходе проведенных исследований показано, что использование предложенной математической модели и алгоритмов вычисления ТЧП требует приблизительно такого же числа «модулярных» сложений, что и «быстрый алгоритм ТЧП», при этом выигрыш по количеству «модулярных» умножений составляет около 80%. В связи с тем, что операция «модулярного» умножения является самой затратной с точки зрения времени выполнения, предложенные алгоритмы позволяют существенно снизить время необходимое для вычисления ТЧП.*

Ключевые слова: цифровая обработка сигналов, ортогональные преобразования сигналов, дискретное преобразование Фурье, алгоритмы Винограда, алгоритм Агарвала – Кули, теоретико-числовое преобразование.

Abstract. *When using a discrete Fourier transform (DFT) to solve digital signal processing (DSP) problems, errors occur in rounding or truncating the results of operations to the word length used by specialized processors (SP). These errors occur in the paths for calculating the real and imaginary parts of the signal. In finite rings and Galois fields, a transformation can be defined whose properties are isomorphic to the properties of DPF and the Search for new ways to improve the efficiency of digital signal processing has led to the activation of the development of mathematical models that have the properties of finite algebraic structures.*

Materials and methods. *The approach proposed in this paper for constructing algorithms for calculating number-theoretic transformations (PPPS) of signals with a minimum number of multiplications, implemented on the basis of Grape's ideas and first described in this paper, allows increasing the speed of PPPS.*

Results and discussions. *The algorithms were divided into five main parts: reordering the processed data, input "modular" additions, output "modular" multiplications, and reordering the received data. To reorder the processed and received data, "modular" addition and multiplication operations were performed at the preparatory stage, excluding them from the execution stage. Also, at the preparatory stage, the powers of an element ε (order N) of a finite ring or Galois field were calculated.*

Conclusion. *In the course of the research, it is shown that the use of the proposed mathematical model and algorithms for calculating the PPP requires approximately the same number of "modular" additions as the "fast PPP algorithm", while the gain in the number of" modular " multiplications is about 80%. Due to the fact that the "modular" multiplication operation is the most expensive in terms of execution time, the proposed algorithms can significantly reduce the time required for calculating the PPI.*

Key words: digital signal processing, orthogonal signal transformations, discrete Fourier transform, Vinograd algorithms, Agarwal-Cooley algorithm, number-theoretic transformation.

Введение. При использовании дискретного преобразования Фурье (ДПФ) для решения задач цифровой обработки сигналов (ЦОС) возникают ошибки округления или усечения результатов операций до используемой специализированными процессорами (СП) длины слова. Указанные ошибки возникают в трактах вычисления действительной и мнимой частей сигнала. В конечных кольцах и полях Галуа может быть определено преобразование, свойства которого изоморфны свойствам ДПФ и лишенное указанных недостатков [1, 2]. Поэтому разработка производительных алгоритмов ЦОС, использующих преимущества целочисленной арифметики и позволяющих устранить отмеченные недостатки ДПФ, является актуальной задачей.

Цель исследования

В работах [1, 2, 3, 4, 5, 6, 7] рассмотрена возможность использования ТЧП в качестве альтернативы ДПФ при решении задач ЦОС. В [1, 6] построен «модулярный» аналог быстрого преобразования Фурье (БПФ), позволяющий вычислять ТЧП за $N \cdot \log_2(N)$ умножений. Кроме этого, в [7] показана возможность повышения скорости выполнения ТЧП в 2,5 раза по сравнению с классическим алгоритмом за счет использования параллельно-конвейерных методов вычисления, реализованных на чисто-систолических матрицах. Целью работы является повышение скорости выполнения ТЧП, определенного для последовательности целых чисел $(x_0, x_1, \ldots, x_{N-2}, x_{N-1})$ по формуле $S_k = \left(\sum_{n=0}^{N-1} x_n \varepsilon_N^{kn}\right) \bmod M$, $k = 0,1,\ldots,N-1$ за счет разработки алгоритмов Винограда [3] для конечных алгебраических структур.

Материалы и методы исследования

В работе [3] описан вывод алгоритмов Винограда дискретного преобразования Фурье, основанный на представлении матрицы $N = N_1 \times N_2 \times \cdots \times N_\nu$ – точечного ДПФ, где N_l – взаимно-простые числа, в виде прямого произведения матриц N_l – точечных ДПФ:

$$W_N = W_{N_1} \otimes W_{N_2} \otimes \cdots \otimes W_{N_\nu}. \quad (1)$$

Вычисление N_l – точечных ДПФ сводится к вычислению круговых сверток за счет использования модульной арифметики в кольце полиномов. Кроме этого, показано, что алгоритмы Винограда требуют на 80% меньше операций умножения, при приблизительно равном числе операций сложения по сравнению с классическими алгоритмами БПФ.

