семнадцатого научно-практического семинара. М.: Институт прикладной математики им. М.В. Келдыша РАН, 2014. С. 292-300.

13. А.И. Недошивина, С.М. Ситник. Приложения геометрических алгоритмов локализации точки на плоскости к моделированию и сжатию информации в задачах видеонаблюдений. Вестник Воронежского государственного технического университета. 2013, Т. 9 (4), С. 108-111.

14. С.М. Ситник. Компьютерный анализ спектральных свойств модифицированных дискретных преобразований Фурье. Доклады Адыгской (Черкесской) Международной академии наук. 2007, Т. 9 (1), С. 98-103.

УДК 519.651

ОБ ОДНОМ ВАРИАНТЕ ДИСКРЕТНОГО ПРЕОБРАЗОВАНИЯ ФУРЬЕ

ON A VARIANT OF DISCREET FOURIER TRANSFORM

Ситник С.М.

Воронежский институт МВД России

г. Воронеж, Россия.

DOI: 10.12737/16947

Аннотация: в работе рассматривается набор преобразований, которые обобщают известное дискретное преобразование Фурье (ДПФ). Эти обобщения определяются при помощи группы перестановок комплексных корней из единицы.

Summary: we consider a class of generalizations of the discreet Fourier transform. They are defined by a group of permutations of roots of unity.

Ключевые слова: дискретное преобразование Фурье, корни из единицы, матричная форма.

Keywords: discreet Fourier transform, roots of unity, matrix form.

Дискретное преобразование Фурье (ДПФ) является одним из самых известных и полезных на практике математических инструментов. Это преобразование широко применяется, например, при проектировании и оптимизации различных автоматизированных систем, 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. Фундамен-

тальное значение также имеют быстрые алгоритмы ДПФ, в которых число необходимых операций уменьшено по сравнению с обычным бесхитростным вычислением за счёт изощрённой оптимизации порядка выполнения действий. Наиболее известны быстрые алгоритмы Гуда, Кули и Тьюки, Винограда, Рейдера. Фундаментальную роль ДПФ играет в современной криптографии.

Несмотря на общеизвестность преобразования ДПФ, некоторые стандартные задачи для него имеют незнакомые широкому кругу специалистов свойства. Рассмотрим в качестве примера естественную задачу о нахождении спектра ДПФ при любом n. Решение этой задачи отсутствует в основной литературе по преобразованиям Фурье и нетривиально. Известно, что четвертая степень ДПФ есть тождественное преобразование, поэтому собственными значениями могут быть лишь числа ± 1, $\pm i$. Основная сложность состоит в вычислении кратностей этих собственных значений. Аналогия с непрерывным преобразованием Фурье, для которого четыре этих значения совершенно равноправны, приводит к весьма правдоподобному предположению, что хотя бы в случае размерности $n = 4m$ собственные значения ДПФ также равноправны, и, следовательно, все имеют кратность m.

Однако вычисления уже при $n = 4$ опровергают это предположение. В этом случае значения -1, $-i$ являются простыми, значение 1 имеет кратность 2, а значение i вообще отсутствует в спектре! Всё это нарушает симметрию спектра, присущую непрерывному случаю.

Определение. Рассмотрим множество корней степени n из единицы, упорядоченное произвольным способом $r = (r_1, r_2, \ldots r_n)$. Назовём модифицированным дискретным преобразованием Фурье (МДПФ), построенным по данной перестановке r множества корней из единицы, оператор с матрицей размеров n x n следующего вида

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

Ясно, что в результате получается с точностью до множителя некоторая степенная матрица (Вандермонда). Всего при данном n получится $n!$ различных модифицированных преобразований. Обычное классическое ДПФ и его обратное также входят 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 преобразования при $n=4m$ с симметричным спектром (а при $n=4$ ещё и с простым), в котором все собственные значения имеют одинаковые кратности. Это не выполняется для обычных ДПФ ни при каких размерностях, как следует из приведённой выше таблицы 2. Такие преобразования с симметричным спектром являются в определённом смысле более естественными, чем обычное ДПФ, так как они ближе к своему непрерывному аналогу в плане равноправности точек спектра. Не исключено, что такие МДПФ за счёт более простых спектральных свойств могут оказаться полезнее в различных вычислительных приложениях.

