МЕТОД СИНТЕЗУ ЧЕТВІРКОВИХ БЕНТ-КВАДРАТІВ АГІЄВИЧА

К. т. н. А. В. Соколов, В. В. Авєкін, В. Г. Жук

Одеський національний політехнічний університет
Україна, м. Одеса
radiosquid@gmail.com

Запропоновано метод синтезу четвіркових бент-квадратів Агієвича за допомогою регулярного оператора т-зсуву та класифікації повної множини спектральних векторів Віленкіна–Крестенсона. Проведені дослідження є основою для побудови регулярних методів синтезу повної множини четвіркових бент-послідовностей, застосовуваних в криптографічних алгоритмах та технології кодового розділення каналів MC-CDMA.

Ключові слова: бент-квадрат Агієвича, перетворення Віленкіна–Крестенсона, т-зсув.

Бент-послідовності є важливим об'єктом сучасної криптографії. Так, вони знайшли свої численні застосування для синтезу генераторів псевдовипадкових ключових послідовностей, нелінійних *S*-блоків підстановки, матриць ортогональних перетворень, нелінійних коректувальних кодів. Іншим практичним застосуванням бент-послідовностей є побудова *C*-кодів постійної амплітуди, що використовуються для зниження величини пік-фактора в системах зв'язку з кодовим ущільненням каналів MC-CDMA.

Теорія синтезу двійкових бент-послідовностей є складною і багатогранною, незважаючи на те, що головне її завдання — синтез повних класів двійкових бент-послідовностей довільної довжини, все ще не вирішене. Останнім часом у зв’язку з розширенням використання принципів багатозначної логіки в сучасній криптографії та телекомунікаціях увага дослідників все більше і більше зосереджується на створенні методів синтезу бент-функцій багатозначної логіки. Так, наприклад, в [1] запропоновано метод синтезу трійкових бент-функцій на основі трійкових бент-квадратів Агієвича. Проте, тризначна логіка мало поширена на практиці, тоді як застосування четвіркової логіки є простим і ефективним на двійкових платформах.

В даній роботі розроблено метод синтезу четвіркових бент-квадратів Агієвича порядку $N = 4^k$, $k \in \mathbb{N}$.

Наведемо приклад роботи запропонованого методу для синтезу бент-квадратів четвертого порядку, але він може бути легко узагальнений на випадок довільного порядку.

Дію методу розглянемо у вигляді кроків, які будемо супроводжувати конкретним прикладом.

Крок 1. Розглянемо множину четвіркових послідовностей довжиною $N = 4$ над алфавітом, $\{1, j, -1, -j\}$, яких існує, відповідно $J = 4^4 = 256$.

Крок 2. Для кожної з даних послідовностей знайдемо четвіркове перетворення Віленкіна–Крестенсона, що будується відповідно до рекурентної формули

$$V_{4^{k+1}} = \begin{bmatrix} V_{4^k} & V_{4^k} & V_{4^k} & V_{4^k} \\ V_{4^k} & V_{4^k}+3 & V_{4^k}+2 & V_{4^k}+1 \\ V_{4^k} & V_{4^k}+2 & V_{4^k} & V_{4^k}+2 \\ V_{4^k} & V_{4^k}+1 & V_{4^k}+2 & V_{4^k}+3 \end{bmatrix}, \; V_1 = 0 . \qquad (1)$$

де «+» — операція додавання mod4, а матриці V представлені у символічній формі, тобто відповідають однозначному перетворенню алфавіту

$$A = \{e^{j(2\pi/4)\cdot 0} \quad e^{j(2\pi/4)\cdot 1} \quad e^{j(2\pi/4)\cdot 2} \; e^{j(2\pi/4\cdot)3}\} \leftrightarrow \{e^{j0^\circ} \quad e^{j90^\circ} \quad e^{j180^\circ} \; e^{j270^\circ}\} \leftrightarrow \{0,1,2,3\} . \qquad (2)$$

Крок 3. Проведемо спектральну класифікацію отриманої множини векторів у відповідності з методикою [2] — на основі набору їх абсолютних значень. В результаті для четвіркових послідовностей довжиною $N = 4$ отримуємо 5 спектральних класів, представлених в таблиці.

Спектральні класи векторів довжини $N = 4$

№	Набір абсолютних значень спектральних векторів	Потужність класу	Приклад вектора	Примітка
1	$\{4(1), 0(3)\}$	16	$\{4\ \ 0\ \ 0\ \ 0\}$	Афінні функції
2	$\{\sqrt{8}(2), 0(2)\}$	16	$\{0\ \ \sqrt{8}e^{j\pi/4}\ \ 0\ \ \sqrt{8}e^{-j\pi/4}\}$	—
3	$\{\sqrt{8}(1), 2(2), 0(1)\}$	64	$\{\sqrt{8}e^{j\pi/4}\ \ 2\ \ 0\ \ 2e^{-j\pi/2}\}$	—
4	$\{\sqrt{10}(1), \sqrt{2}(3)\}$	128	$\left\{\sqrt{10}e^{jarctg(1/3)}\ \ \sqrt{2}e^{j\pi/4}\ \ \sqrt{2}e^{-j\pi/4}\ \ \sqrt{2}e^{-j3\pi/4}\right\}$	—
5	$\{2(4)\}$	32	$\left\{2e^{j\pi}\ \ 2\ \ 2\ \ 2\right\}$	Бент-функції

Крок 4. До кожного вектора-представника застосовується оператор *m*-зсуву, де $m = 4$, в результаті чого отримуємо повну множину базових четвіркових бент-квадратів Агієвича.

