УДК 004.052.2

РАЗРАБОТКА БЫСТРОГО АЛГОРИТМА ВЫЧИСЛЕНИЯ ТЕОРЕТИКО-ЧИСЛОВЫХ ПРЕОБРАЗОВАНИЙ СИГНАЛОВ

Юрданов Д.В., Калмыков М.И., Гостев Д.В., Калмыков И.А.

ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru

Целью исследований является повышение скорости выполнения ортогональных преобразований сигналов при использовании теоретико-числовых преобразований в конечных полях. Использование быстрых алгоритмов дискретного преобразования Фурье позволяет повысить скорость цифровой обработки сигналов (ЦОС) за счет параллельных вычислений. Однако быстрое преобразование Фурье (БПФ) обладает рядом недостатков. Во-первых, это наличие двух вычислительных трактов для обработки действительной и мнимой части сигнала. Во-вторых, использование тригонометрических функций в качестве поворачивающих коэффициентов, что приводит к ошибкам округления. Решить данную проблему можно за счет использования теоретико-числового преобразования сигнала. Однако при выполнении ортогональных преобразований сигналов в конечных полях Галуа не используются быстрые алгоритмы, подобные быстрым алгоритмам преобразованиям Фурье. Поэтому разработка быстрого алгоритма вычисления теоретико-числового преобразования является актуальной задачей.

Ключевые слова: цифровая обработка сигналов, ортогональные преобразования сигналов, быстрое преобразование Фурье, быстрые алгоритмы, теоретико-числовые преобразования

DEVELOPMENT OF FAST ALGORITHM FOR COMPUTING NUMBER-THEORETIC TRANSFORMS OF SIGNALS

Yurdanov D.V., Kalmykov M.I., Gostev D.V., Kalmykov I.A.

Federal State Autonomous Educational Institution Higher Education «North-Caucasian Federal University, Stavropol, e-mail: kia762@yandex.ru

The aim of the research is to increase the speed of execution of orthogonal transformation of signals when using number-theoretic transforms in finite fields. The use of fast algorithms of discrete Fourier transform allows to increase the speed of digital signal processing (DSP) due to parallel computing. However, the fast Fourier transform (FFT) has a number of drawbacks. First, is the presence of two computational paths for processing the real and imaginary parts of the signal. Secondly, the use of trigonometric functions as twiddle factors, which leads to rounding errors. To solve this problem through the use of number-theoretic transform of the signal. However, when carrying out orthogonal transformation of signals in finite fields, Galois does not use fast algorithms, fast algorithms similar to Fourier transforms. Therefore, the development of fast algorithm for computing number-theoretic transform is an urgent task.

Keywords: digital signal processing, orthogonal transformation of signals, fast Fourier transform, fast algorithms, number-theoretic transform

Цифровая обработка сигналов (ЦОС) относится к числу наиболее динамически развивающихся областей инженерной деятельности [2, 8, 10]. Медицина, системы сотовой связи, телекоммуникации, Internet-технологии, обработка звука и изображений, навигация – вот далеко не полный перечень приложений, в которых активно используются методы ЦОС. В настоящее время широкое применение нашли специализированные процессоры (СП) цифровой обработки сигналов, которые базируются на реализации ортогональных преобразований сигналов. Такие ортогональные преобразования сигналов, как правило, определены над полем комплексных чисел. Среди таких преобразований сигналов можно выделить быстрые преобразования Фурье (БПФ) [1, 4, 9]. Однако они имеют ряд недостатков, которые связаны с наличием двух вычислительных трактов для обработки действительной и мнимой части сигнала, а также с ошибками округления, вызванных использованием в качестве поворачивающих коэффициентов функций синусов и косинусов. Поэтому разработка новых алгоритмов ортогональных преобразований сигналов с использованием целочисленной арифметики, позволяющих устранить отмеченные недостатки, является актуальной задачей.

Цель исследования

Основным недостатком ортогональных преобразований сигналов на основе БПФ является использование в качестве ортогональных базисов тригонометрических функций. Решить данную проблему можно за счет перехода к целочисленному вычислению. В работах [1, 3, 5, 7] предлагается выполнять цифровую обработку сигнала с использованием теоретико-чис-

ловых преобразований (ТЧП). Однако такие целочисленные преобразования сигналов имеют малую производительность, так как они подобны дискретному преобразованию Фурье (ДПФ). Поэтому целью работы является повышение скорости выполнения ортогональных преобразований сигналов за счет разработки быстрого алгоритма ТЧП.

