УДК 517.443
DOI: 10.20310/1810-0198-2016-21-2-408-416

МОДИФИЦИРОВАННОЕ ДИСКРЕТНОЕ ПРЕОБРАЗОВАНИЕ ФУРЬЕ, ОСНОВАННОЕ НА ПЕРЕСТАНОВКАХ ГРУППЫ КОМПЛЕКСНЫХ КОРНЕЙ ИЗ ЕДИНИЦЫ

© **Е. В. Рыжкова, С. М. Ситник**

В работе рассматривается набор преобразований, которые обобщают известное дискретное преобразование Фурье (ДПФ). Эти обобщения определяются при помощи группы перестановок комплексных корней из единицы. Различным перестановкам соответствуют различные новые ДПФ. На этом пути удается построить преобразования с лучшими по сравнению со стандартным ДПФ спектральными свойствами. Например, для размерности равной четырем, стандартное ДПФ имеет неполный кратный спектр, а большинство новых преобразований имеют простой спектр. Приводятся результаты расчетов параметров преобразований на компьютере, а также некоторые гипотезы об их спектральных свойствах. Рассматривается возможность применения введенных обобщенных преобразований Фурье в криптографии.
Ключевые слова: дискретное преобразование Фурье; корни из единицы; перестановки; спектр матрицы; собственные вектора.

1. Введение

Дискретное преобразование Фурье (ДПФ) является одним из самых известных и полезных на практике математических инструментов. Это преобразование широко применяется, например, в электродинамике и оптике, теории кодирования и криптографии, при анализе систем связи и фильтрации сигналов, в алгоритмах сжатия информации и вычислительной томографии.

Важность ДПФ для приложений определяется в том числе и тем, что задачи о вычислении ДПФ, циклической свертки последовательностей, произведения больших чисел или многочленов по существу эквивалентны [1]. Фундаментальное значение также имеют быстрые алгоритмы ДПФ, в которых число необходимых операций уменьшено по сравнению с обычным бесхитростным вычислением за счет изощренной оптимизации порядка выполнения действий [2]–[3]. Наиболее известны быстрые алгоритмы Гуда, Кули и Тьюки, Винограда, Рейдера. Фундаментальную роль ДПФ играет в современной криптографии [5].

ДПФ определяется матрицей порядка n с элементами

$$f_{kj} = \frac{1}{\sqrt{n}} \exp\left(-i\frac{2\pi kj}{n}\right),\ 0 \leqslant k \leqslant n-1,\ 0 \leqslant j \leqslant n-1.$$

Таким образом, матрица ДПФ устроена так: первая строка и столбец состоят из единиц, во второй строке стоят комплексные корни из единицы (с точностью до множителя) порядка n, следующие строки являются последовательными степенями второй строки. Так, например, при $n=4$ матрица ДПФ имеет вид

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}.$$

Несмотря на широкую известность преобразования ДПФ, некоторые стандартные задачи для него имеют малоизвестные широкому кругу специалистов свойства. Рассмотрим в качестве примера естественную задачу о нахождении спектра ДПФ при любом n. Решение этой задачи отсутствует в литературе по преобразованиям Фурье и нетривиально. Известно, что четвертая степень ДПФ есть тождественное преобразование, поэтому собственными значениями могут быть лишь числа $\pm 1, \pm i$. Вопрос состоит в вычислении кратностей этих чисел. Аналогия с непрерывным преобразованием Фурье, для которого четыре этих числа совершенно равноправны, приводит к весьма правдоподобному предположению, что хотя бы в случае размерности $n = 4N$ собственные значения ДПФ также равноправны, и, следовательно, все имеют кратность N. Однако вычисления уже при $n = 4$ опровергают это предложение. В этом случае значения $-1, -i$ являются простыми, значение 1 имеет кратность 2, а значение i вообще отсутствует в спектре! Все это нарушает симметрию спектра, присущую непрерывному случаю.

