УДК519.711

МЕТОД ПОИСКА СИММЕТРИЧЕСКИХ МАТРИЦ ФУНКЦИЙ ВИЛЕНКИНА-КРЕСТЕНСОНА

Д. С. Демьяник, *инженер,*
ООО «Неткрекер»,
ул. Супруна, д. 11, г. Сумы, 40000, Украина;
E-mail: demyanik1985@ukr.net

Статья посвящена исследованиям систем функций Виленкина-Крестенсона (ВКФ). Данные функции подходят для проведения обобщённых дискретных преобразований Фурье. Одним из преимуществ базиса ВКФ является существование большого множества симметрических матриц преобразования одинаковой размерности. В статье описан метод поиска полного набора таких матриц.

Ключевые слова: *функции Виленкина-Крестенсона, ортогональные преобразования, обобщённые преобразования Фурье, матрица преобразования, индикаторная матрица.*

ВВЕДЕНИЕ

Одним из этапов обработки сигнала часто является получение его спектра. Обычно под спектром сигнала понимается ортогональное преобразование базисом для которого выступает ряд Фурье. При цифровой обработке данных имеют дело с дискретными преобразованиями Фурье. При этом само преобразование сигнала сводится к получению весовых коэффициентов линейно независимых дискретных функций. Количество весовых коэффициентов равно количеству отсчётов дискретного сигнала. Восстанавливается дискретный сигнал из дискретного спектра путём суммирования функций, умноженных на соответствующий весовой коэффициент. Кроме, собственно, функций Фурье для получения спектра сигнала может быть использован любой базис линейно независимых функций. Получение спектра сигнала в базисе отличном от базиса Фурье часто называют обобщёнными преобразованиями Фурье. При этом для того, чтобы погрешности прямого и обратного преобразований были минимальными необходимо, чтобы набор функций, представляющий собой базис для обобщённых преобразований, был ортогональным [1]. А для того, чтобы с дискретным спектром было удобно работать, эти функции должны иметь одинаковые нормы. Таким образом, базис должен быть ортонормированным. В этом случае формулы прямого и обратного обобщённого дискретного преобразования Фурье принимают следующий вид:

$$S(k) = \sum_{x=0}^{N-1} s(x)\varphi_k(x),$$

$$s(x) = \frac{1}{N}\sum_{k=0}^{N-1} S(k)\overline{\varphi_k(x)}, \qquad (1)$$

где $s(x)$ – дискретный сигнал, а $S(k)$ – его спектр в выбранном базисе дискретных ортонормированных функций $\varphi_k(x)$; N – количество отсчётов

сигнала; x – аргумент функции или порядковый номер отсчёта, являющийся нормированным временем; k – порядковый номер (или просто – порядок) базисной функции. Черта над функцией означает комплексно-сопряжённую функцию.

Базис тригонометрических дискретно-экспоненциальных функций (ДЭФ) – дискретный базис Фурье – стал исторически первым базисом, который использовали для дискретных ортогональных преобразований. Базис описывается следующей формулой:

$$\varphi_k(x) = e^{j\frac{2\pi}{N}kx}, \qquad (2)$$

значение переменных, использованных в этом выражении, совпадает со значением переменных из системы (1).

Одним из базисов, который недостаточно изучен на сегодняшний день и который может применяться для ортогональных дискретных преобразований, является базис функций Виленкина-Крестенсона (ВКФ).

ПОСТАНОВКА ЗАДАЧИ

Базис дискретных преобразований может быть описан при помощи матрицы. Практический интерес представляют симметрические базисы ВКФ, поскольку именно для симметрических базисов возможно применение алгоритма быстрых преобразований. Одним из преимуществ систем ВКФ перед ДЭФ является наличие очень большого числа симметричных матриц преобразования для первого базиса, по сравнению с относительно малым количеством симметричных матриц для второго. Это достоинство систем ВКФ может быть использовано, в частности, в криптографии.

Для изучения свойств данных базисов необходимо иметь возможность синтезировать полный объём симметрических базисов ВКФ с заданными параметрами. Задачей данной статьи является описание метода, позволяющего найти всё множество симметрических матриц систем ВКФ с известными параметрами.