Материалы и методы исследования

В настоящее время конечные поля Галуа нашли применение в цифровых телекоммуникационных системах в основном в направлениях, связанных с построением корректирующих кодов, а также с формированием псевдослучайных последовательностей. Использование конечных полей для задач цифровой обработки сигналов ограничено из-за отсутствия критериев существования быстрых алгоритмов вычисления теоретико-числовых преобразований, являющихся альтернативой преобразованию Фурье. Указанное ограничение обусловлено тем, что в отличие от комплексного случая, в модулярной арифметике, не существуют примитивные (первообразные) корни из единицы любой степени. Поэтому разработка алгоритмов быстрого вычисления ТЧП и критериев их существования, позволит повысить эффективность работы инфокоммуникационных систем.

Для многих практических приложений ЦОС используется быстрое преобразование Фурье. При реализации БПФ возможны несколько вариантов организации вычислений в зависимости от способа деления последовательности $x_0, x_1, x_2, \ldots, x_{N-1}$ длины N на части. В случае четного N возможно использование варианта «прореживания по времени», который определяется как сумма двух $\frac{N}{2}$ точечных дискретных преобразований Фурье

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

где $W_{N/2}=e^{-i\frac{2\pi}{N/2}}$, $i=\sqrt{-1}$, x_{2n}, x_{2n+1}, – подпоследовательности длины $\frac{N}{2}$ с четными и нечетными номерами соответственно. Из равенства (1) видно, что реализация БПФ характеризуется наличием двух вычислительных трактов, влияющих на схемные затраты и надежность спецпроцессора ЦОС. Кроме того, БПФ в качестве поворачивающих коэффициентов использует иррациональные числа, что снижает точность вычислений. Устранить данные недостатки возможно за счет использования ТЧП, определенного в алгебраической системе, обладающей свойствами кольца или поля [2, 6, 10].

Пусть $GF(M)$ – конечное поле Галуа, G_N – циклическая группа порядка N, $\varepsilon_N \in GF(M)$ – примитивный корень порядка N (ε_N элемент поля $GF(M)$, удовлетворяющий условию $(\varepsilon_N)^N=1 \bmod M$ и $(\varepsilon_N)^L\neq 1 \bmod M$ для любого натурального $L<N$). Тогда ТЧП последовательности $x_0, x_1, x_2, \ldots, x_{N-1}$, где $x_i \in G_N$ $k=0, 1, \ldots N-1$ имеет вид

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

Обратное теоретико-числовое преобразование имеет вид

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

Очевидно, что ТЧП по своей структуре наилучшим образом реализуются с использованием цифровой элементной базы. Например, если взять ε_N в виде степени двойки, то умножение в (2) и (3) на степени ε_N при вычислении ТЧП заменяется сдвигами кодовых слов и приведением сдвинутых кодовых слов по модулю числа M [2].

В работе [10] показана возможность повышения скорости выполнения ТЧП за счет использования разработанного алгоритма применения модулярных кодов. Если в качестве числа M использовать составные числа Мерсена, то выражения (2) и (3) можно свести к многомерной параллельной обработке.

Свойства ТЧП изоморфны свойствам дискретного преобразования Фурье. Следовательно, должна существовать возможность вычисления ТЧП с использованием быстрых алгоритмов, аналогичных БПФ. Перенесем подходы, используемые при построении БПФ с прореживанием по времени из поля комплексных чисел (1) в конечное поле Галуа $GF(M)$. Принимая во внимание (1), перепишем (2) в виде:

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

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

Из выражения (4) вытекает условие разложения N точечного ТЧП в сумму двух ТЧП длины $N/2$. Рассмотрим следующую теорему.

Теорема. Пусть $GF(M)$ – конечное поле Галуа, N – четное число, G_N – циклическая группа порядка N, $\varepsilon_N \in GF(M)$ – примитивный корень порядка N, удовлетворяющий

$$(\varepsilon_N)^N=1 \bmod M. \quad (5)$$

Тогда ТЧП последовательности $x_0, x_1, x_2, \ldots, x_{N-1}$, где $x_i \in G_N$ представимо в виде суммы ТЧП подпоследовательностей с четными x_{2n}, и нечетными x_{2n+1} номерами.