Приведем таблицу кратностей собственных значений матрицы ДПФ для начальных значений размерности n. Из табл. 1 видно, что если отбросить начальные размерности $n = 2$ и $n = 3$, то несимметричность спектра проявляется при $n = 4$, а затем при переходе к следующей размерности кратность одного из четырех собственных значений увеличивается на единицу. Мы отметили в таблице соответствующие приращения размерностей знаками «+» и выделили жирным шрифтом, закономерность появления этих приращений простая: они добавляются циклически обходом четырех корней против часовой стрелки.

n	***1***	***i***	***-1***	***-i***
2	1	0	1	0
3	1	1+	1	0
4	2	0	1	**1**+
5	2	**1**+	1	1
6	2	1	**2**+	1
7	2	1	2	**2**+
8	**3**+	1	2	2
9	3	**2**+	2	2
10	3	2	**3**+	2
11	3	2	3	**3**+
12	**4**+	2	3	3
13	4	**3**+	3	3
14	4	3	**4**+	3
15	4	3	4	**4**+
16	**5**+	3	4	4
17	5	**4**+	4	4
18	5	4	**5**+	4
19	5	4	5	**5**+
20	**6**+	4	5	5

Таблица 1. Кратности собственных значений матриц ДПФ

Окончательные значения кратностей точек спектра при всех значениях размерностей матрицы n приведены в следующей табл. 2.

n	1	i	-1	- i
4N	***N+1 (+)***	N-1	N	N
4N+1	N+1	***N (+)***	N	N
4N+2	N+1	N	***N+1 (+)***	N
4N+3	N+1	N	N+1	***N+1 (+)***

Таблица 2. Формулы для кратностей собственных значений матриц ДПФ

Данный результат был для произвольного значения n доказан знаменитым математиком Исаем Шуром (I. Schur) в 1921 году [7], результат несколько раз переоткрывался и стал фольклорным. (Отметим, что в одной замечательной книге, знаменитой множеством нестандартных фактов и заключений, Исайа Шур назван белорусским математиком, он действительно родился в Бобруйске). Основным моментом при доказательстве неожиданно является тот факт, что для нахождения указанных кратностей необходимо вычисление знаменитых квадратичных тригонометрических сумм Гаусса [4], которые являются следами матриц ДПФ. Нахождение точной формулы для квадратичных тригонометрических сумм заняло у Гаусса около 10 (!) лет с 1801 по 1811 гг., сам он написал об этой задаче, «что решение многих трудных вопросов теории чисел не отняло столько дней, сколько взяло лет работы решение вопроса об этом». Для сравнения, теория гипергеометрических функций была создана Гауссом за несколько месяцев, что прослеживается по его подробным дневникам.

Непросто выписываются и соответствующие наборы собственных векторов для матрицы ДПФ. В этом направлении представляют интерес либо несложные алгоритмы получения собственных векторов, либо их особенно простой вид. Например, интересны вещественные наборы собственных векторов.

Данная работа возникла из наблюдения, что матрица ДПФ составляется нами по очевидному геометрическому способу: корни из единицы обходятся против часовой стрелки. Например, при $n=4$ порядок такой: $1, -i, -1, i$. Но равновозможны и логичны и все другие способы упорядочивания множества корней, при этом возникает целое множество различных новых дискретных преобразований Фурье.

2. Группы перестановок корней и модифицированные дискретные преобразования Фурье.

О п р е д е л е н и е 1. *Рассмотрим множество корней степени n из единицы, упорядоченное произвольным способом: $r_1, r_2, \ldots, r_n$. Назовем модифицированным дискретным преобразованием Фурье (МДПФ), построенным по данной перестановке множества корней из единицы, оператор с матрицей размеров $n \times n$, для которой в строке с номером k стоят величины $r_1^{k-1}, r_2^{k-1}, \ldots, r_n^{k-1}$ в соответствии с выбранной перестановкой.*

Ясно, что в результате получится некоторая матрица Вандермонда. Мы будем также нормировать эту матрицу множителем $\frac{1}{\sqrt{n}}$. В результате получится такая матрица МДПФ:

$$F_r = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & \ldots & 1 \\ r_1 & r_2 & \ldots & r_n \\ r_1^2 & r_2^2 & \ldots & r_n^2 \\ \ldots & \ldots & & \ldots \\ r_1^{n-1} & r_2^{n-1} & \ldots & r_n^{n-1} \end{pmatrix}.$$

Всего при данном n получится $n!$ различных модифицированных преобразований. Обычное классическое ДПФ также входит в этот набор, остальные являются новыми. Так при $n=4$ получаются 24 различных МДПФ, при $n=5$ получаются 120 преобразований. Целью работы является изучение спектральных свойств указанных новых модифицированных преобразований Фурье. В частности, представляют особый интерес при $n=4N$ преобразования с симметричным спектром (при $n=4$ с простым), что не выполняется для обычных МДПФ ни в каких размерностях. Такие преобразования с симметричным спектром являются в определенном смысле более естественными, чем обычное МДПФ, так как они более похожи на свой непрерывный аналог в плане равноправности точек спектра. Не исключено, что такие преобразования за счет более простых спектральных свойств могут оказаться полезными при различных приложениях.