Перенесем подходы, используемые при выводе алгоритмов Винограда ДПФ, описанные в [3], для построения эффективных алгоритмов вычисления ТЧП при $N = p$ и $N = p^\alpha$, где p – простое число, $\alpha > 1$.

1. Пусть $N = p$, тогда матрица ТЧП $H_p\big|_{k,n\neq 0}$ (без первых строки и столбца) в конечном кольце Z_M:

$$H_p\big|_{k,n\neq 0} = \begin{bmatrix} \varepsilon_p & \varepsilon_p^2 & \varepsilon_p^3 & \cdots & \varepsilon_p^{p-1} \\ \varepsilon_p^2 & \varepsilon_p^4 & \varepsilon_p^6 & \cdots & \varepsilon_p^{2(p-1)} \\ \varepsilon_p^3 & \varepsilon_p^6 & \varepsilon_p^9 & \cdots & \varepsilon_p^{3(p-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \varepsilon_p^{p-1} & \varepsilon_p^{2(p-1)} & \varepsilon_p^{3(p-1)} & \cdots & \varepsilon_p^{(p-1)(p-1)} \end{bmatrix} \bmod M, \quad (2)$$

где $\varepsilon_p \in Z_M$ –такое число, что $(\varepsilon_p)^p = 1 \bmod M$ и $(\varepsilon_p)^L \neq 1 \bmod M$, $\forall L, 0 < L < p$) перестановкой столбцов может быть преобразована в циклическую $(p-1)\times(p-1)$ матрицу $\widetilde{H}_{p-1}$. Взаимно-однозначное соответствие между показателями степени q и номерами элементов $\varepsilon_p^q \bmod M$ циклической матрицы $\widetilde{H}_{p-1}$ задается выражением:

$$q = a^n \bmod p, n = 0,\ldots,p-2, \quad (3)$$

где a – примитивный элемент конечного поля Галуа $GF(p)$.

2. Пусть $N = p^{\alpha}$, $\alpha > 1$ – целое число. Тогда вычисление N – точечного ТЧП в кольце Z_M можно свести к вычислению двух $p^{\alpha-1}$ – точечных ТЧП и одной $(p-1)p^{\alpha-1}$ – точечной циклической свертки в Z_M. Взаимно-однозначное соответствие между показателями степени q_k и номерами элементов $\varepsilon_{p^{\alpha}}^{q_k} \bmod M$ циклических матриц $\widetilde{H}_{(p-1)p^{\alpha-k}}$, $k = 1,\ldots,\alpha$ задается выражением:

$$q_k / p^{k-1} = a_k^{n_k} \bmod p^{\alpha+1-k},\ n_k = 0,\ldots,(p-1)p^{\alpha-k} - 1, \tag{4}$$

где a_k – элемент конечного поля Галуа $GF\left(p^{\alpha+1-k}\right)$ удовлетворяющий условию $a_k^{n_k} \neq 1 \bmod p^{\alpha+1-k}$, $n_k = 1,\ldots,(p-1)p^{\alpha-k} - 1$ и $a_k^{n} = 1 \bmod p^{\alpha+1-k}$ при $n = (p-1)p^{\alpha-k}$.

Результаты исследования и их обсуждение

Полученные алгоритмы можно разделить на пять основных частей: переупорядочивание обрабатываемых данных, входные «модулярные» сложения, выходные «модулярные» умножения, переупорядочивание полученных данных. Для переупорядочивания обрабатываемых и полученных данных требуется выполнение «модулярных» операций сложения и умножения, которые можно выполнить на подготовительном этапе, исключив их из этапа выполнения. Также на подготовительном этапе целесообразно провести вычисление степеней элемента ε (порядка N) конечного кольца или поля Галуа.

Пример 1. Пусть $N = p = 7$, $\varepsilon_7 \in Z_M$, примитивным элементом поля $GF(7)$ является $a = 3$, соответствие (3) имеет вид: $\begin{array}{cccccc} n & 0 & 1 & 2 & 3 & 4 & 5 \\ \hline q & 1 & 3 & 2 & 6 & 4 & 5 \end{array}$ и матрица $H_7\big|_{k,\,n\neq 0}$ преобразуется к виду:

