УДК 004.052.2

РАЗРАБОТКА МНОГОКАНАЛЬНОГО СИСТОЛИЧЕСКОГО АЛГОРИТМА ВЫЧИСЛЕНИЯ ТЕОРЕТИКО-ЧИСЛОВЫХ ПРЕОБРАЗОВАНИЙ СИГНАЛОВ В ПОЛЕ ГАЛУА GF(M)

[1]Калмыков М.И., [1]Юрданов Д.В., [1]Кононова Н.В., [1]Калмыков И.А., [2]Тынчеров К.Т.

[1]ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru;
[2]ФГБОУ ВО «Уфимский государственный нефтяной технический университет», филиал, Октябрьский

В настоящее время беспроводные системы, реализующие такие стандарты, как IEEE 802.11 и IEEE 802.16, широко применяют методы цифровой обработки сигналов (ЦОС), в частности мультиплексирование с ортогональным частотным разделением OFDM. Использование технологии передачи сигналов, построенной на применении нескольких ортогональных несущих, позволяет обеспечить достаточно высокую спектральную эффективность сигнала OFDM, а также устойчивость к узкополосной интерференции. Данные результаты достигаются за счет перехода к параллельной передаче данных, а также применения ортогонального дискретного преобразования Фурье (ДПФ). Однако, дискретное преобразование Фурье, как и его быстрые алгоритмы, обладают недостатками. Среди них можно отметить наличие двух вычислительных трактов, а также значительные погрешности при выполнении ортогональных преобразований сигналов из-за применения тригонометрических функций. Устранить данные недостатки возможно за счет использования целочисленных теоретико-числовых преобразований (ТЧП) сигналов. Однако реализация ТЧП характеризуется значительными временными затратами. Поэтому разработка методов реализации теоретико-числовых преобразований сигналов, позволяющих устранить данный недостаток, является актуальной задачей. Целью статьи является повышение скорости выполнения ТЧП за счет разработки алгоритма, использующего параллельно-конвейерные методы на основе многоканальных систолических матриц.

Ключевые слова: цифровая обработка сигналов, ортогональные преобразования сигналов, дискретное преобразование Фурье, систолические алгоритмы, теоретико-числовое преобразование

DEVELOPMENT OF MULTI-CHANNEL SYSTOLIC ALGORITHM FOR COMPUTING NUMBER-THEORETIC TRANSFORMS OF THE SIGNALS IN THE GALOIS FIELD GF(M)

[1]Kalmykov M.I., [1]Yurdanov D.V., [1]Kononova N.V., [1]Kalmykov I.A., [2]Tyncherov K.T.

[1]Federal State Autonomous Educational Institution Higher Professional Education «North-Caucasian Federal University», Stavropol, e-mail: kia762@yandex.ru;
[2]Branch of Ufa State Petroleum Technological University, Oktyabrskiy

Currently, wireless systems that implement such standards as IEEE 802.11 and IEEE 802.16, widely used methods of digital signal processing (DSP), in particular, multiplexing with orthogonal frequency division OFDM. The use of signal transmission technology, based on the use of several orthogonal carriers, allows to provide a sufficiently high spectral efficiency OFDM signal, as well as resistance to narrowband interference. These results are achieved through the transition to parallel data transmission, as well as the use of orthogonal discrete Fourier transform (DFT). However, the discrete Fourier transform, like its fast algorithms, has drawbacks. Among them we can note the presence of two computational paths, as well as significant errors in the performance of orthogonal signal transformations due to the use of trigonometric functions. It is possible to eliminate these drawbacks by using integer number-theoretic transformations (NTT) of signals. However, the implementation of NTT is characterized by significant time costs. Therefore, the development of methods for the implementation of theoretical and numerical transformations of signals to eliminate this drawback is an urgent task. The aim of the article is to increase the speed of the NTT by developing an algorithm using parallel-conveyor methods based on multichannel systolic matrices.