Далее приводятся результаты расчетов на компьютере для случая $n=4$. Получившиеся 24 модифицированных преобразования Фурье разбиты нами на группы из похожих по своим свойствам преобразований. Далее мы указываем номер соответствующего преобразования, образующую его перестановку корней и для каждой группы кратко перечисляем основные особенности на примере первого преобразования из данной группы.

1) $r=(1,-i,-1,i)$ (это обычное ДПФ), 2) $r=(1,i,-1,-i)$ (это его обратное).

Квадрат преобразования с номером 1 является действительной матрицей перестановок вида

$$F_r^2=\begin{pmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{pmatrix},$$

спектр кратный $(1,1,-1,-i)$, характеристический полином получен в явном виде: $x^4-(1-i)x^3-(1+i)x^2+(1-i)x+i$, как и набор действительных собственных векторов: $(-1,1,1,1),(0,-1,0,1),(2,1,0,1),(1,0,1,0)$.

3) $r=(-1,i,1,-i)$ 4) $r=(-1,-i,1,i)$.

Квадрат преобразования с номером 3 является действительной матрицей вида

$$F_r^2=\begin{pmatrix}0&0&1&0\\0&-1&0&0\\1&0&0&0\\0&0&0&-1\end{pmatrix},$$

спектр кратный $(1,i,i,-i)$, характеристический полином получен в явном виде

$$x^4-(1+i)x^3+(1+i)x^2-(1+i)x+i,$$

как и набор комплексных собственных векторов: $(0,-1,0,1)$, $(-1,-2i,1,0)$, $(i,1,-i,1)$, $(1,0,1,0)$.

В случаях 1–4 перестановки состоят из корней, занумерованных по кругу, причем нумерация начинается не с первообразных корней $-1,1$. Четвертая степень преобразования есть единичная матрица. Построено явно диагонализирующее преобразование.

5) $r=(-1,i,1,-i)$, 6) $r=(-1,-i,1,i)$, 7) $r=(i,-1,-i,1)$, 8) $r=(-i,-1,i,1)$.

В случаях 5–8 перестановки состоят из корней, занумерованных по кругу, причем нумерация начинается с первообразных корней $-i,i$. Степени преобразования с номером 5 имеют вид:

$$F_r^2=\begin{pmatrix}0&1&0&0\\i&0&0&0\\0&0&0&-1\\0&0&-i&0\end{pmatrix},\quad F_r^4=\begin{pmatrix}i&0&0&0\\0&i&0&0\\0&0&i&0\\0&0&0&i\end{pmatrix},\quad F_r^{16}=E.$$

Отметим, что F_r^2 напоминает матрицы спинорных представлений, а ее ненулевые блоки похожи на матрицы Паули. Это модифицированное МДПФ имеет простой спектр, состоящий из значений $\sqrt[4]{i}$, в отличии от классического преобразования той же размерности с кратным спектром !!! Характеристический полином получен в явном виде: $x^4 - i$.

С этого момента начинаются вычислительные затруднения у пакета MATHEMATICA, он не смог посчитать по одной компоненте каждого из собственных векторов по своему алгоритму, выдав их как корни некоторых уравнений высокой степени. Например, первому собственному значению соответствует такой собственный вектор

$$\left\{s, \left(1 - \sqrt{2} + \sqrt{4 - 2\sqrt{2}}\right) i, \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i, 1\right\},$$

где s является первым по нумерации пакета MATHEMATICA корнем возвратного уравнения восьмой степени

$$s^8 - 8s^7 + 32s^6 - 24s^5 + 2s^4 + 24s^3 + 32s^2 + 8s + 1 = 0.$$

9) $r = \{1, -1, i, -i\}$, 10) $r = \{1, -1, -i, i\}$, 11) $r = \{1, i, -i, -1\}$, 12) $r = \{1, -i, i, -1\}$.