$$\widetilde{H}_6 = \begin{bmatrix} \varepsilon_7^1 & \varepsilon_7^3 & \varepsilon_7^2 & \varepsilon_7^6 & \varepsilon_7^4 & \varepsilon_7^5 \\ \varepsilon_7^3 & \varepsilon_7^2 & \varepsilon_7^6 & \varepsilon_7^4 & \varepsilon_7^5 & \varepsilon_7^1 \\ \varepsilon_7^2 & \varepsilon_7^6 & \varepsilon_7^4 & \varepsilon_7^5 & \varepsilon_7^1 & \varepsilon_7^3 \\ \varepsilon_7^6 & \varepsilon_7^4 & \varepsilon_7^5 & \varepsilon_7^1 & \varepsilon_7^3 & \varepsilon_7^2 \\ \varepsilon_7^4 & \varepsilon_7^5 & \varepsilon_7^1 & \varepsilon_7^3 & \varepsilon_7^2 & \varepsilon_7^6 \\ \varepsilon_7^5 & \varepsilon_7^1 & \varepsilon_7^3 & \varepsilon_7^2 & \varepsilon_7^6 & \varepsilon_7^4 \end{bmatrix} \bmod M$$

Тогда искомое ТЧП последовательности целых чисел $x = (x_0, x_1, x_2, x_3, x_4, x_5, x_6)$ принимает вид:

$$S_0 = \left(\sum_{n=0}^{6} x_n\right) \bmod M;$$

$$\begin{bmatrix} S_1 \\ S_3 \\ S_2 \\ S_6 \\ S_4 \\ S_5 \end{bmatrix} = \left(\begin{bmatrix} x_0 \\ x_0 \\ x_0 \\ x_0 \\ x_0 \\ x_0 \end{bmatrix} + \left[\widetilde{H}_6\right] \cdot \begin{bmatrix} x_1 \\ x_3 \\ x_2 \\ x_6 \\ x_4 \\ x_5 \end{bmatrix} \right) \bmod M = \left(\begin{bmatrix} x_0 \\ x_0 \\ x_0 \\ x_0 \\ x_0 \\ x_0 \end{bmatrix} + \begin{bmatrix} y_1 \\ y_3 \\ y_2 \\ y_6 \\ y_4 \\ y_5 \end{bmatrix} \right) \bmod M. \tag{5}$$

Выражение (5) представляет сумму по модулю M столбца $(x_0, x_0, x_0, x_0, x_0, x_0)^T$ и 6-ти точечной циклической свертки $y = (y_1, y_3, y_2, y_6, y_4, y_5)^T$ последовательностей $\varepsilon = \left(\varepsilon_7^1, \varepsilon_7^3, \varepsilon_7^2, \varepsilon_7^6, \varepsilon_7^4, \varepsilon_7^5\right)$ и $x = (x_1, x_3, x_2, x_6, x_4, x_5)$. Для вычисления циклической свертки построим «модулярный» аналог алгоритма Агарваля – Кули [1], являющийся методом представления одномерной $N-1=6$-ти точечной свертки в виде двумерной $(N_1 \times N_2) = 2 \times 3$ – точечной циклической свертки.

Сопоставим индексам $n = 0,1,\ldots,5$ элементов последовательностей y, ε, x пару координат $(n_1, n_2) = ((n) \bmod 2, (n) \bmod 3)$, получим взаимно-однозначное соответствие:

$$0 \to (0,0),\ 1 \to (1,1),\ 2 \to (0,2),\ 3 \to (1,0),\ 4 \to (0,1),\ 5 \to (1,2).$$

Переупорядочим лексикографически элементы вектора y в соответствии с координатами (n_1, n_2) получим $(y_1, y_4, y_2, y_6, y_3, y_5)^T$, искомая круговая свертка принимает вид:

$$\begin{bmatrix} y_1 \\ y_4 \\ y_2 \\ y_6 \\ y_3 \\ y_5 \end{bmatrix} = \left(\begin{bmatrix} \varepsilon_7^1 & \varepsilon_7^4 & \varepsilon_7^2 & \varepsilon_7^6 & \varepsilon_7^3 & \varepsilon_7^5 \\ \varepsilon_7^4 & \varepsilon_7^2 & \varepsilon_7^1 & \varepsilon_7^3 & \varepsilon_7^5 & \varepsilon_7^6 \\ \varepsilon_7^2 & \varepsilon_7^1 & \varepsilon_7^4 & \varepsilon_7^5 & \varepsilon_7^6 & \varepsilon_7^3 \\ \varepsilon_7^6 & \varepsilon_7^3 & \varepsilon_7^5 & \varepsilon_7^1 & \varepsilon_7^4 & \varepsilon_7^2 \\ \varepsilon_7^3 & \varepsilon_7^5 & \varepsilon_7^6 & \varepsilon_7^4 & \varepsilon_7^2 & \varepsilon_7^1 \\ \varepsilon_7^5 & \varepsilon_7^6 & \varepsilon_7^3 & \varepsilon_7^2 & \varepsilon_7^1 & \varepsilon_7^4 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_4 \\ x_2 \\ x_6 \\ x_3 \\ x_5 \end{bmatrix} \right) \bmod M =$$