Доказательство. Из условия (5) следует существование примитивного корня $\varepsilon_{N/2} = (\varepsilon_N)^2 \bmod M$ порядка $N/2$. Преобразуем выражение (4) с учетом равенства (5):

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

$$= \left(\left(\sum_{n=0}^{N/2-1} x_{2n} \times \varepsilon_{N/2}^{-kn} \right) \bmod M + \left(\varepsilon_N^{-k} \sum_{n=0}^{N/2-1} x_{2n+1} \times \varepsilon_{N/2}^{-nk} \right) \bmod M \right) \bmod M =$$

$$= \left(S_{11}(k) + \varepsilon_N^{-k} S_{12}(k) \right) \bmod M , \quad (6)$$

где $S_{11}(k)$ и $S_{12}(k)$ – ТЧП последовательностей с четными x_{2n}, и нечетными x_{2n+1} номерами.

Так как $S_{11}(k)$ и $S_{12}(k)$ имеют размерность $N/2$, формулу (6) можно использовать только для вычисления $S(k)$ при $0 \le k < N/2$. Для случая следует воспользоваться периодичностью ТЧП:

$$S_{11}\left(k + \frac{N}{2}\right) = S_{11}(k) \text{ и } S_{12}\left(k + \frac{N}{2}\right) = S_{12}(k) . \quad (7)$$

С учетом (7) при условии $N/2 \le k < N$ формулу (6) можно переписать в виде

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

Теорема доказана.

В отличие от БПФ в поле комплексных чисел, в котором существуют корни из единицы любой степени ($\sqrt[N]{1} = e^{i\frac{2\pi}{N}}$, $i = \sqrt{-1}$), условие представления размерности ТЧП в виде степени двойки не является достаточным для существования быстрого ТЧП с «прореживанием по времени» ввиду отсутствия в конечных полях корней из единицы любой степени. Рассмотрим примеры использования доказанной теоремы.

Результаты исследования и их обсуждение

Воспользуемся для вычисления ТЧП сигнала конечные поля *GF*(17), *GF*(29). При этом в поле *GF*(17) длина входной последовательности равна 16 отсчетам, а в конечном поле *GF*(29) – длина входного вектора будет составлять 28 отсчетов.

Пример 1. Выполним теоретико-числовое преобразование вектора (x_0, x_1, x_2, ..., x_{15}) = (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15) в поле *GF*(17), для чего подготовим цепочку примитивных корней: $\varepsilon_{16} = 3$, $\varepsilon_8 = 9$, $\varepsilon_4 = 13$, $\varepsilon_2 = 16$. Заметим, что подобранные числа удовлетворяют условию

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

На первом этапе разработанного быстрого алгоритма ТЧП по модулю 17 получаем

$$S_{31}(0) = \left| x_0 + x_8 \right|_{17}^{+} = 8 ; \; S_{31}(1) = \left(x_0 + 16^{-1} x_8 \right)_{17} = 9 ;$$

$$S_{32}(0) = \left(x_4 + x_{12} \right)_{17} = 16 ; \; S_{32}(1) = \left(x_4 + 16^{-1} x_{12} \right)_{17} = 9 ;$$

$$S_{21}(0) = (S_{31}(0) + 13^{-0} S_{32}(0))_{17} = 7; \; S_{21}(1) = (S_{31}(1) + 13^{-1} S_{32}(1))_{17} = (9 + 13^{-1} * 9)_{17} = 11.$$

$$S_{21}(2) = \left(S_{31}\left(2 - \frac{4}{2}\right) + 13^{-2} S_{32}\left(2 - \frac{4}{2}\right) \right)_{17} = (S_{31}(0) + 13^{-2} S_{32}(0))_{17} = (8 + 13^{-2} * 16)_{17} = 9;$$

$$S_{21}(3) = \left(S_{31}\left(3 - \frac{4}{2}\right) + 13^{-3} S_{32}\left(3 - \frac{4}{2}\right) \right)_{17} = (S_{31}(1) + 13^{-3} S_{32}(1))_{17} = (9 + 13^{-3} * 9)_{17} = 7;$$

Аналогичным образом получаются остальные спектральные составляющие ТЧП. Структура и конкретные значения 16-точечного ТЧП представлена на рис. 1.

Пример 2. Вычислим ТЧП входного вектора отсчетов (x_0, x_1, x_2, ..., x_{15}, x_{27}) = (0, 1, 2, ..., 26, 27) в конечном поле Галуа GF(29). Для этого необходимо вычислить следующую цепочку примитивных корней: $\varepsilon_{28} = 2$, $\varepsilon_{14} = 4$, $\varepsilon_7 = 16$. Структура и конкретные значения 28-точечного ТЧП представлены на рис. 2.