Это оставшиеся перестановки, начинающиеся с 1.

Квадрат преобразования с номером 9 является комплексной матрицей следующего вида

$$F_r^2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2} + \frac{i}{2} & -\frac{i}{2} & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} + \frac{i}{2} & \frac{1}{2} - \frac{i}{2} \\ 0 & \frac{1}{2} - \frac{i}{2} & \frac{1}{2} & \frac{i}{2} \end{pmatrix}.$$

Аналогично устроены другие четные степени данной матрицы.

Это МДПФ также имеет простой спектр:

$$\left\{-\frac{\sqrt{7}+1}{4} - \frac{\sqrt{7}-1}{4} i, \frac{\sqrt{7}-1}{4} + \frac{\sqrt{7}+1}{4} i, -1, 1\right\}.$$

Характеристический полином получен в явном виде:

$$x^4 + \left(\frac{1}{2} - \frac{i}{2}\right) x^3 - (1+i)x^2 - \left(\frac{1}{2} - \frac{i}{2}\right) x + i.$$

Найден в явном виде набор из двух комплексных и двух вещественных собственных векторов: $\left\{0, \frac{1}{2} i \left((2+i) + \sqrt{7}\right), -\frac{1}{2} i \left((2-i) + \sqrt{7}\right), 1\right\}$, $\left\{0, -\frac{1}{2} i \left((-2-i) + \sqrt{7}\right), \frac{1}{2} i \left((-2+i) + \sqrt{7}\right), 1\right\}$, $\{-1, 1, 1, 1\}$, $\{3, 1, 1, 1\}$.

Осталось рассмотреть оставшиеся преобразования.

13) $r = \{i, 1, -1, -i\}$, 14) $r = \{-i, 1, -1, i\}$, 15) $r = \{-1, 1, i, -i\}$, 16) $r = \{-1, 1, -i, i\}$,

17) $r = \{i, -1, 1, -i\}$, 18) $r = \{-i, i, 1, -1\}$, 19) $r = \{-i, -1, 1, i\}$, 20) $r = \{i, -i, 1, -1\}$,

21) $r = \{i, -i, -1, 1\}$, 22) $r = \{-i, i, -1, 1\}$, 23) $r = \{-1, i, -i, 1\}$, 24) $r = \{-1, -i, i, 1\}$.

Для первого их них с номером 13 квадрат преобразования является комплексной матрицей следующего вида

$$F_r^2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ \frac{i}{2} & 0 & -\frac{1}{2} + \frac{i}{2} & \frac{1}{2} \\ -\frac{1}{2} + \frac{i}{2} & 0 & 0 & -\frac{1}{2} - \frac{i}{2} \\ \frac{1}{2} & 0 & -\frac{1}{2} - \frac{i}{2} & -\frac{i}{2} \end{pmatrix}.$$

Остальные степени состоят из заполненных матриц со все более громоздкими элементами.

Все эти МДПФ имеют простой спектр !!! Для преобразования с номером 13 спектр состоит из значения 1 и трех занумерованных в определенном порядке корней уравнения

$$2s^6 - 2s^5 + 3s^4 - 2s^3 + 3s^2 - 2s + 2 = 0,$$

которые MATHEMATICA не сумела вычислить в явном виде (хотя это возможно, т. к. данное возвратное уравнение сводится к кубическому). Характеристический полином получен в явном виде:

$$x^4 - \left(\frac{3}{2} + \frac{i}{2}\right) x^3 + (1+i)x^2 - \left(\frac{1}{2} + \frac{3}{2}i\right) x + i.$$

Собственный вектор один найден в явном виде $\{1, 1, -1, 1\}$, в трех остальных по одной компоненте равны 1, остальные найдены в неявном виде как занумерованные в определенном порядке корни уравнений вида

$$s^6 + 2s^5 + 6s^4 + 14s^3 + 25s^2 + 12s + 4 = 0, s^3 - s^2 - 4s + 2 = 0.$$

Таким образом, получается довольно неожиданный результат, что подавляющее большинство МДПФ при $n = 4$ в плане спектральных свойств устроены проще стандартного, так как все они имеют простой спектр. Из приведенных результатов вычислений следует, что лишь четыре преобразования имеют кратный спектр, как и классическое. Они отвечают случаям, когда в перестановке корни обходятся на единичной окружности по часовой стрелке или против нее, причем начиная не с первообразных корней. При этом, МДПФ, отвечающие обходу по окружности при старте с первообразных корней, по-видимому, обладают наиболее простыми спектральными свойствами.