$$= \left(\begin{bmatrix} \begin{bmatrix} \varepsilon_7^1 & \varepsilon_7^4 & \varepsilon_7^2 \\ \varepsilon_7^4 & \varepsilon_7^2 & \varepsilon_7^1 \\ \varepsilon_7^2 & \varepsilon_7^1 & \varepsilon_7^4 \end{bmatrix} & \begin{bmatrix} \varepsilon_7^6 & \varepsilon_7^3 & \varepsilon_7^5 \\ \varepsilon_7^3 & \varepsilon_7^5 & \varepsilon_7^6 \\ \varepsilon_7^5 & \varepsilon_7^6 & \varepsilon_7^3 \end{bmatrix} \\ \begin{bmatrix} \varepsilon_7^6 & \varepsilon_7^3 & \varepsilon_7^5 \\ \varepsilon_7^3 & \varepsilon_7^5 & \varepsilon_7^6 \\ \varepsilon_7^5 & \varepsilon_7^6 & \varepsilon_7^3 \end{bmatrix} & \begin{bmatrix} \varepsilon_7^1 & \varepsilon_7^4 & \varepsilon_7^2 \\ \varepsilon_7^4 & \varepsilon_7^2 & \varepsilon_7^1 \\ \varepsilon_7^2 & \varepsilon_7^1 & \varepsilon_7^4 \end{bmatrix} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_4 \\ x_2 \\ x_6 \\ x_3 \\ x_5 \end{bmatrix} \right) \bmod M \tag{6}$$

Перепишем выражение (6), принимая во внимание, что матрица выражения (6) является циклической матрицей размера $2 \times 2 \left(N_1 \times N_1\right)$, элементами которой являются циклические матрицы размера $3 \times 3 \left(N_2 \times N_2\right)$:

$$\begin{bmatrix} Y_0 \\ Y_1 \end{bmatrix} = \left(\begin{bmatrix} \mathrm{E}_0 & \mathrm{E}_1 \\ \mathrm{E}_1 & \mathrm{E}_0 \end{bmatrix} \cdot \begin{bmatrix} X_0 \\ X_1 \end{bmatrix} \right) \bmod M, \tag{7}$$

где

$$Y_0 = \left(y_1, y_4, y_2\right)^T; Y_1 = \left(y_6, y_3, y_5\right)^T;$$
$$X_0 = \left(x_1, x_4, x_2\right)^T; X_1 = \left(x_6, x_3, x_5\right)^T;$$
$$\mathrm{E}_0 = \begin{bmatrix} \varepsilon_7^1 & \varepsilon_7^4 & \varepsilon_7^2 \\ \varepsilon_7^4 & \varepsilon_7^2 & \varepsilon_7^1 \\ \varepsilon_7^2 & \varepsilon_7^1 & \varepsilon_7^4 \end{bmatrix}; \mathrm{E}_1 = \begin{bmatrix} \varepsilon_7^6 & \varepsilon_7^3 & \varepsilon_7^5 \\ \varepsilon_7^3 & \varepsilon_7^5 & \varepsilon_7^6 \\ \varepsilon_7^5 & \varepsilon_7^6 & \varepsilon_7^3 \end{bmatrix}$$

Выражение (7) представляет из себя двухэлементную циклическую свертку (элементами являются строки длины 3) и может быть вычислено в кольце Z_M следующим образом:

$$M_1 = \left(\frac{\mathrm{E}_0 + \mathrm{E}_1}{2} \cdot \left(X_0 + X_1\right) \right) \bmod M = \left(\frac{1}{2} \cdot \begin{bmatrix} \varepsilon_7^1 + \varepsilon_7^6 & \varepsilon_7^4 + \varepsilon_7^3 & \varepsilon_7^2 + \varepsilon_7^5 \\ \varepsilon_7^4 + \varepsilon_7^3 & \varepsilon_7^2 + \varepsilon_7^5 & \varepsilon_7^1 + \varepsilon_7^6 \\ \varepsilon_7^2 + \varepsilon_7^5 & \varepsilon_7^1 + \varepsilon_7^6 & \varepsilon_7^4 + \varepsilon_7^3 \end{bmatrix} \cdot \begin{bmatrix} x_1 + x_6 \\ x_4 + x_3 \\ x_2 + x_5 \end{bmatrix} \right) \bmod M; \tag{8}$$

