УДК 519.711

ПРОГРАМНИЙ СИНТЕЗ ІНДИКАТОРНИХ МАТРИЦЬ ДЛЯ СИСТЕМ ВІЛЕНКИН—АКРЕСТЕНСОНА ФУНКЦІЙ

Білецький А. Я., д-р техн. наук; Дем'яник Д. С

Національний авіаційний університет

Deniska-85@inbox.ru

Стаття присвячена дослідженням ортогонального базису функцій Віленкіна—Крестенсона. У цьому базисі спектр сигналу можливо отримати швидше, ніж за допомогою класичного тригонометричного базису Фур'є. Іншою його перевагою є можливість синтезувати на порядки більшу кількість симетричних матриць перетворення, ніж для класичного базису. Саме про синтез таких матриць йде мова у статті.

Ключові слова: перетворення Фур'є, функції Віленкіна—Крестенсона, спектральний аналіз.

The article is dedicated to the researching of orthogonal basis of Vilenkin-Krestenson functions. Signal's spectrum can be obtained faster in this basis than in classic Fourier's trigonometrical basis. The second it's advantage is ability to synthesize in few degrees more symmetrical transform matrices than for classic basis. The synthesis of these matrices is the object of this article.

Key words: Fourier:transform, Vilenkin—Krestenson's functions, spectral analysis.

Вступ

Однією з найпоширеніших операцій, що здійснюються при обробці сигналів, є отримання їх спектрів. Спектри знаходяться за допомогою перетворень Фур'є. Для дискретної послідовності відліків сигналу це перетворення являє собою отримання вагових коефіцієнтів для лінійно незалежних дискретних функцій. Кількість цих коефіцієнтів дорівнює кількості відліків дискретного сигналу. Сума функцій, кожна з яких помножена на свій коефіцієнт, дає вихідну послідовність відліків з точністю до деякого постійного множника. Для того щоб мінімізувати похибки обчислень, набір використовуваних для перетворень Фур'є функцій має бути ортогональним [1]. Для зручності роботи з отриманим набором коефіцієнтів, що називається дискретним спектром сигналу, функції повинні бути ортонормованими. Формули прямого і зворотного дискретних перетворень Фур'є (ДПФ) мають вигляд:

© А. Я. Білецький, Д. С. Дем'яник, 2010

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

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

де $s(x)$ — дискретний сигнал; $S(k)$ — його спектр у вибраному базисі дискретних ортонормованих функцій $\varphi_k(x)$; N — кількість відліків сигналу; x — аргумент функції або порядковий номер відліку, що є нормованим часом; k — порядковий номер (або просто — порядок) базисної функції. Риска над функцією означає комплексно-пов'язану функцію.

Історично першим і часто використовуваним для отримання спектру дискретних сигналів набором функцій є базис тригонометричних (дискретно-експоненційних) функцій Фур'є (ДЕФ). Ці функції мають такий вигляд:

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

причому змінні функції збігаються зі змінними, що використовуються в системі (1). Базис функцій Віленкина—Крестенсона (ВКФ) може бути успішно використаний для вирішення завдань, пов'язаних зі спектральним аналізом. Проте він ще не знайшов широкого розповсюдження.

Постановка завдання

Однією з переваг систем ВКФ перед системами ДЕФ є наявність дуже великого числа симетричних систем перетворення для першого базису порівняно з відносно малою кількістю симетричних матриць для другого. Ця перевага систем ВКФ може бути використана в криптографії. У цій статті описується метод пошуку симетричних систем ВКФ.

Теоретичні відомості

Матриця системи ВКФ являє собою кронекеровську ступінь матриці ДЕФ. Тому матрицю ДЕФ можна вважати окремим випадком матриці ВКФ [2]. Функції базису Віленкина—Крестенсона мають такий вигляд:

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

де m — основа системи числення; k_i — i-й розряд числа k записаного в позиційній m-ічній системі; n — число розрядів у m-ічному поданні значення N, яке визначає довжину вибіркових відліків сигналу, причому спектр дискретної послідовності знаходиться шляхом множення вектора-стовпця, що містить відліки сигналу на матрицю перетворення.