Keywords: digital signal processing, orthogonal signal transformations, discrete Fourier transform, systolic algorithms, number-theoretic transformation

В настоящее время методы цифровой обработки сигналов (ЦОС) находят новые сферы своего применения. Так как алгоритмы ЦОС обладают достаточно высокой вычислительной сложностью, то для обеспечения обработки сигналов в режиме реального времени используются спецпроцессоры (СП). Среди методов цифровой обработки сигналов особое место принадлежит ортогональным преобразованиям сигналов, которые используют дискретное преобразование Фурье (ДПФ) и его быстрые алгоритмы. Наиболее наглядно это проявляется в беспроводных системах передачи данных, использующих технологию OFDM. Основными недостатками дискретных преобразований Фурье (ДПФ) с точки зрения цифровой обработки сигналов являются ошибки, возникающие вследствие округления или усечения результатов операций до используемой специализированными процессорами длины слова и наличие двух вычислительных трактов [1, 2]. Причем в конечных полях и кольцах может быть определено преобразование, аналогичное ДПФ и лишенное указанных недо-

статков [3]. Поэтому разработка алгоритмов ЦОС, использующих преимущества целочисленной арифметики и позволяющих устранить отмеченные недостатки ДПФ, является актуальной задачей.

С точки зрения реализации СП преобразований сигналов на основе ДПФ существует проблема представления словами конечной длины поворачивающих коэффициентов, являющихся иррациональными числами [4, 5]. Одним из направлений решения данной проблемы является использование конечных полей или колец с целью замены операций над действительными числами операциями над целыми числами. В работах [1, 2] предлагается в качестве альтернативы ДПФ использовать теоретико-числовые преобразования (ТЧП). Однако реализация ТЧП характеризуется значительными временными затратами. Поэтому разработка методов реализации теоретико–числовых преобразований сигналов, позволяющих устранить данный недостаток, является актуальной задачей. В работе [6] предложено использовать систолический принцип организации вычислений для повышения скорости выполнения ТЧП и разработан чисто-систолический алгоритм вычисления ТЧП (ЧСМ ТЧП) сигналов. Дальнейшее снижение временных затрат на выполнение ДВП возможно за счет применения многоканальных систолических матриц (МСМ). Поэтому целью работы является повышение скорости выполнения ТЧП за счет разработки алгоритма, использующего параллельно-конвейерные методы на основе многоканальных систолических матриц.

Материалы и методы исследования

Систолический принцип организации вычислений является одним из направлений построения систем ЦОС. Ячейки систолических процессоров (процессорные элементы) имеют, как правило, простую структуру и работают параллельно, выполняя одинаковую для одинаковых типов ячеек базовую операцию. Результаты вычислений предыдущей ячейки являются входными данными для последующей, передача данных осуществляется по всем локальным связям, причем данные в систолическом процессоре обрабатываются по мере выполнения всей необходимой совокупности базовых операций.

В работе [6] рассмотрены чисто-систолические матрицы, реализующие вычисления ТЧП по схеме Горнера. В ходе проведенных исследований было установлено, что перенос подходов, используемых при построении чисто-систолических СП ДПФ из поля комплексных чисел в конечные поля Галуа $GF(M)$ позволяет повысить скорость вычисления ТЧП в 2,5 раза по сравнению с классическим алгоритмом. Рассмотрим возможность использования подходов, применяемых при проектировании многоканальных систолических СП ДПФ для разработки алгоритмов вычисления ТЧП.

ТЧП определяется для последовательностей целых чисел S_k и x_n, $k,\ n = 0,\ 1, \ldots, N-1$, как пара преобразований:

$$S_k = \left(\sum_{n=0}^{N-1} x_n \varepsilon_N^{kn} \right) \bmod M , \qquad (1)$$

$$x_n = \left(N^{-1} \sum_{k=0}^{N-1} S_k \varepsilon_N^{-kn} \right) \bmod M , \qquad (2)$$

со структурой, похожей на структуру ДПФ. M, N – взаимно простые целые положительные числа, кроме этого, необходимым условием существования ТЧП является делимость $P_i - 1$ на N, где P_i – любой из простых сомножителей M, ε_N – такое число, что $(\varepsilon_N)^N = 1 \bmod M$ и $(\varepsilon_N)^L \neq 1 \bmod M$, $\forall L < N$).