$$M_2 = \left(\frac{\mathrm{E}_0 - \mathrm{E}_1}{2} \cdot \left(X_0 - X_1\right) \right) \bmod M = \left(\frac{1}{2} \cdot \begin{bmatrix} \varepsilon_7^1 - \varepsilon_7^6 & \varepsilon_7^4 - \varepsilon_7^3 & \varepsilon_7^2 - \varepsilon_7^5 \\ \varepsilon_7^4 - \varepsilon_7^3 & \varepsilon_7^2 - \varepsilon_7^5 & \varepsilon_7^1 - \varepsilon_7^6 \\ \varepsilon_7^2 - \varepsilon_7^5 & \varepsilon_7^1 - \varepsilon_7^6 & \varepsilon_7^4 - \varepsilon_7^3 \end{bmatrix} \cdot \begin{bmatrix} x_1 - x_6 \\ x_4 - x_3 \\ x_2 - x_5 \end{bmatrix} \right) \bmod M; \tag{9}$$

$$Y_0 = \left(M_1 + M_2\right) \bmod M; Y_1 = \left(M_1 - M_2\right) \bmod M \tag{10}$$

Таким образом, вычисление 2-точечной свертки (7) сводится к вычислению 2-х 3-точечных круговых сверток M_1 и M_2 по формулам (8) и (9) в кольце Z_M.

В [4] приведен алгоритм вычисления 3-х точечной циклической свертки вещественных последовательностей, использующий 4 умножения и 11 сложений. Использование указанного алгоритма для вычисления свертки в кольце Z_M возможно в случае существования элемента $3^{-1} \in Z_M$.

Вычислим ТЧП последовательности $x = \left(x_0, x_1, x_2, x_3, x_4, x_5, x_6\right) = \left(1, 2, 3, 4, 5, 6, 7\right)$ в кольце Z_{5419}, используя элемент $\varepsilon_7 = 4096$. Поскольку в Z_{5419} существуют элементы $2^{-1} = 2710$ и $3^{-1} = 3613$, использование алгоритма 3-х точечной циклической свертки [4] последовательностей $\left(4096, 64, 5411\right)$, $\left(2, 5, 3\right)$ и $\left(4907, 5165, 2032\right)$, $\left(7, 4, 6\right)$ позволяет вычислить $M_1 = \left(2705, 2705, 2705\right)^T$, $M_2 = \left(2537, 2111, 1508\right)^T$ за 8 умножений и 22 сложений в

кольце Z_{5419}. Аналогичный результат получается при использовании формул (8) и (9) за 18 умножений и 36 сложений в кольце Z_{5419}. Вычисления по формуле (10) дают $Y_0 = (5242, 4816, 4213)^T$ **и** $Y_1 = (168, 594, 1197)^T$ за 6 сложений в кольце Z_{5419}. Подставив $(Y_0, Y_1)^T = (y_1, y_4, y_2, y_6, y_3, y_5)^T = (5242, 4816, 4213, 168, 594, 1197)^T$ в (5), получаем искомое 7-ми точечное ТЧП $(S_0, S_1, S_2, S_3, S_4, S_5, S_6) = (28, 5243, 4214, 595, 4817, 1198, 169)$ за 8 умножений и 40 сложений в кольце Z_{5419}.

Пример 2. Пусть $N = p^{\alpha} = 3^2$, $\varepsilon_9 \in Z_M$, в этом случае $k = 1, 2$, $a_1 = a_2 = 2$ и соответствие (4) принимает вид: $\begin{matrix} n_1 & 0 & 1 & 2 & 3 & 4 & 5 \\ q_1 & 1 & 2 & 4 & 8 & 7 & 5 \end{matrix}$, $\begin{matrix} n_2 & 0 & 1 \\ q_2 & 3 & 6 \end{matrix}$. Осуществив перестановку строк и столбцов матричного представления 9-ти точечного ТЧП получаем:

$$\begin{bmatrix} S_0 \\ S_3 \\ S_6 \\ S_1 \\ S_2 \\ S_4 \\ S_8 \\ S_7 \\ S_5 \end{bmatrix} = \left(\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & \varepsilon_9^3 & \varepsilon_9^6 & \varepsilon_9^3 & \varepsilon_9^6 & \varepsilon_9^3 & \varepsilon_9^6 \\ 1 & 1 & 1 & \varepsilon_9^6 & \varepsilon_9^3 & \varepsilon_9^6 & \varepsilon_9^3 & \varepsilon_9^6 & \varepsilon_9^3 \\ 1 & \varepsilon_9^3 & \varepsilon_9^6 & \varepsilon_9^1 & \varepsilon_9^2 & \varepsilon_9^4 & \varepsilon_9^8 & \varepsilon_9^7 & \varepsilon_9^5 \\ 1 & \varepsilon_9^6 & \varepsilon_9^3 & \varepsilon_9^2 & \varepsilon_9^4 & \varepsilon_9^8 & \varepsilon_9^7 & \varepsilon_9^5 & \varepsilon_9^1 \\ 1 & \varepsilon_9^3 & \varepsilon_9^6 & \varepsilon_9^4 & \varepsilon_9^8 & \varepsilon_9^7 & \varepsilon_9^5 & \varepsilon_9^1 & \varepsilon_9^2 \\ 1 & \varepsilon_9^6 & \varepsilon_9^3 & \varepsilon_9^8 & \varepsilon_9^7 & \varepsilon_9^5 & \varepsilon_9^1 & \varepsilon_9^2 & \varepsilon_9^4 \\ 1 & \varepsilon_9^3 & \varepsilon_9^6 & \varepsilon_9^7 & \varepsilon_9^5 & \varepsilon_9^1 & \varepsilon_9^2 & \varepsilon_9^4 & \varepsilon_9^8 \\ 1 & \varepsilon_9^6 & \varepsilon_9^3 & \varepsilon_9^5 & \varepsilon_9^1 & \varepsilon_9^2 & \varepsilon_9^4 & \varepsilon_9^8 & \varepsilon_9^7 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_3 \\ x_6 \\ x_1 \\ x_2 \\ x_4 \\ x_8 \\ x_7 \\ x_5 \end{bmatrix} \right) \bmod M =$$