Швидкі перетворення Фур'є (ШПФ) дискретної послідовності в базисі ВКФ потребують меншої кількості обчислень, ніж ШПФ аналогічної за довжиною послідовності в базисі ДЕФ [2].

Для того, щоб відновити сигнал за його спектром, необхідно спектр сигналу, представлений у вигляді вектора-стовпця, помножити праворуч на матрицю, що транспонована відносно до матриці перетворення і містить елементи, комплексно-сполучені з елементами матриці перетворення.

Отже, що якщо матриця перетворення симетрична, то від матриці зворотного перетворення вона буде відрізнятися лише знаком перед комплексними частинами своїх елементів. Відповідно, при ШПФ графи прямого і зворотного перетворень матимуть однакові форми. У цьому і полягає завдання використання саме симетричних систем ВКФ. Можливість використання в криптографії перетворень Фур'є в базисі ВКФ, про яку згадувалося вище, полягає в тому, що спектр дискретної послідовності являє собою криптограму, розшифровка якої можлива за наявності «правильної» матриці перетворення.

Пошук симетричних систем ВКФ

Якщо число дочірніх симетричних систем, які можна отримати з материнської системи ДЕФ, переставляючи її рядки (або стовпці), збігається з кількістю натуральних чисел на інтервалі, які не мають з N спільних дільників, то для систем ВКФ це число на порядки більше [3]. Тому дуже нераціонально шукати симетричні системи, послідовно змінюючи місцями рядки вихідної матриці і перевіряючи симетричність отриманої матриці. На практиці для пошуку і зберігання симетричних систем ВКФ набагато більш економічним є використання індикаторних матриць. Індикаторними матрицями систем ВКФ є такі невироджені в кільці залишків за модулем m квадратні n-го порядку матриці M з елементами, що належать множині (0, 1, …, m–1), за допомогою яких встановлюється однозначна відповідність

$$y = (xM)_m,$$

між номером рядка матриці ВКФ-Пелі і номером рядка нової системи ВКФ [3].

Матриця ВКФ-Пелі утворюється в результаті m-ічної інверсії номерів рядків матриці, сформованої за формулою (2), тобто

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

Видно, що розмірність індикаторної матриці завжди дорівнює параметру n і не залежить від параметра m системи ВКФ, і тому у багато разів менше розмірності системи ВКФ, що дорівнює m^n.

Визначник індикаторної матриці не має загальних дільників з m; крім того, всі індикаторні матриці є симетричними. Це набір необхідних і достатніх умов для того, щоб назвати матрицю порядку n, що містить елементи від 0 до m–1, індикаторною для симетричної системи ВКФ з параметрами m і n. Таким чином, завдання пошуку симетричних систем ВКФ із заданими параметрами зводиться до пошуку всіх можливих матриць, що задовольняють переліченим вище в цьому абзаці умовам.

Програмна реалізація пошуку індикаторних матриць систем ВКФ

Розроблена програма здійснює пошук індикаторних матриць і відображення на екрані будь-якої з них. Структурна схема тієї частини програми, яка знаходить індикаторні матриці, зображена на рис. 1.

Рис. 1. Блок-схема програми

У відповідні поля у вікні програми потрібно ввести значення *m* і *n*. Потім слід натиснути кнопку «Синтезировать индикаторные матрицы». Програма шукатиме числа, що мають спільний дільник з *m*, якщо такі числа знаходяться, то вони заносяться до масиву «заборонених визначників».

Після цього в програмі створюється одновимірний масив, що має довжину $\frac{(n+1)n}{2}$. Цей масив —скорочена форма запису матриці. Він міститиме майже вдвічі менше елементів, ніж індикаторна матриця. Таке скорочення можливе завдяки правосторонній симетрії, яка притаманна матрицям. Вільними елементами матриці є *n* елементів, що лежать уздовж побічної діагоналі, а також всі елементи, що лежать вище неї. Їх кількість дорівнює сумі натуральних чисел від 1 до *n*, яке визначається наведеним вище виразом. Приклад початкового масиву (що є скороченою формою запису матриці розмірністю 5×5, яка містить одиниці вздовж побічної діагоналі і нулі в інших комірках) подано на рис. 2.