3. Некоторые обобщения, дополнения и приложения

При произвольных n доказана унитарность всех МДПФ. Следовательно, все их спектры лежат на единичной окружности, и получен явный вид обратных преобразований. Это несложно установить пользуясь тем, что все МДПФ являются произведениями обычного ДПФ и соответствующих матриц перестановок. Отметим, что некоторые частные случаи рассмотренных здесь матриц МДПФ известны и используются в современных быстрых алгоритмах Гуда и Рейдера [1].

К сожалению, установить строго другие содержательные результаты о спектральных свойствах при произвольных n не удается ввиду сложности доказательств. При помощи компьютера для небольших n вычислены начальные степени преобразований, проекторы на собственные подпространства и резольвенты, различные стандартные алгебраические факторизации матриц. На основании анализа компьютерных вычислений представляется верной следующая гипотеза.

Гипотеза 1. При всех размерностях матриц МДПФ, кратных четырем, размерности собственных подпространств не совпадают только для МДПФ, отвечающим циклическим круговым перестановкам, которые начинаются не с первообразных корней.

Если эта гипотеза верна, то за стандартный ДПФ выбран самый неудачный вариант с точки зрения вопроса о простоте устройства спектра.

Гипотеза 2. Все МДПФ имеют базис из вещественных собственных векторов.

Заметим, что автору не известен общий критерий наличия вещественного базиса из собственных векторов у произвольной комплексной матрицы. Для обычного ДПФ способ построения такого базиса предложен в [6], идея построения следующая. Пусть уже вычислены

кратности всех собственных чисел и соответствующие проекторы на собственные подпространства, тогда собственные вектора можно получить по следующему элементарному алгоритму: выбрать стандартный базис (а в принципе – и любой другой), и подействовать на орты последовательно всеми проекторами нужное число раз с учетом кратности значений спектра. К сожалению, полного набора собственных векторов при произвольном выборе начального базиса может и не получиться.

Мы рассмотрели в работе варианты с перестановками корней, т. е. столбцов матрицы обычного ДПФ. Можно рассмотреть дальнейшее обобщение, когда одновременно переставляются и строки, т. е. мы отказываемся от того, чтобы МДПФ определялось степенной матрицей. Такие преобразования также являются унитарными и частично исследованы на компьютере. Их удобно использовать для анализа сигналов, в которых редкие ненулевые элементы разбросаны среди нулевых. Для таких сигналов ДПФ неустойчиво при вычислениях и обладает другими нежелательными свойствами. Тогда можно при помощи первой матрицы перестановки собрать все ненулевые элементы вместе, выполнить преобразование, а затем при помощи второй матрицы обратной перестановки восстановить первоначальный порядок следования элементов в массиве данных. Применение МДПФ к преобразованному сгруппированному сигналу является более предпочтительным и дает ряд вычислительных преимуществ.

Введенные МДПФ позволяют также обобщить тригонометрические суммы Гаусса [4].

О п р е д е л е н и е 2. *Обобщенной квадратичной суммой Гаусса называется след матрицы соответствующего МДПФ, то есть*

$$G(P,Q,n)=\sum_{k=0}^{n-1}\exp\left(i\frac{2\pi}{n}p(k)q(k)\right), P=(p(0),p(1),...,p(n-1)),\quad Q=(q(0),q(1),...,q(n-1)),$$

где P,Q *– две произвольные перестановки множества чисел* $(0,1,\ldots,n-1)$.

ОТКРЫТАЯ ПРОБЛЕМА. Вычислить в явном виде обобщенные квадратичные суммы Гаусса в терминах заданных перестановок P и Q, порождающих соответствующее МДПФ.