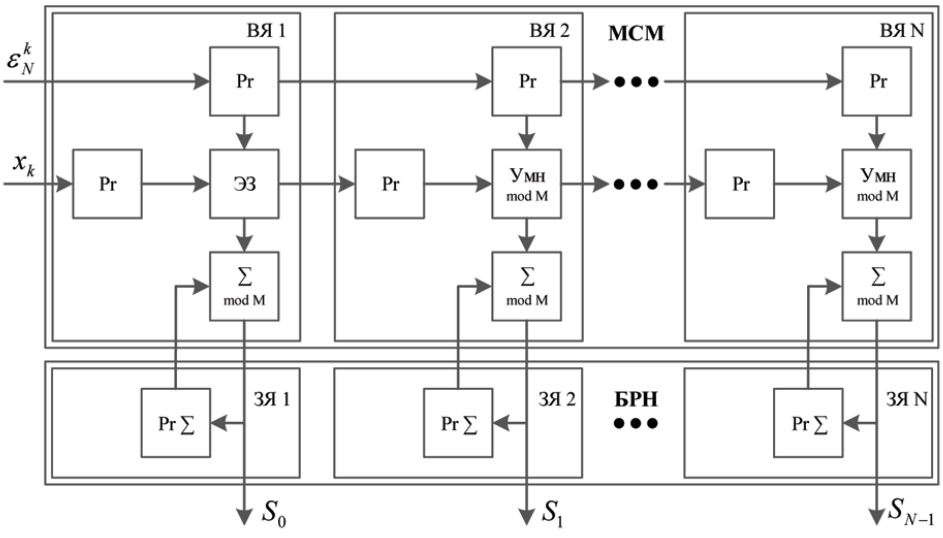

Рис. 1. Многоканальная систолическая матрица с блоком регистров-накопителей для вычисления ТЧП

В работе [4–1] показано, если ε_N является степенью двойки, то умножения в (1) и (2) можно осуществить сдвигами кодовых слов и приведением результата по модулю M.

Перенесем подходы, используемые при построении многоканальных систолических СП ДПФ из поля комплексных чисел в конечные кольца Z_M и представим структуру многоканальной систолической матрицы (МСМ) с блоком регистров-накопителей (БРН) для вычисления ТЧП (МСМ ТЧП) на рис. 1. Ячейки БРН содержат накапливающий регистр Pr Σ, предназначенный для хранения промежуточных значений S_k. Каждая l-я ячейка ($l \in \overline{1, N}$) МСМ ТЧП реализует вычисления S_k по формуле (1) следующим образом:

$$s_{l,n} = \left(s_{l,(n-1)} + x_{(n-l)}\varepsilon_N^{(n-l)(l-1)}\right) \bmod M, \quad \forall\ n = 1, 2, \ldots, 2N-1, \qquad (3)$$

где $s_{l,n}$ – значение накопленной суммы в n-й такт вычислений $\left(l \le n \le N + l - 1\right)$ в l-м регистре Pr Σ, $s_{l,(n-1)}$ – то же на $(n-1)$ – такте, $x_{(n-l)}$ – значение отсчета исходных данных на n-м такте в l-й ячейке, $\varepsilon_N^{(n-l)(l-1)}$ – значение степени $(n-l)(l-1)$ элемента порядка N, поступающего на вход l-ячейки в n-й такт.

Из формулы (3) видно, что вычисления $s_{l,n}$ осуществляются в независимых ячейках МСМ ТЧП, причем операции умножения и сложения разделены и $s_{l,(n-1)} = 0,\ \forall n \le l$. На рис. 2 представлена структура отдельной ячейки МСМ.