$$= \left(\begin{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 1 & 1 \\ \varepsilon_9^3 & \varepsilon_9^6 & \varepsilon_9^3 \\ \varepsilon_9^6 & \varepsilon_9^3 & \varepsilon_9^6 \end{bmatrix} & \begin{bmatrix} 1 & 1 & 1 \\ \varepsilon_9^6 & \varepsilon_9^3 & \varepsilon_9^6 \\ \varepsilon_9^3 & \varepsilon_9^6 & \varepsilon_9^3 \end{bmatrix} \\ \begin{bmatrix} 1 & \varepsilon_9^3 & \varepsilon_9^6 \\ 1 & \varepsilon_9^6 & \varepsilon_9^3 \\ 1 & \varepsilon_9^3 & \varepsilon_9^6 \end{bmatrix} & \begin{matrix} \varepsilon_9^1 & \varepsilon_9^2 & \varepsilon_9^4 \\ \varepsilon_9^2 & \varepsilon_9^4 & \varepsilon_9^8 \\ \varepsilon_9^4 & \varepsilon_9^8 & \varepsilon_9^7 \end{matrix} & \begin{matrix} \varepsilon_9^8 & \varepsilon_9^7 & \varepsilon_9^5 \\ \varepsilon_9^7 & \varepsilon_9^5 & \varepsilon_9^1 \\ \varepsilon_9^5 & \varepsilon_9^1 & \varepsilon_9^2 \end{matrix} \\ \begin{bmatrix} 1 & \varepsilon_9^6 & \varepsilon_9^3 \\ 1 & \varepsilon_9^3 & \varepsilon_9^6 \\ 1 & \varepsilon_9^6 & \varepsilon_9^3 \end{bmatrix} & \begin{matrix} \varepsilon_9^8 & \varepsilon_9^7 & \varepsilon_9^5 \\ \varepsilon_9^7 & \varepsilon_9^5 & \varepsilon_9^1 \\ \varepsilon_9^5 & \varepsilon_9^1 & \varepsilon_9^2 \end{matrix} & \begin{matrix} \varepsilon_9^1 & \varepsilon_9^2 & \varepsilon_9^4 \\ \varepsilon_9^2 & \varepsilon_9^4 & \varepsilon_9^8 \\ \varepsilon_9^4 & \varepsilon_9^8 & \varepsilon_9^7 \end{matrix} \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_3 \\ x_6 \\ x_1 \\ x_2 \\ x_4 \\ x_8 \\ x_7 \\ x_5 \end{bmatrix} \right) \bmod M \qquad (11)$$

Выражение (11) можно свести к вычислению 6-ти точечной циклической свертки и двух 3-точечных ТЧП следующим образом:

$$\begin{bmatrix} \widetilde{S}_1 \\ \widetilde{S}_2 \\ \widetilde{S}_4 \\ \widetilde{S}_8 \\ \widetilde{S}_7 \\ \widetilde{S}_5 \end{bmatrix} = \left(\begin{bmatrix} \varepsilon_9^1 & \varepsilon_9^2 & \varepsilon_9^4 & \varepsilon_9^8 & \varepsilon_9^7 & \varepsilon_9^5 \\ \varepsilon_9^2 & \varepsilon_9^4 & \varepsilon_9^8 & \varepsilon_9^7 & \varepsilon_9^5 & \varepsilon_9^1 \\ \varepsilon_9^4 & \varepsilon_9^8 & \varepsilon_9^7 & \varepsilon_9^5 & \varepsilon_9^1 & \varepsilon_9^2 \\ \varepsilon_9^8 & \varepsilon_9^7 & \varepsilon_9^5 & \varepsilon_9^1 & \varepsilon_9^2 & \varepsilon_9^4 \\ \varepsilon_9^7 & \varepsilon_9^5 & \varepsilon_9^1 & \varepsilon_9^2 & \varepsilon_9^4 & \varepsilon_9^8 \\ \varepsilon_9^5 & \varepsilon_9^1 & \varepsilon_9^2 & \varepsilon_9^4 & \varepsilon_9^8 & \varepsilon_9^7 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_4 \\ x_8 \\ x_7 \\ x_5 \end{bmatrix} \right) \bmod M, \qquad (12)$$

