ПОСТРОЕНИЕ ТРОИЧНЫХ БЕНТ-ПОСЛЕДОВАТЕЛЬНОСТЕЙ

к.т.н. [1]Соколов А.В., к.ф.-м.н. [2]Жданов О.Н., инж. [1]Барабанов Н.А.
[1]Одесский национальный политехнический университет
[2]Сибирский государственный аэрокосмический университет
(Одесский национальный политехнический университет,
Украина, Одесса, 65044, пр. Шевченко 1, тел. +38 (050) 492 32 57,
e-mail: radiosquid@gmail.com)

In this paper we consider the question of constructing of ternary sequences of length $N=9$, having a uniform absolute values of Vilenkin-Christenson spectrum coefficients, by analogy with binary bent sequences with uniform absolute values of Walsh-Hadamard spectrum coefficients. Found $J=486$ highly nonlinear perfect algebraic structures can be used in the construction of generators of pseudorandom key sequences, cryptographic S-boxes, as well as in telecommunication systems using code division multiple access principle (CDMA).

Хорошо известны применения бент-последовательностей в современной криптографии и системах передачи информации, например, в технологии CDMA. Эффективность бент-последовательностей обусловлена их большой нелинейностью и равномерностью спектра Уолша-Адамара. Высокая практическая ценность данных классов последовательностей, а также внедрение m-ичных систем передачи и обработки информации диктует необходимость дальнейшего поиска последовательностей, обладающих подобными свойствами над другими алфавитами.

Рассмотрим алфавит $\{0,1,2\}$ и векторы длины $N=3^k=3^2=9$ над данным алфавитом, каждый вектор можно трактовать как функцию трехзначной логики (для краткости далее 3-функция). В данном множестве 3-функций линейные функции могут быть определены как

$$\varphi'(x_0,\ldots,x_{k-1})=a_0x_0+a_1x_1+\ldots+a_{k-1}x_{k-1}(\mathrm{mod}\,3)=\sum_{i=0}^{k-1}a_ix_i(\mathrm{mod}\,3), \qquad (1)$$

Для двоичных сигналов известно однозначное отображение между двоичным и бинарным кодом как $0\to"+",1\to"-"$. Определим подобное отображение для исследуемых троичных последовательностей как [1]

$$0\to e^{j0^\circ},1\to e^{j120^\circ},2\to e^{j240^\circ}. \qquad (2)$$

По аналогии с двоичным случаем бент-последовательность определим как троичную последовательность $\mathbf{B}$ длины $N=3^k$, обладающую равномерным по модулю спектром Виленкина-Крестенсона [1]

$$\mathbf{S}(\omega)=\mathbf{BW},\ \omega=\overline{0,N-1}, \qquad (3)$$

где, $\mathbf{W}$ — модификация ортогонального преобразования Виленкина-Крестенсона, полученная путем применения преобразования (2) к множеству линейных функций (1):

$$\mathbf{W}=\begin{bmatrix} e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} \\ e^{j0^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j0^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j0^\circ} & e^{j120^\circ} & e^{j240^\circ} \\ e^{j0^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j0^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j0^\circ} & e^{j240^\circ} & e^{j120^\circ} \\ e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j120^\circ} & e^{j120^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j240^\circ} & e^{j240^\circ} \\ e^{j0^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j0^\circ} & e^{j240^\circ} & e^{j0^\circ} & e^{j120^\circ} \\ e^{j0^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j120^\circ} & e^{j0^\circ} & e^{j240^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j0^\circ} \\ e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j240^\circ} & e^{j240^\circ} & e^{j0^\circ} & e^{j120^\circ} & e^{j120^\circ} & e^{j120^\circ} \\ e^{j0^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j240^\circ} & e^{j0^\circ} & e^{j120^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j0^\circ} \\ e^{j0^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j0^\circ} & e^{j120^\circ} & e^{j0^\circ} & e^{j240^\circ} \end{bmatrix}. \quad (4)$$

Проведенные экспериментальные исследования позволили установить: в полном множестве последовательностей длины $N=9$ существует точно $J=486$ последовательностей, обладающих равномерным по модулю спектром (3), т.е. $|\mathbf{S}(\omega)|=const$.

Пример. Рассмотрим последовательность

$$\mathbf{B}=\left\{e^{j0^\circ}\ e^{j120^\circ}\ e^{j0^\circ}\ e^{j240^\circ}\ e^{j240^\circ}\ e^{j0^\circ}\ e^{j0^\circ}\ e^{j240^\circ}\ e^{j240^\circ}\right\}, \quad (5)$$

для которой в соответствии с (3) может быть найдено преобразование Виленкина-Крестенсона

$$\mathbf{S}(\omega)=\left\{3e^{-j60^\circ}\ 3e^{-j60^\circ}\ 3e^{j60^\circ}\ 3e^{j60^\circ}\ 3e^{-j60^\circ}\ 3e^{-j60^\circ}\ 3e^{j60^\circ}\ 3e^{j180^\circ}\ 3e^{j60^\circ}\right\}, \quad (6)$$

и выполняется условие $|S(\omega)|=const$, (5) является бент-последовательностью.

Исследования весовых структур найденного множества бент-последовательностей привели к результату: в полном множестве троичных бент-последовательностей существуют два тройственных набора по аналогии с дуальными парами двоичных бент-последовательностей [2]

$$\begin{bmatrix} \{1,4,4\}(54); \\ \{4,1,4\}(54); \\ \{4,4,1\}(54); \end{bmatrix} \quad \begin{bmatrix} \{5,2,2\}(108); \\ \{2,5,2\}(108); \\ \{2,2,5\}(108), \end{bmatrix} \quad (7)$$

(в круглых скобках указаны количества бент-последовательностей, обладающих указанной весовой структурой).

Таким образом, в работе введено понятие троичной бент-последовательности, найден полный класс таких последовательностей длины $N=9$, обладающих равномерным по модулю спектром Виленкина-Крестенсона. Построенные конструкции могут быть использованы для генерации псевдослучайных ключевых последовательностей, криптографических *S*-блоков подстановки, а также в системах передачи информации, использующих принцип кодового разделения каналов (CDMA).

Библиографический список

1. Трахтман, А.М. Основы теории дискретных сигналов на конечных интервалах / А.М. Трахтман, В.А. Трахтман. — М.: «Сов. радио», 1975. — 208 с.

2. Мазурков, М.И. Генератор ключевых последовательностей на основе дуальных пар бент-функций / М.И. Мазурков, Н.А. Барабанов, А.В. Соколов. — Труды ОПУ, 2013. — Вып. 3 (42). — С. 150—156.