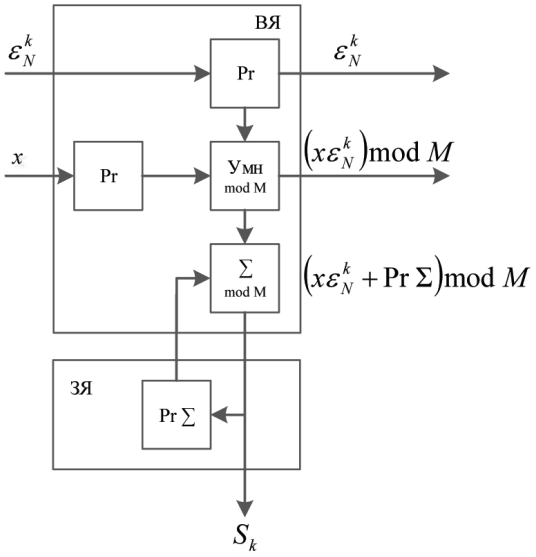

Рис. 2. Структура отдельной ячейки МСМ ТЧП

В каждый такт работы длительностью τ отдельная ячейка МСМ ТЧП (рис. 2) выполняет операции: п/п длительностью τ_1 (передача на выход значения ε_N^k, поступившего в ячейку на предыдущем такте; передача на выход результата предыдущего умножения; прием новых значений ε_N^{k+1} и x), Умн mod M длительностью τ_2 (умножение ε_N^{k+1} на x по mod M), Σ mod M длительностью τ_3 (суммирование результата умножения $\left(x\varepsilon_N^k\right) \bmod M$ с содержимым регистра Pr Σ), з/с длительностью τ_4 (запись результата текущей суммы в Pr Σ, считывание результата суммирования в выходную шину на $(N-1+l)$-м такте и очистка Pr Σ l-й ячейки, $l \in \overline{1, N}$) в соответствии с рис. 3.

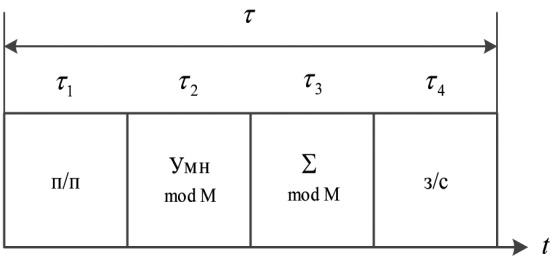

Рис. 3. Такт работы отдельной ячейки МСМ ТЧП

В соответствии с (1) при вычислении S_0 отсутствуют операции умножения, поэтому первая ячейка МСМ ТЧП (рис. 1) является вырожденной, элемент задержки (ЭЗ) указанной ячейки синхронизирует микротакты передачи задержкой на время τ_2 микротакта умножения. Временная диаграмма работы МСМ ТЧП при $N = 5$ представлена на рис. 4.

Перед началом вычислений содержимое всех регистров Pr Σ равно нулю. На первом такте значения x_0 и ε_N^0 загружаются в первую ячейку МСМ ТЧП. Через время $\tau_1 + \tau_2$ в соответствии с рис. 3 выполняется суммирование x_0 с содержимым Pr Σ первой ячейки (на первом такте равным нулю) по модулю M. На микротакте τ_4 результат суммирования (в нашем случае – x_0), записывается в Pr Σ первой ячейки. На втором такте работы МСМ ТЧП (рис. 4) значения x_0 и ε_N^0 передаются из первой ячейки во вторую, значения x_1 и ε_N^1 загружаются в первую ячейку. На микротакте τ_2 второго такта работы МСМ ТЧП – x_1 задерживается в элементе задержки, во второй ячейке – x_0 умножается на ε_N^0 по модулю M. Далее, на микротакте τ_3 в первой и второй ячейках МСМ ТЧП выполняется суммирование по модулю M, результаты которого записываются в регистры Pr Σ первой и второй ячеек соответственно. Со второго такта первая и вторая ячейки работают синхронно (рис. 4).