$$\begin{bmatrix} S_0 \\ S_3 \\ S_6 \end{bmatrix} = \left(\begin{bmatrix} 1 & 1 & 1 \\ 1 & \varepsilon_9^3 & \varepsilon_9^6 \\ 1 & \varepsilon_9^6 & \varepsilon_9^3 \end{bmatrix} \cdot \begin{bmatrix} x_0 + x_3 + x_6 \\ x_1 + x_4 + x_7 \\ x_2 + x_5 + x_8 \end{bmatrix} \right) \bmod M, \qquad (13)$$

$$\begin{bmatrix}\hat{S}_0\\ \hat{S}_1\\ \hat{S}_2\end{bmatrix}=\begin{bmatrix}\hat{S}_3\\ \hat{S}_4\\ \hat{S}_5\end{bmatrix}=\begin{bmatrix}\hat{S}_6\\ \hat{S}_7\\ \hat{S}_8\end{bmatrix}=\left(\begin{bmatrix}1 & 1 & 1\\ 1 & \varepsilon_9^3 & \varepsilon_9^6\\ 1 & \varepsilon_9^6 & \varepsilon_9^3\end{bmatrix}\cdot\begin{bmatrix}x_0\\ x_3\\ x_6\end{bmatrix}\right)\bmod M, \quad (14)$$

$$\begin{bmatrix}S_1\\ S_2\\ S_4\\ S_8\\ S_7\\ S_5\end{bmatrix}=\left(\begin{bmatrix}\tilde{S}_1\\ \tilde{S}_2\\ \tilde{S}_4\\ \tilde{S}_8\\ \tilde{S}_7\\ \tilde{S}_5\end{bmatrix}+\begin{bmatrix}\hat{S}_1\\ \hat{S}_2\\ \hat{S}_4\\ \hat{S}_8\\ \hat{S}_7\\ \hat{S}_5\end{bmatrix}\right)\bmod M$$

Свертку (12) можно вычислить способом, описанным в примере 1, 3-точечные ТЧП (13) и (14) вычисляются с помощью 2-точечной циклической свертки [4], при этом легко подсчитать количество необходимы операций «модулярного» умножения – 19, сложения – 81.

Заключение. Применение ТЧП вместо ДПФ в задачах ЦОС позволяет устранить ошибки округления и усечения результатов операций [1, 2, 3, 5], при этом необходим один вычислительный тракт. В ходе проведенных исследований показано, что использование предложенной математической модели и алгоритмов вычисления ТЧП требует приблизительно такого же числа «модулярных» сложений, что и «быстрый алгоритм ТЧП» [6], при этом выигрыш по количеству «модулярных» умножений составляет около 80 %. В связи с тем, что операция «модулярного» умножения является самой затратной с точки зрения времени выполнения, предложенные алгоритмы позволяют существенно снизить время необходимое для вычисления ТЧП.

Финансирование: Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-37-00009.

ЛИТЕРАТУРА

1. Yurdanov D., Kalmykov M., Gostev D., Kalmykov I. The implementation of information and communication technologies with the use of modular codes. CEUR Workshop Proceedings 1837, 2017. – P. 206–212.

2. Абстрактные алгебраические системы и цифровая обработка сигналов / Вариченко Л. В., Лабунец В. Г., Раков М. А. Киев: Наук. Думка, 1986. – 248 с.

3. Макклеллан Дж. Г., Рейдер Ч. М. Применение теории чисел в цифровой обработке сигналов; пер. с англ. / под ред. Ю. И. Манина. М.: Радио и связь, 1993. – 356 с.

4. Нуссбаумер Г. Быстрое преобразование Фурье и алгоритмы вычисления сверток: Пер. с англ. М.: Радио и связь, 1985. 248 с., ил.

5. Юрданов Д. В., Калмыков М. И., Журавлев К. М., Калмыков И. А. Использование теоретико-числовых преобразований для систем связи с OFDM // Международный журнал прикладных и фундаментальных исследований. 2017. № 3–2. С. 178–182.

6. Юрданов Д. В., Калмыков М. И., Гостев Д. В., Калмыков И. А. Разработка быстрого алгоритма вычисления теоретико-числовых преобразований сигналов // Фундаментальные исследования. 2017. №10. Часть 1. С. 67–71.