Сформулированные в работе условия разложимости N-точечного ТЧП на преобразования меньшей размерности и доказательство теоремы позволяют

разрабатывать быстрые алгоритмы ТЧП вычисления ортогональных преобразований сигналов в конечных полях. Это было продемонстрировано на примерах 1 и 2. Наиболее эффективны быстрые алгоритмы ТЧП в случае, когда длина вектора исходных данных является степенью двойки и выполнены условия (5). В этом случае деление последовательностей на две части можно продолжать до тех пор, пока не получатся двухэлементные последовательности, что было показано в примере 1.

Оценим эффективность быстрого алгоритма ТЧП с прореживанием по времени, обусловленную разложением N-точечного преобразования на несколько малых. Для вычисления N-точечного ТЧП по формуле (2) требуется N^2 операций. Наибольшая степень ускорения вычислений может быть достигнута при $N = 2^k$ и существовании примитивного корня порядка N. Число требуемых при этом операций можно оценить как $N \cdot \log_2(N)$. Таким образом, вычислительные затраты по сравнению с непосредственным использованием формулы (2) уменьшаются в $N/\log_2(N)$ раз.

Заключение

Основное преимущество ТЧП по сравнению с ДПФ состоит в том, что корни из единицы имеют простое представление, что позволяет в вычислениях заменить комплексную арифметику на целочисленную. Использование быстрых ТЧП с прореживанием по времени имеет смысл, если число элементов в анализируемой последовательности является степенью 2 и только при существовании в конечном поле $GF(M)$ примитивного корня порядка длины анализируемой последовательности. В этом случае разработанный алгоритм быстрого ТЧП сигнала не является приближенным алгоритмом, причем ускорение достигается исключительно за счет оптимальной организации вычислений.