На третьем такте работы МСМ ТЧП значения x_0, ε_N^0 загружаются в третью ячейку; x_1 и ε_N^1 – во вторую ячейку; x_2 и ε_N^2 – в первую. Далее ячейки $l = 1, 2, 3$ работают синхронно, на четвертом такте в работу включается четвертая ячейка и т.д. В соответствии с временной диаграммой работы МСМ ТЧП, на N-м такте параллельно работают все ячейки. В конце N-го такта, в результате выполненного первой ячейкой суммирования получается значение S_0. На $(N+1)$-м такте значение S_1 будет сформировано во второй ячейке МСМ ТЧП, на $(N+2)$-м, в третьей ячейке и т.д. Холостой ход при торможении конвейера выполняется в случае, если на $(N+1)$-м такте в МСМ ТЧП не поступают новые данные. Если на $(N+1)$-м такте в МСМ ТЧП поступают новые данные, то происходит совместная обработка двух строк исходных данных в такты с шестого по девятый. МСМ ТЧП переходит в установившийся режим работы, если, начиная с такта $2N$, на обработку поступают новые данные. Таким образом, на рис. 4 можно выделить три режима работы МСМ ТЧП: разгон конвейера (первые N тактов); установившийся режим работы; торможение конвейера (последние $(N-1)$ тактов).

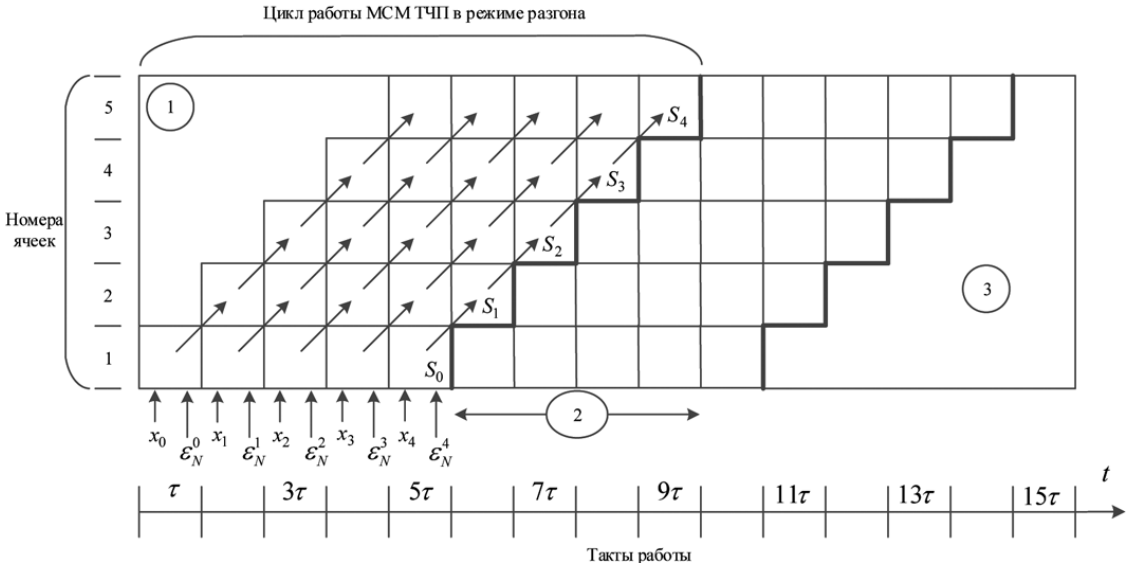

Рис. 4. Временная диаграмма работы МСМ ТЧП: 1 – начальный (холостой) ход при разгоне конвейера; 2 – обработка двух строк исходных данных в соседних циклах; 3 – холостой ход при торможении конвейера

Приведем оценки характеристик вычислительного процесса МСМ ТЧП в установившемся режиме с учетом временной диаграммы работы (рис. 4):

– число тактов в каждом цикле вычислений

$$K_y = 2N - 1; \tag{4}$$

– число вычислительных тактов

$$K_в = K_y = 2N - 1; \tag{5}$$

– число базовых операций, используемых для вычисления коэффициентов ТЧП

$$K_{бв} = N^2; \tag{6}$$

– производительность МСМ ТЧП в числе базовых операций

$$P_{бо} = P_{яч} N, \tag{7}$$

где $P_{яч} = \dfrac{1}{\tau}$ – производительность одной ячейки (в числе базовых операций), $\tau = \tau_1 + \tau_2 + \tau_3 + \tau_4$, τ – время выполнения базовой операции (рис. 3);