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Матрица системы ВКФ является кронекеровской степенью матрицы ДЭФ. Поэтому матрицу ДЭФ можно считать частным случаем матрицы ВКФ [2]. Базисная функция системы ВКФ выглядит следующим образом:

$$\varphi_k(x) = e^{j\frac{2\pi}{m}\sum_{i=1}^{n} k_i x_i}, \qquad (3)$$

где m – основание системы счисления; k_i – i-й разряд числа k записанного в позиционной m-ичной системе; n – число разрядов в m-ичном представлении значения N, которое определяет длину выборочных отсчетов сигнала, причем $N = m^n$. Спектр дискретной последовательности находится путём умножения вектора-столбца, содержащего отсчёты сигнала, на матрицу преобразования.

Быстрое преобразование Фурье (БПФ) дискретной последовательности в базисе ВКФ требуют меньшего количества вычислений, чем БПФ аналогичной по длине последовательности в базисе ДЭФ [2].

Для того чтобы восстановить сигнал по его спектру необходимо спектр сигнала, представленный в виде вектора-столбца, умножить справа на матрицу, транспонированную по отношению к матрице преобразования и содержащую элементы, комплексно-сопряжённые с элементами матрицы преобразования. Очевидно, что если матрица преобразования симметрична, то от матрицы обратного преобразования она будет отличаться лишь знаком перед комплексными частями своих элементов. Соответственно при БПФ графы прямого и обратного преобразований будут иметь одинаковые формы. В этом и заключается интерес использования именно симметричных систем ВКФ. Возможность использования в криптографии преобразований Фурье в базисе ВКФ, о которой упоминалось выше, заключается в том, что спектр дискретной последовательности представляет собой криптограмму, расшифровка которой возможна при наличии «правильной» матрицы преобразования. Кроме того, ортогональные преобразования в базисе ВКФ могут быть использованы и для определения частоты гармонического сигнала, который принимается на фоне помехи.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Поиск симметричных систем ВКФ. Если число дочерних симметричных систем, которые можно получить из материнской системы ДЭФ, переставляя её строки (или столбцы), совпадает с количеством натуральных чисел на интервале $1...N-1$, не имеющих с N общих делителей, то для систем ВКФ это число на порядки больше [3]. Поэтому очень нерационально искать симметричные системы, последовательно меняя местами строки исходной матрицы и проверяя симметричность полученной матрицы. На практике для поиска и хранения симметричных систем ВКФ гораздо более экономичным является использование индикаторных матриц. Индикаторными матрицами систем ВКФ являются такие невырожденные в кольце вычетов по модулю m квадратные n-го порядка матрицы M с элементами, принадлежащими множеству {0, 1,..., m-1}, с помощью которых устанавливается однозначное соответствие

$$y = (xM)_m \tag{4}$$

между номером $x \in \overline{0, N-1}$ строки матрицы ВКФ-Пэли и номером строки y новой системы ВКФ [3]. Матрица ВКФ-Пэли образуется в результате m-ичной инверсии номеров строк матрицы, сформированной по формуле (2), т. е.

$$\varphi_k^{Peli}(x) = e^{j\frac{2\pi}{m}\sum_{i=1}^{n} k_{n+1-i}x_i}. \tag{5}$$

Видно, что размерность индикаторной матрицы всегда равна параметру n и не зависит от параметра m системы ВКФ и поэтому во много раз меньше размерности системы ВКФ, равной m^n.

Определитель индикаторной матрицы не имеет общих делителей с m, кроме того, все индикаторные матрицы являются симметричными. Это набор необходимых и достаточных условий для того, чтобы назвать матрицы порядка n, содержащую элементы от 0 до m-1, индикаторной для симметричной системы ВКФ с параметрами m и n. Таким образом, задача поиска симметричных систем ВКФ с заданными параметрами сводится к поиску всех возможных матриц, удовлетворяющих перечисленным выше в этом абзаце параметрам.

Программная реализация поиска индикаторных матриц систем ВКФ. Разработанная программа осуществляет поиск индикаторных матриц и отображение на экране любой из них. Структурная схема той части программы, которая находит все индикаторные матрицы, изображена на рис. 1.