Отметим, что ДПФ широко применяются в криптографии. На основе результатов настоящей работы можно в принципе предложить следующий алгоритм шифрования информации. Отправитель и получатель заранее знают, какой из вариантов МДПФ данного порядка используется при обмене, а противнику 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 ДПФ находит применения в теории операторов преобразования и компьютерной графике [8-14].

Список литературы

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

2. Минин Л.А., Ситник С.М., Ушаков С.Н. Поведение коэффициентов узловых функций, построенных из равномерных сдвигов функций Гаусса и Лоренца//Научные ведомости Белгородского государственного университета. Серия: Математика, Физика. 2014, №7 (183), Выпуск 35, С. 214-217.

3. Киселев Е.А., Минин Л.А., Новиков И. Я., Ситник С. М. О константах Рисса для некоторых систем целочисленных сдвигов// Математические заметки. 2014, Том 96, выпуск 2, С. 239-250.

4. С.М. Ситник, А.С. Тимашов. Метод конечномерных приближений в задачах квадратичной экспоненциальной интерполяции сигналов. Вестник Воронежского института МВД России.2014, № 2, С. 163-171.

5. E.A. Kiselev, L.A. Minin, I.Ya. Novikov, S.M. Sitnik. On the Riesz Constants for Systems of Integer Translates. Mathematical Notes. Springer. 2014, Vol. 96 (1-2), P. 228-238.

6. С.М. Ситник. Обобщённые дискретные преобразования Фурье и их спектральные свойства. "Новые информационные технологии в автоматизированных системах". Материалы семнадцатого научно-практического семинара. М.: Институт прикладной математики им. М.В. Келдыша РАН, 2014. С. 281-291.

7. С.М. Ситник. Компьютерный анализ спектральных свойств модифицированных дискретных преобразований Фурье. Доклады Адыгской (Черкесской) Международной академии наук. 2007, Т. 9 (1), С. 98-103.

8. Ситник С. М. Унитарность и ограниченность операторов Бушмана-Эрдейи нулевого порядка гладкости// Препринт. Институт автоматики и процессов управления ДВО АН СССР.—1990.—44 С.

9. Ситник С. М. Решение задачи об унитарном обобщении операторов преобразования Сонина–Пуассона // Научные ведомости Белгородского государственного университета.—2010.—Вып. 18,№5 (76).—С. 135–153.

10. Катрахов В.В., Ситник С.М. Композиционный метод построения B--эллиптических, B--гиперболических и B--параболических операторов преобразования// ДАН СССР, 1994. № 337;3. С.307-311.

11. Ситник С.М. Факторизация и оценки норм в весовых лебеговых пространствах операторов Бушмана-Эрдейи// ДАН СССР. 1991. т.320, №6. С. 1326--1330.

12. Катрахов В.В., Ситник С.М. Краевая задача для стационарного уравнения Шрёдингера с сингулярным потенциалом// ДАН СССР. 1984. Т. 278, №4. С.797-799.

13. А.И. Недошивина, С.М. Ситник. Приложения геометрических алгоритмов локализации точки на плоскости к моделированию и сжатию информации в задачах видеонаблюдений. Вестник Воронежского государственного технического университета. 2013, Т. 9 (4), С. 108-111.

14. Ситник С.М., Тимашов А.С. Расчёт конечномерной математической модели в задаче квадратичной экспоненциальной интерполяции // Научные ведомости Белгородского государственного университета. Серия: Математика, Физика.-2013.- №19 (162). Вып. 32.- С. 184-186.

15. Ситник С.М., Тимашов А.С. Приложения экспоненциальной аппроксимации по целочисленным сдвигам функций Гаусса // Вестник Воронежского государственного университета инженерных технологий.- 2013.- № 2 (56).- С. 90-94.