– производительность ЧСМ ТЧП для вычисления всего ТЧП по формуле (3)

$$P_{ТЧП} = \frac{P_{бо}}{N^2} = \frac{P_{яч} N}{N^2} = \frac{P_{яч}}{N}; \tag{8}$$

– время выполнения всего ТЧП в установившемся режиме

$$T_{ТЧП} = K_в \tau = (2N - 1)\tau. \tag{9}$$

Результаты исследования и их обсуждение

Рассмотрим пример реализации ТЧП по модулю $M = 7$. Для выполнения ТЧП на основе разработанного алгоритма потребуется 6 ячеек МСМ. В качестве $\varepsilon_{N=6} = 3$. С помощью данного числа можно получить все ненулевые вычеты по модулю $M = 7$. В этом случае получаем $\left|\varepsilon^0\right|_7^+ = 1, \left|\varepsilon^1\right|_7^+ = 3, \left|\varepsilon^2\right|_7^+ = 2, \left|\varepsilon^3\right|_7^+ = 6, \left|\varepsilon^4\right|_7^+ = 4, \left|\varepsilon^{05}\right|_7^+ = 5$. Пусть входной вектор имеет вид равный $x_n = \{4, 5, 2, 1, 4, 3\}$. Согласно выражению (1) получаем

$$S_k = \begin{vmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{vmatrix} \times \begin{vmatrix} 4 \\ 5 \\ 2 \\ 1 \\ 4 \\ 3 \end{vmatrix}^T = \begin{vmatrix} 5 \\ 4 \\ 1 \\ 1 \\ 2 \\ 4 \end{vmatrix}.$$

Рассмотрим работу МСМ, реализующей ТЧП по модулю $M = 7$. На первом такте работы на входы ячейки 1 МСМ подаются значения $x_0 = 4$ и коэффициент $\left|\varepsilon^0\right|_7^+ = 1$, которые записываются в соответствующие регистры Рг. Затем значение $x_0 = 4$ попадает на элемент задержки, а потом суммируется по модулю 7, предыдущим содержимым регистра $Рг_{\Sigma 1}$. В результате в данный регистр записывается результат $s_{1,1} = \left(s_{1,0} + x_0 \varepsilon^{0)}\right) \bmod M = \left|0 + 4\right|_7^+ = 4$.

На втором такте работы на входы ячейки 1 МСМ подаются значения $x_1 = 5$ и коэффициент $\left|\varepsilon^1\right|_7^+ = 3$, которые записываются в соответствующие регистры Рг. Затем число $x_1 = 5$ подается на элемент

задержки ЭЗ. А затем суммируется с содержимым регистра $Рг_{\Sigma 1}$. В результате в данный регистр записывается результат $s_{1,2} = \left(s_{1,1} + x_1\varepsilon^{1)}\right) \bmod M = \left|4+5\right|_7^+ = 2$. Одновременно с этими операциями из ячейки 1 в регистры Рг. ячейки 2 подаются значение $\left|\varepsilon^0\right|_7^+ = 1$ и $x_0 = 4$. Умножитель по модулю реализует операцию $s_{1,1} \cdot \varepsilon^0 \bmod 7 = \left|4 \cdot 1\right|_7^+ = 4$.

Результат умножения подается на сумматор по модулю $M = 7$ второй ячейки, где выполняется $s_{2,2} = \left(s_{2,1} + x_0\varepsilon^0\right) \bmod M = \left|0+4\right|_7^+ = 4$. Результат записывается в регистр $Рг_{\Sigma 2}$.