Авторам представляется, что это чрезвычайно сложная задача, никаких даже приблизительных путей ее решения в настоящее время не видно (с такой оценкой согласился в частной переписке и один из авторов монографии [4] Bruce Berndt). Тем не менее, решение сформулированной открытой проблемы позволило бы находить размерности собственных подпространств МДПФ при любых размерностях теоретически, без компьютера.

Представляют также интерес быстрые модифицированные ДПФ в сравнении со стандартным БПФ.

Отметим, что ДПФ широко применяются в криптографии. На основе результатов настоящей работы можно предложить следующий алгоритм шифрования информации. Отправитель и получатель заранее знают, какой из вариантов МДПФ данного порядка используется при обмене, а противнику (атакующему) это не известно. Ввиду огромности числа $n!$ подобный алгоритм может быть не менее стойким, чем стандартные алгоритмы с большой длиной ключа. Кроме того, при данном методе требуется минимальная модификация существующих алгоритмов и программ, сводящаяся к простой замене одной матрицы на другую. Кроме того, модифицированное преобразование Фурье и суммы Гаусса связаны с квадратичным или дробным преобразованием Фурье, которое находит применения в методе квадратичной экспоненциальной аппроксимации сигналов [8]–[11], а также в теории операторов преобразования [12]–[15].

СПИСОК ЛИТЕРАТУРЫ

1. *Ноден П., Китте К.* Алгебраическая алгоритмика М.: Мир, 1999.

2. *Нуссбаумер Г.* Быстрое преобразование Фурье и алгоритмы вычисления сверток. М.: Радио и связь, 1985.

3. *Блэйхут Р.* Быстрые алгоритмы цифровой обработки сигналов. М.: Мир, 1989.
4. *Berndt B.C., Evans R.J, Williams K.S.* Gauss and Jacobi Sums. Wiley and Sons, 1998.
5. *Ященко В.* (ред.) Введение в криптографию. СПб.: Питер, 2001.
6. *Matveev V.B.* Intertwining relations between the Fourier transform and discrete Fourier transform // Inverse Problems. 2001. No. 17. P. 633–657.
7. *Schur I.* Uber die Gausssschen Summen // Nach. Gessel. Gottingen, Math-Phys Klasse. 1921. P. 147–153.
8. *Киселев Е.А., Минин Л.А., Новиков И.Я., Ситник С.М.* О константах Рисса для некоторых систем целочисленных сдвигов // Математические заметки. 2014. Т. 96. Вып. 2. С. 239–250.
9. *Zhuravlev M.V., Kiselev E.A., Minin L.A., Sitnik S.M.* Jacobi theta-functions and systems of integral shifts of Gaussian functions // Journal of Mathematical Sciences, Springer. 2011. V. 173. № 2. P. 231–241.
10. *Минин Л.А., Журавлев М.В., Ситник С.М.* О вычислительных особенностях интерполяции с помощью целочисленных сдвигов гауссовых функций // Научные ведомости Белгородского государственного университета. Математика. Физика. 2009. № 13 (68). Вып. 17/2. С. 89–99.
11. *Ситник С.М., Тимашов А.С., Ушаков С.Н.* Метод конечномерных приближений в задачах квадратичной экспоненциальной интерполяции // Научные ведомости Белгородского государственного университета. Математика. Физика. 2015. № 17 (214). Вып. 40. С. 130–142.
12. *Sitnik S.M.* Transmutations and Applications: a survey // arXiv: 1012.37412012. 2012. 141 P.
13. *Катрахов В.В., Ситник С.М.* Краевая задача для стационарного уравнения Шредингера с сингулярным потенциалом // Доклады Академии наук СССР. 1984. Т. 278. № 4. С. 797–799.
14. *Ситник С.М.* Факторизация и оценки норм в весовых лебеговых пространствах операторов Бушмана-Эрдейи // ДАН СССР. 1991. Т. 320. № 6. С.1326–1330.
15. *Ситник С.М.* Компьютерный анализ спектральных свойств модифицированных дискретных преобразований Фурье. // Доклады Адыгской (Черкесской) Международной академии наук. 2007. Т. 9. № 1. С. 98–103.

Поступила в редакцию 25 февраля 2016 года.