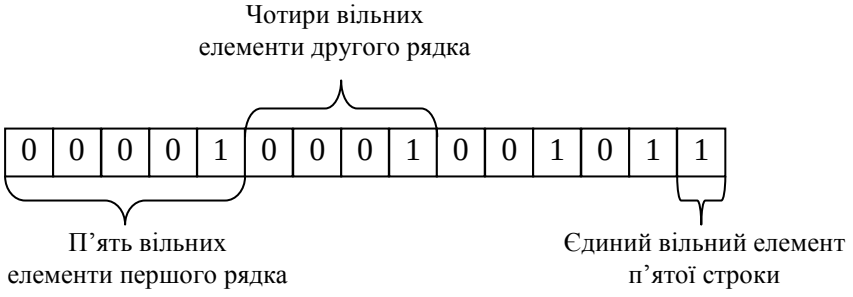

Рис. 2. Структура скороченої форми запису матриці

Якщо цей масив розділити на кілька рядків таким чином: 5 перших елементів — перший рядок, 4 наступних — другий, і т.д., самий останній елемент — п'ятий рядок, то вийде ліва верхня частина матриці; елементи, розташовані нижче побічної діагоналі визначаються властивістю симетрії матриці.

Далі цей масив за описаним правилом перетворюється в матрицю. Програма знаходить визначник матриці. Якщо визначник не має загальних дільників з m, масив заноситься у файл, а лічильник індикаторних матриць збільшується на одиницю.

На наступному етапі програма збільшує молодший (самий правий) розряд масиву, що не дорівнює $m - 1$, на одиницю.

Всі елементи, розташовані праворуч від нього, анулюються. Над цим масивом проводяться дії, описані в попередньому абзаці. Так відбувається доти доки всі елементи масиву не зрівнюватимуть $m - 1$. Після цього на екран виводиться кількість симетричних матриць для системи ВКФ із заданими параметрами; з'являється можливість виведення на екран будь-якої з знайдених матриць.

Для виведення на екран знайденої матриці потрібно у відповідне поле ввести номер матриці і натиснути кнопку «Показать индикаторную матрицу». Після цього програма відкриє файл, створений після натискання кнопки «Синтезировать индикаторные матрицы», відрахує в ньому потрібну кількість байт, що дорівнює введеному номером, зменшеному на одиницю та помноженого на $\frac{(n+1)n}{2}$, і вибере послідовність довжиною $\frac{(n+1)n}{2}$. Потім перетворює отриманий масив в матрицю, яку і відображує на екрані. Після цього можна ввести новий номер.

Висновок

Описана програма показала результати, які підтвердили результати, викладені в праці [3], як знайдені практично, так і розрахункові. Індикаторні матриці, знайдені програмою, можуть бути надалі використані для перетворень Фур'є в заданих базисах ВКФ. БПФ у різних базисах ВКФ, як зазначалося раніше, може бути використано для шифрування файлів. Ключем при подібному шифруванні може бути або індикаторна матриця базису ВКФ, або номер індикаторної матриці (якщо на стороні дешифратора відомі всі індикаторні матриці для системи ВКФ із заданими параметрами).

ЛІТЕРАТУРА

1. *Бабак В. П.* Сигналы и спектры: учебн. 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 інтервалах / А. М. Трахтман, В. А. Трахтман. — М. : Сов. радио, 1975. — 208 с.

3. *Белецкий А.Я.* Преобразования Грея: монография. — В 2-х т. — Т. 2. Прикладные аспекты / А. Я. Белецкий, А. А. Белецкий, Е. А. Белецкий. — К. : Книжкове вид-во НАУ, 2007. — 644 с.

Стаття надійшла до редакції 14.09.10.