7. Топоркова Е. В., Калмыков М. И., Степанова Е. П., Юрданов Д. В., Калмыков И. А. Разработка чисто-систолического алгоритма вычисления теоретико-числовых преобразований сигналов // Современная наука и инновации 2018. № 3. С. 28–36.

REFERENCES

1. Yurdanov D., Kalmykov M., Gostev D., Kalmykov I. The implementation of information and communication technologies with the use of modular codes. CEUR Workshop Proceedings 1837, 2017. – P. 206–212.

2. Abstraktnye algebraicheskie sistemy i tsifrovaya obrabotka signalov / Varichenko L. V., Labunets V. G., Rakov M. A. Kiev: Nauk. Dumka, 1986. 248 s.

3. Makklellan Dzh. G., Reyder Ch. M. Primenenie teorii chisel v tsifrovoy obrabotke signalov; per. s angl. / pod red. Yu. I. Manina. M.: Radio i svyaz', 1993. 356 s.

4. Nussbaumer G. Bystroe preobrazovanie Fur'e i algoritmy vychisleniya svertok: Per. s angl. M.: Radio i svyaz', 1985. 248 s., il.

5. Yurdanov D. V., Kalmykov M. I., Zhuravlev K. M., Kalmykov I. A. Ispol'zovanie teoretiko-chislovykh preobrazovaniy dlya sistem svyazi s OFDM // Mezhdunarodnyy zhurnal prikladnykh i fundamental'nykh issledovaniy. 2017. № 3–2. S. 178–182.

6. Yurdanov D. V., Kalmykov M. I., Gostev D. V., Kalmykov I. A. Razrabotka bystrogo algoritma vychisleniya teoretiko-chislovykh preobrazovaniy signalov // Fundamental'nye issledovaniya. 2017. №10. Chast' 1. S. 67–71.

7. Toporkova E. V., Kalmykov M. I., Stepanova E. P., Yurdanov D. V., Kalmykov I. A. Razrabotka chisto-sistolicheskogo algoritma vychisleniya teoretiko-chislovykh preobrazovaniy signalov // Sovremennaya nauka i innovatsii 2018. № 3. S. 28–36.

ОБ АВТОРАХ

Калмыков Максим Игоревич, аспирант кафедры Информационной безопасности автоматизированных систем ФГАОУ ВО «Северо-Кавказский федеральный университет» (СКФУ). 355009, г. Ставрополь, ул. Пушкина 1. Тел.: +79064710242; E-mail: kia762@yandex.ru

Kalmykov Maksim Igorevich, post-graduate student of the Department of information security of automated systems of North Caucasus Federal University (NCFU). 355009, Stavropol, Pushkin St., 1. Tel: +79064710242; E-mail: kia762@yandex.ru

Юрданов Дмитрий Владимирович, аспирант кафедры Информационной безопасности автоматизированных систем ФГАОУ ВО «Северо-Кавказский федеральный университет» (СКФУ). 355009, г. Ставрополь, ул. Пушкина 1. Тел.: +79188048327; E-mail: stavrodim77@yandex.ru

Yurdanov Dmitry Vladimirovich, post-graduate student of the Department of information security of automated systems of North Caucasus Federal University (NCFU). 355009, Stavropol, Pushkin St., 1. Tel: + 79188048327; E-mail: stavrodim77@yandex.ru

Калмыков Игорь Анатольевич, доктор технических наук, профессор, профессор кафедры Информационной безопасности автоматизированных систем ФГАОУ ВО «Северо-Кавказский федеральный университет» (СКФУ). 355009, г. Ставрополь, ул. Пушкина 1. Тел.: +79187733001; E-mail: kia762@yandex.ru

Kalmykov Igor Anatolyevich, doctor of technical Sciences, Professor, Professor of the Department of Information security of automated systems of North Caucasus Federal University (NCFU). 355009, Stavropol, Pushkin St., 1. Tel: + 79187733001; E-mail: kia762@yandex.ru

Ефременков Иван Дмитриевич, аспирант кафедры Информационной безопасности автоматизированных систем ФГАОУ ВО «Северо-Кавказский федеральный университет» (СКФУ). 355009, г. Ставрополь, ул. Пушкина 1. Тел.: +79188048327; E-mail: stavrodim77@yandex.ru

Efremenkov Ivan Dmitrievich, post-graduate student of the Department of information security of automated systems of North Caucasus Federal University (NCFU). 355009, Stavropol, Pushkin St., 1. Tel: + 79188048327; E-mail: stavrodim77@yandex.ru

Дата поступления в редакцию: 15.06.2019
После рецензирования: 1.08.2019
Дата принятия к публикаци: 5.08.2019