Рыжкова Елена Валерьевна, Воронежский институт Министерства внутренних дел России, г. Воронеж, Российская Федерация, кандидат педагогических наук, доцент кафедры математики и моделирования систем, e-mail: dikareva_ev@mail.ru

Ситник Сергей Михайлович, Воронежский институт Министерства внутренних дел России, г. Воронеж, Российская Федерация, кандидат физико-математических наук, доцент кафедры математики и моделирования систем, e-mail: mathsms@yandex.ru

UDC 517.443
DOI: 10.20310/1810-0198-2016-21-2-408-416

THE MODIFIED DISCREET FOURIER TRANSFORM BASED ON THE GROUP OF ROOTS OF UNITY

© **E. V. Ryzhkova, S. M. Sitnik**

In the paper we consider a set of transformations which generalize a standard discreet Fourier transform (DFT). These generalizations are based on permutations for the group of roots of unity. Different permutations define different new DFT's. On this way we construct transformations with more natural spectral properties. For example in dimension four the standard DFT has incomplete multiple spectrum but almost all newly defined transforms a simple one. We give some numerical computer results and spectral hypotheses. Applications to cryptography is briefly outlined.
Key words: discreet Fourier transform; roots of unity; permutations; matrix spectrum; eigenvectors.

REFERENCES

1. *Noden P., Kitte K.* Algebraic algorithmics. M.: Mir, 1999.

2. *Nussbaumer G.* Fast Fourier transform and convolution numerical algorithms. M.: Radio I Svyaz, 1985.

3. *Blayhoot P.* Fast algorithms for digital signal processing. M.: Mir, 1989.

4. *Berndt B.C., Evans R.J, Williams K.S.* Gauss and Jacobi Sums. Wiley and Sons, 1998.

5. *Yaschenko V.* Introduction to cryptology. St. Petersburg, 2001.

6. *Matveev V.B.* Intertwining relations between the Fourier transform and discrete Fourier transform // Inverse Problems. 2001. № 17. P. 633–657.

7. *Schur I.* Uber die Gaussschen Summen // Nach. Gessel. Gottingen, Math-Phys Klasse. 1921. P. 147–153.

8. *Kiselev E.A., Minin L.A., Novikov I. Ya., Sitnik S.M.* On Riesz constants for some systems of integer translations // Math. Notes. 2014. V. 96. № 2. P. 239–250.

9. *Zhuravlev M.V., Kiselev E.A., Minin L.A., Sitnik S.M.* Jacobi theta-functions and systems of integral shifts of Gaussian functions // Journal of Mathematical Sciences, Springer. 2011. V. 173. № 2. P. 231–241.

10. *Zhuravlev M.V., Minin L.A., Sitnik S.M.* On numerical analysis of interpolation by integer translations of the Gaussian function // Scientific Bulletin of Belgorod State University. 2009. V. 13 (68). № 17/2. P. 89–99.

11. *Sitnik S.M., Timashov A.S., Uschakov S.N.* Finite dimensional approximations in problems of quadratic interpolation // Scientific Bulletin of Belgorod State University. 2015. V. 17 (214). № 40. P. 130–142.

12. *Sitnik S.M.* Transmutations and Applications: a survey // arXiv: 1012.37412012. 2012. 141 P.

13. *Katrahov V.V. , Sitnik S.M.* Boundary-value problem for stationary Schrodinger equation with singular potential // DAN SSSR. 1984. V. 278. № 4. P. 797–799.

14. *Sitnik S.M.* Factorization and norm estimates in weighted Lebesgue spaces of Buschman-Erdelyi transmutations // DAN SSSR. 1991. V. 320. № 6. P.1326–1330.

15. *Sitnik S.M.* Computer analysis of spectral properties of modified discreet Fourier transforms // Doklady Adygskoi International Academy of Sciences. 2007. V. 9. № 1 P. 98-103.

Received 25 February 2016.

Ryzhkova Elena Valeryevna, Voronezh Institute of the Russian Ministry of Internal Affairs, Voronezh, the Russian Federation, Candidate of Pedagogical Sciences, Associate Professor of the Mathematics and System Modelling Department, e-mail: dikareva_ev@mail.ru

Sitnik Sergei Michailovich, Voronezh Institute of the Russian Ministry of Internal Affairs, Voronezh, the Russian Federation, Candidate of Physics and Mathematics, Associate Professor of the Mathematics and System Modelling Department, e-mail: mathsms@yandex.ru