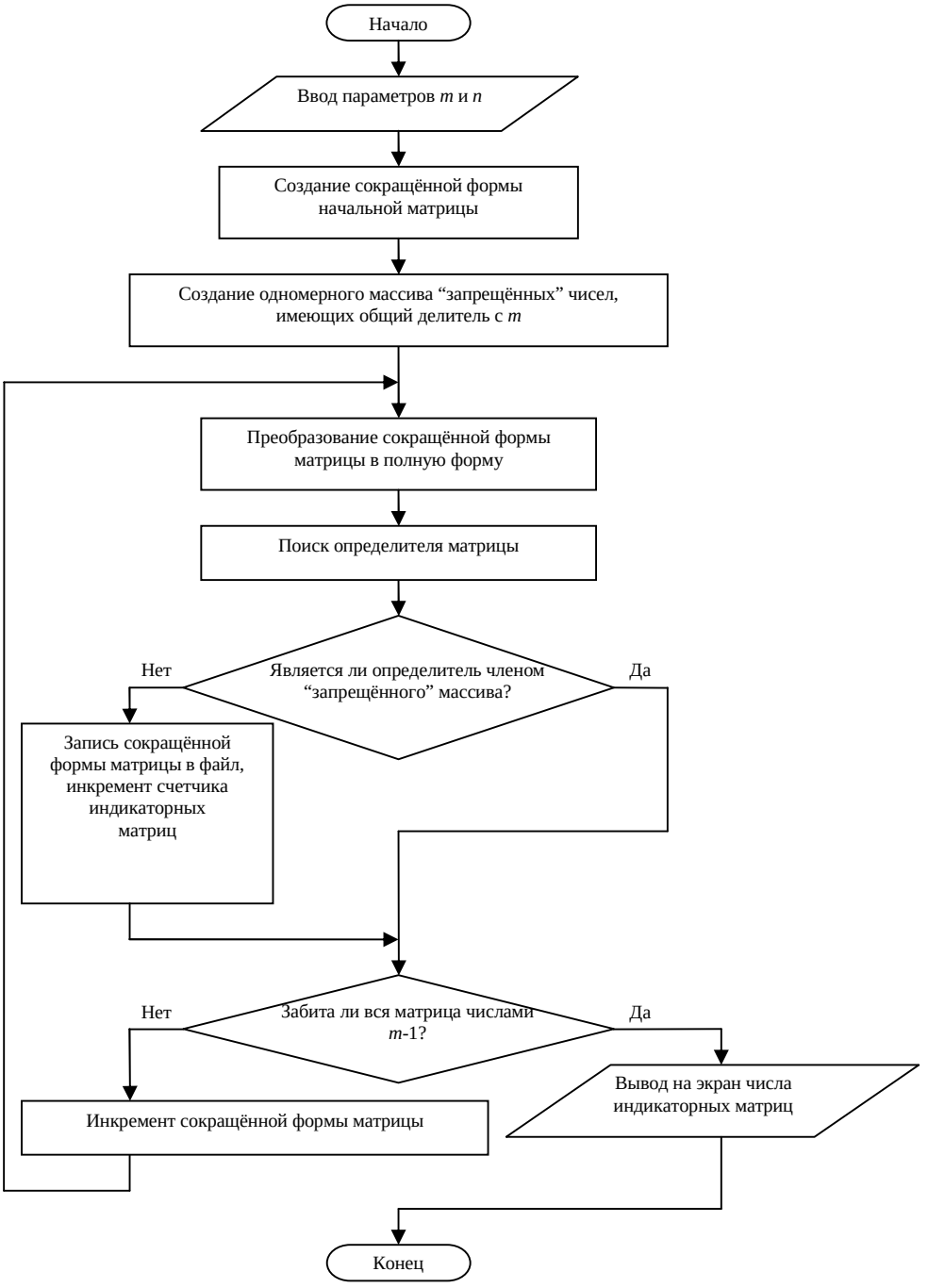

Рисунок 1 – Блок-схема программы

В соответствующие поля в окне программы нужно ввести значения m и n. Затем нужно нажать кнопку “Синтезировать индикаторные матрицы”. Программа ищет числа, имеющие общий делитель с m, если такие числа находятся, то они помещаются в массив “запрещённых определителей”.

После этого в программе создаётся одномерный массив, имеющий длину $\frac{(n+1)n}{2}$, представляющий собой сокращённую форму записи матрицы. Этот массив содержит почти вдвое меньше элементов, чем индикаторная матрица. Подобное сокращение возможно благодаря правосторонней симметрии, которой обладают матрицы. Уникальными элементами матрицы являются n элементов, лежащих вдоль побочной диагонали, а также все элементы лежащие выше неё. Их количество равно сумме натуральных чисел от 1 до n, которое определяется указанным выше выражением. Пример начального массива (представляющего сокращённую форму записи матрицы размерностью n^2, содержащую единицы вдоль побочной диагонали и нули в других ячейках) представлен на рис. 2.