На третьем такте работы на входы ячейки 1 МСМ подаются значения $x_2 = 2$ и коэффициент $\left|\varepsilon^2\right|_7^+ = 2$, которые записываются в соответствующие регистры Рг. Затем число $x_2 = 2$ подается на элемент задержки ЭЗ. А затем суммируется с содержимым регистра $Рг_{\Sigma 1}$. В результате в данный регистр записывается результат $s_{1,3} = \left(s_{1,2} + x_2\varepsilon^2\right) \bmod M = \left|2+2\right|_7^+ = 4$. Одновременно с этими операциями из ячейки 1 в регистры Рг. второй ячейки подается значение $\left|\varepsilon^1\right|_7^+ = 3$ и $x_1 = 5$, а из ячейки 2 в регистры Рг. третьей ячейки подается значение $\left|\varepsilon^0\right|_7^+ = 1$ и $x_0 = 4$. Умножитель ячейки 2 реализует операцию $x_1 \cdot \varepsilon^1 \bmod 7 = \left|5 \cdot 3\right|_7^+ = 1$.

Результат умножения подается на сумматор по модулю ячейки 2, где выполняется операция $s_{2,3} = \left(s_{2,2} + x_1\varepsilon^1\right) \bmod M = \left|4+1\right|_7^+ = 5$. Результат суммы записывается в регистр $Рг_{\Sigma 2}$. Умножитель третьей ячейки по модулю $M = 7$ реализует $x_0 \cdot \varepsilon^0 \bmod 7 = \left|4 \cdot 1\right|_7^+ = 4$.

Результат умножения подается на сумматор по модулю $M = 7$ третьей ячейки, где выполняется $s_{3,3} = \left(s_{3,2} + x_0\varepsilon^0\right) \bmod M = \left|0+4\right|_7^+ = 4$. Результат записывается в регистр $Рг_{\Sigma 3}$.

Дальше алгоритм выполняется подобным образом. Спустя 6 тактов с выхода первой ячейки МСМ будет выдаваться результат $S_0 = \left|4+5+2+1+4+3\right|_7^+ = 5$. На следующих пяти тактах работы будут получены оставшиеся коэффициенты ТЧП $S_1 - S_5$.

Достоинствами МСМ ТЧП являются: 100 % использование оборудования. В работе [6] показано, что длительность вычисления в установившемся режиме равна $T_{ТЧП} = 2N\tau$. Для рассмотренного примера это составит $T_{ТЧП} = 2N\tau = 12\tau$. При использовании МСМ для вычисления ТЧП потребуется $T_{ТЧП} = (2N-1)\tau = 11\tau$. Таким образом, использование разработанного алгоритма вычисления ТЧП с использованием МСМ позволило повысить скорость вычисления в 1,09 раза по сравнению алгоритмом на основе ЧСМ и в более чем в 3 раза по сравнению с классическим алгоритмом ТЧП.

Заключение

Использование ТЧП вместо ДПФ в задачах ЦОС позволяет устранить ошибки округления результатов операций за счет перехода к целым числам, а также сократить один тракт. Разработанный алгоритм МСМ ТЧП, в отличие от ЧСМ ТЧП, может быть использован для параллельно-конвейерного расчета любого количества спектральных коэффициентов S_k, $k \in \overline{0, N-1}$. В ходе проведенных исследований показано, что использование разработанного алгоритма вычисления ТЧП с использованием МСМ позволило повысить скорость вычисления в 1,09 раза по сравнению алгоритмом ЧСМ и в более чем в 3 раза по сравнению с классическим алгоритмом ТЧП, в поле $GF(7)$.

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

Список литературы

1. Шапошников А.В. Быстрый алгоритм вычисления теоретико-числового преобразования // Актуальные проблемы современной науки. 2013. № 2. С. 204–207.

2. Червяков Н.И., Коляда А.А., Ляхов П.А. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях. М.: ФИЗМАТЛИТ, 2017. 400 с.

3. 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.

4. Ananda Mohan Residue Number Systems. Theory and Applications. Springer International Publishing Switzerland. 2016. 734 p.

5. Steven G. Johnson and Matteo Frigo, A modied split-radix FFT with fewer arithmetic operations. IEEE Transactions on Signal Processing 55. 2007. no. 1. P. 111–119.

6. Топоркова Е.В., Степанова Е.П. Разработка чисто-систолического алгоритма вычисления теоретико-числовых преобразований сигналов // Современная наука и инновации. 2018. № 4. С. 28–36.