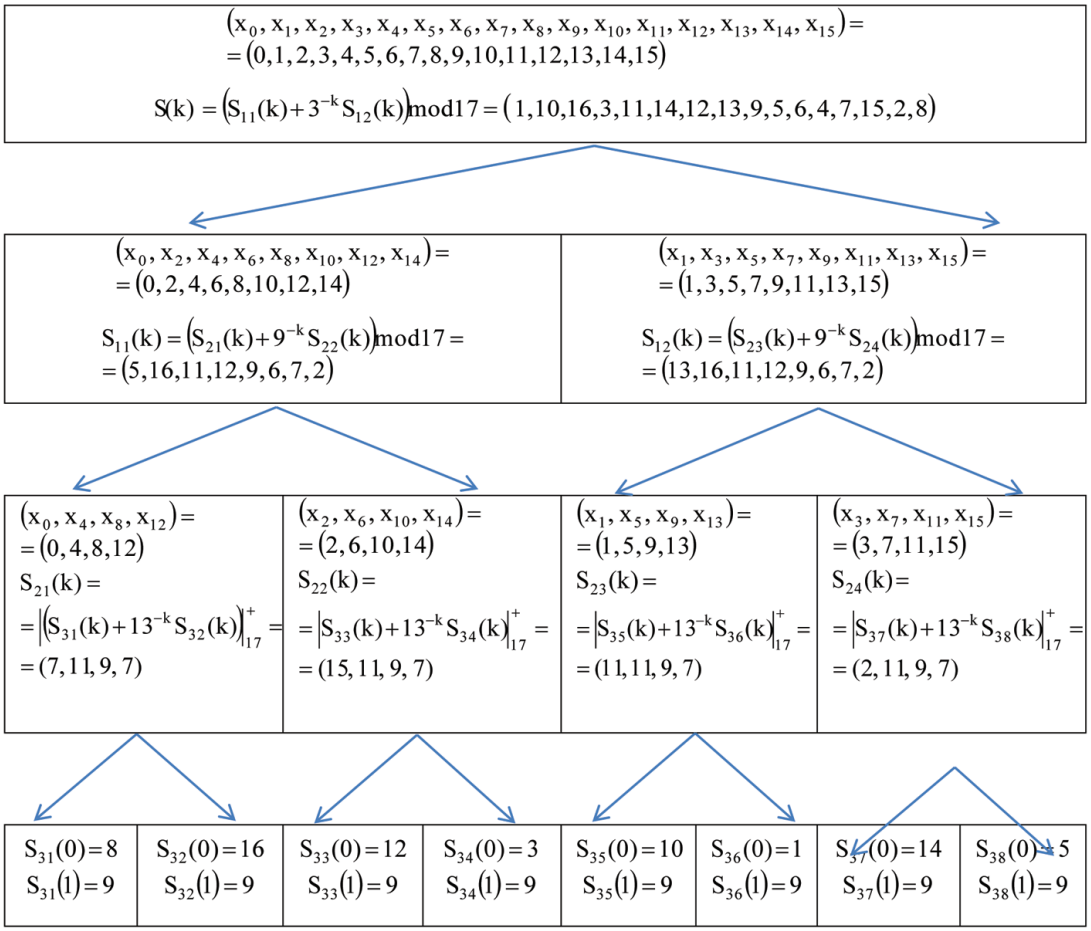

Рис. 1. Структура быстрого ТЧП по модулю 17 при N = 16

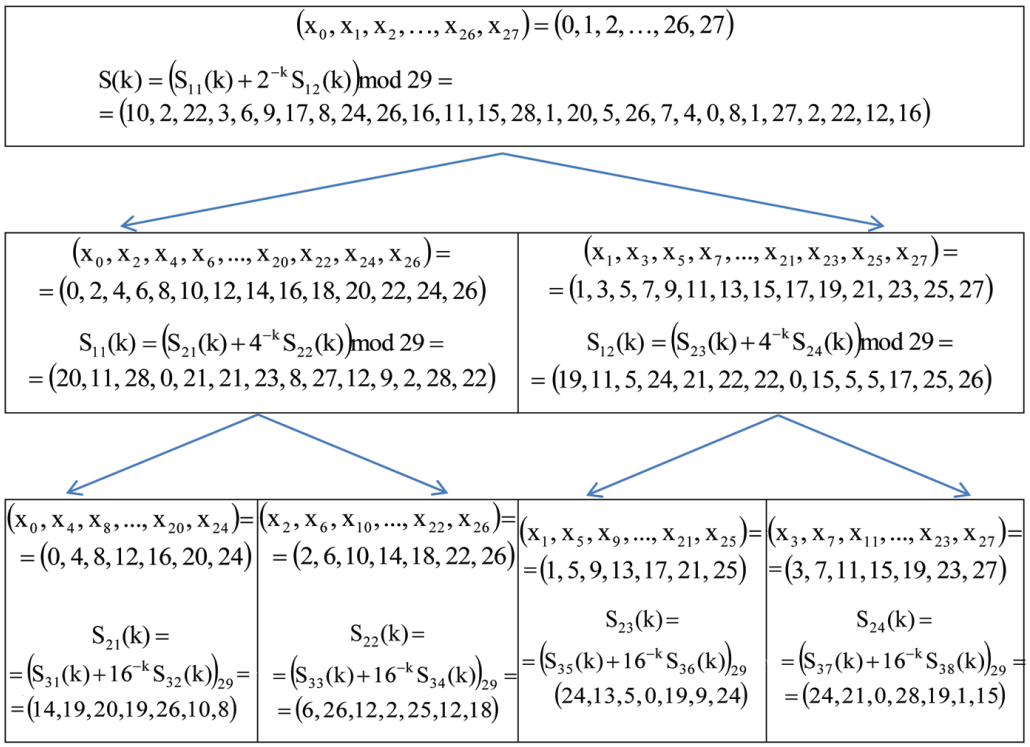

Рис. 2. Структура быстрого ТЧП по модулю 29 при N = 28

Разработанный алгоритм быстрого выполнения ТЧП сигнала с прореживанием по времени предназначен для одновременного расчета всех спектральных коэффициентов $S(k)$. Если необходимо получить значения коэффициентов для некоторых k, предпочтительнее использовать прямую формулу ТЧП.

Список литературы

1. Арслан Х., Чен Ши Нинг. Сверхширокополосная беспроводная связь. – М.: Техносфера, 2012. – 550 с.

2. Власов Е.Г. Конечные поля в телекоммуникационных приложениях. Теория и применение FEC, CRC и М-последовательностей. Практическое пособие. – М.: Инфа-М, 2016. – 285 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. Чернов В.М. Квазипараллельный алгоритм безошибочного вычисления свертки в редуцированных кодах Мерсена-Люка // Компьютерная оптика. – 2015. – № 2. – С. 241–248.

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

6. 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.

7. 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.

8. Jörg Arndt Matters Computational. Ideas, Algorithms, Source Code. – Springer Berlin Heidelberg, 2011. – 731 p.

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

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