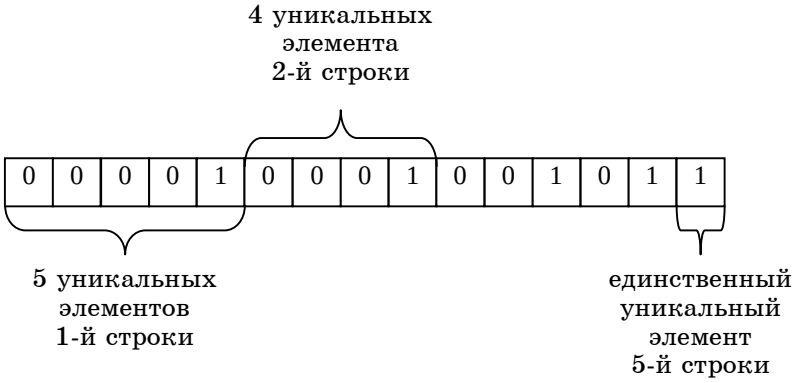

Рисунок 2 – Структура сокращённой формы записи матрицы

Если этот массив разбить на несколько строк следующим образом: 5 первых элементов – первая строка, 4 следующих – вторая, и т.д., самый последний элемент – пятая строка, то получится левая верхняя часть матрицы; элементы, расположенные ниже побочной диагонали, определяются свойством симметрии матрицы.

Далее этот массив по описанному правилу преобразуется в матрицу. Программа находит определитель матрицы. Если определитель не имеет общих делителей с m, массив заносится в файл, а счётчик индикаторных матриц увеличивается на 1.

На следующем этапе программа увеличивает младший (самый правый) разряд массива, не равный m-1, на единицу. Над этим массивом проводятся действия, описанные в предыдущем абзаце. Так происходит до тех пор, пока все элементы массива не становятся равны m-1. Массивы, соответствующие всем найденным индикаторным матрицам заносятся в файл.

ВЫВОДЫ

Описанный в статье метод позволяет найти всё множество симметрических матриц ВКФ с заданными параметрами. Количество

таких матриц, найденное при помощи данного метода, совпадает с оценкой, приведённой в [3]. Полученные матрицы могут быть применены для быстрых обобщённых преобразований Фурье.

SUMMARY

SEARCH METHOD OF SYMMETRIC MATRICES OF VYLENKYN–KRESTENSON FUNCTIONS

D. S. Demyanyk,
«Netkreker " Ltd
11. Supruna Str., Sumy, 40000, Ukraine;
E-mail: demyanik1985@ukr.net

Article is dedicated to researches of Vilenkin-Krestenson's functions (VKF). These functions can be used for generalized discrete Fourier transformations. One of the advantages of VKF basis is an existence of big quantity of symmetrical equidimensional transformation matrices. Method of investigation of full totality of such matrices is described in the article.

Keywords: *Vilenkin-Krestenson functions, orthogonal transforms, generalized Furier transforms, transformation matrix, indicator matrix.*

РЕЗЮМЕ

МЕТОД ПОШУКУ СИМЕТРИЧНИХ МАТРИЦЬ ФУНКЦІЙ ВИЛЕНКИНА–КРЕСТЕНСОНА

Д. С. Дем'яник,
ТОВ « НЕТКРЕКЕР»,
вул. Супруна, 11, м. Суми, 40000, Україна;
E-mail: demyanik1985@ukr.net

Стаття присвячена дослідженням систем функцій Виленкина-Крестенсона (ВКФ). Дані функції підходять для проведення узагальнених дискретних перетворень Фур'є. Однією з переваг базису ВКФ є існування великої множини симетричних матриць перетворення однакової розмірності. У статті описаний метод пошуку повного набору таких матриць.

Ключові слова: *функції Виленкина-Крестенсона, ортогональні перетворення, узагальнені перетворення Фур'є, матриця перетворення, індикаторна матриця.*

СПИСОК ЛИТЕРАТУРЫ

1. Бабак В. П. Сигналы и спектры : учебное пособие / В. П. Бабак, А. Я. Белецкий, А.Н. Гуржий. – К. : Книжкове вид-во НАУ, 2005. – 520 с.
2. Трахтман А. М. Основы теории дискретных сигналов на конечных интервалах / А. М.Трахтман, В. А. Трахтман. - М. : Сов. Радио, 1975. – 208 с.
3. Белецкий А. Я. Преобразования Грея : монография; в двух томах / А. Я. Белецкий, А. А.Белецкий, Е. А. Белецкий. – Т. 2. Прикладные аспекты. – К. : Книжкове вид-во НАУ, 2007. – 644 с.

Поступила в редакцию 6 ноября 2013 г.