Визначення [3]. Оператором *m*-зсуву числа *a* на величину *b* називається порозрядне складання чисел a і b, що представлені у *m*-ковій системі числення за модулем *m*.

Наприклад, оператор четвіркового зсуву буде мати вигляд наступної матриці (яка для випадку порядку $N = 4$ вироджується в матрицю з циклічним зсувом строк):

$$F_4 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{bmatrix} \tag{3}$$

Крок 5. Застосовуючи оператор четвіркового зсуву до векторів-представників, які отримані на *Кроці 3*, будуємо базові четвіркові бент-квадрати Агієвича для кожного спектрального класу:

$$BS_1 = \begin{bmatrix} 4&0&0&0 \\ 0&0&0&4 \\ 0&0&4&0 \\ 0&4&0&0 \end{bmatrix};\ BS_2 = \begin{bmatrix} 0 & \sqrt{8}e^{j\pi/4} & 0 & \sqrt{8}e^{-j\pi/4} \\ \sqrt{8}e^{j\pi/4} & 0 & \sqrt{8}e^{-j\pi/4} & 0 \\ 0 & \sqrt{8}e^{-j\pi/4} & 0 & \sqrt{8}e^{j\pi/4} \\ \sqrt{8}e^{-j\pi/4} & 0 & \sqrt{8}e^{j\pi/4} & 0 \end{bmatrix};\ BS_3 = \begin{bmatrix} \sqrt{8}e^{j\pi/4} & 2 & 0 & 2e^{-j\pi/2} \\ 2 & 0 & 2e^{-j\pi/2} & \sqrt{8}e^{j\pi/4} \\ 0 & 2e^{-j\pi/2} & \sqrt{8}e^{j\pi/4} & 2 \\ 2e^{-j\pi/2} & \sqrt{8}e^{j\pi/4} & 2 & 0 \end{bmatrix};$$

$$BS_4 = \begin{bmatrix} \sqrt{10}e^{jarctg(1/3)} & \sqrt{2}e^{j\pi/4} & \sqrt{2}e^{-j\pi/4} & \sqrt{2}e^{-j3\pi/4} \\ \sqrt{2}e^{j\pi/4} & \sqrt{2}e^{-j\pi/4} & \sqrt{2}e^{-j3\pi/4} & \sqrt{10}e^{jarctg(1/3)} \\ \sqrt{2}e^{-j\pi/4} & \sqrt{2}e^{-j3\pi/4} & \sqrt{10}e^{jarctg(1/3)} & \sqrt{2}e^{j\pi/4} \\ \sqrt{2}e^{-j3\pi/4} & \sqrt{10}e^{jarctg(1/3)} & \sqrt{2}e^{j\pi/4} & \sqrt{2}e^{-j\pi/4} \end{bmatrix};\ BS_5 = \begin{bmatrix} 2e^{j\pi} & 2 & 2 & 2 \\ 2 & 2 & 2 & 2e^{j\pi} \\ 2 & 2 & 2e^{j\pi} & 2 \\ 2 & 2e^{j\pi} & 2 & 2 \end{bmatrix}. \tag{4}$$

Кожен з представлених четвіркових бент-квадратів (4) відповідає бент-послідовності у часовій області. Базові бент-квадрати є основою для побудови регулярних методів синтезу повної множини четвіркових бент-послідовностей, застосовуваних для побудови генераторів псевдовипадкових послідовностей, ортогональних перетворень для алгоритмів стиску, кодів постійної амплітуди для технології MC-CDMA, а також *S*-блоків підстановки.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Sokolov, A.V. Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties // Journ. of Telecom., Electrnic and Comp. Eng.— Vol. 8.— N 9.— P. 39—43.

2. Мазурков М.И., Соколов А.В., Барабанов Н.А. Метод синтеза бент-последовательностей в базисе Виленкина-Крестенсона // Изв. ВУЗов. Радиоэлектроника. — 2016. — Т. 59, № 11. — С. 47—55.

3. Трахтман А.М., Трахтман В.А. Основы теории дискретных сигналов на конечных интервалах.— Рипол Классик, 1975.

A. V. Sokolov, V. V. Avekin, V. G. Zhuk

Synthesis method of quaternary Agievich bent-squares

We propose a synthesis method of quaternary Agievich bent-squares based on regular operator of m-shift and the classification of complete set of Vilenkin-Chrestenson spectral vectors. The performed research is the basis for further construction of regular synthesis methods of complete sets of quaternary bent-sequences which are widely used in cryptographic algorithms and MC-CDMA technology.

Keywords: Agievich bent-square, Vilenkin-Chrestenson transform, m-shift.