УДК 510.644

[1]О. Н. ЖДАНОВ, [2]А. В. СОКОЛОВ

МЕТОД СИНТЕЗА БАЗОВЫХ ТРОИЧНЫХ БЕНТ-КВАДРАТОВ НА ОСНОВЕ ОПЕРАТОРА ТРИАДНОГО СДВИГА

[1]Сибирский государственный аэрокосмический университет им. академика М. Ф. Решетнева
[2]Одесский национальный политехнический университет

Применение совершенных алгебраических конструкций в современных системах передачи информации, основанных на технологии кодового разделения каналов MC-CDMA (Multi Code Code Division Multiple Access), а также в криптографии, диктует необходимость их дальнейшего исследования. Одними из наиболее часто используемых совершенных алгебраических конструкций являются двоичные бент-функции, обладающие равномерным спектром амплитуд Уолша-Адамара и, соответственно, максимально удаленные от кодовых слов аффинного кода. Помимо двоичных бент-функций в настоящее время особое внимание уделяется разработке методов синтеза их многозначных аналогов. В частности, одним из эффективных методов синтеза многозначных бент-функций признан метод, основанный на бент-квадратах Агиевича. В настоящей статье разработан регулярный метод синтеза троичных бент-квадратов на основе произвольного спектрального вектора и регулярного оператора триадного сдвига. Проведена классификация спектральных векторов длин $N = 3$ и $N = 9$. На основе проведенной классификации уточнено определение многозначной бент-последовательности с учетом феномена существования многозначных бент-последовательностей для длин, определяющихся нечетной степенью основания. Полученные в статье результаты являются ценными для практического применения: разработки новых кодов постоянной амплитуды для технологии MC-CDMA, криптографических примитивов, алгоритмов сжатия информации, сигнальных конструкций, алгоритмов блочного и поточного шифрования, основанных на перспективных принципах многозначной логики. Разработанный метод синтеза бент-квадратов Агиевича также является базой для дальнейших теоретических исследований: разработки методов перестановок строк и столбцов базовых бент-квадратов, синтеза составных бент-квадратов. Кроме того, полученные данные о спектральной классификации векторов органично ставят задачу синтеза бент-функций длин $N = 3^{2k+1}$, $k \in \mathbb{N}$.

Ключевые слова: *бент-функции, многозначная логика, бент-квадрат Агиевича.*

Введение

Применение совершенных алгебраических конструкций получает все большее распространение в современных системах передачи и обработки информации. Данное обстоятельство обуславливает внимание исследователей к разработке методов синтеза и изучению свойств классов совершенных двоичных решеток, конструкций полей Галуа, последовательностей де Бре йна, бент-последовательностей. Последние обладают большой практической ценностью ввиду их использования в криптографии для построения *S*-блоков подстановки, а также в технологии кодового разделения каналов MC-CDMA (Multi-Code Code Division Multiple Access) для конструирования кодов постоянной амплитуды (С-кодов), снижающих пик-фактор передаваемых в системе сигналов [1].

Еще одной тенденцией в построении новейших систем передачи информации является переход к использованию принципов многозначной логики с целью повышения помехоустойчивости [2]. Данное обстоятельство диктует необходимость разработки новых методов синтеза многозначных бент-последовательностей, в частности, троичных бент-последовательностей, описанных в [3]. Тем не менее, практика показывает [4], что задача описания классов бент-последовательностей является сложной и многогранной, требует разработки новых видов представления данных структур. Одним из значительных достижений в теории синтеза двоичных бент-последовательностей стали бент-квадраты Агиевича [5, 6], позволившие провести классификацию полного множества бент-функций в соответствии с видом спектра Уолша-Ада-

мара их сегментов. Описание бент-последовательностей с помощью бент-квадратов Агиевича в настоящее время переросло в целое направление теории бент-последовательностей, в частности, разработаны методы их синтеза и размножения [7]. В связи с актуальностью и практической ценностью вопросов исследования многозначных совершенных алгебраических конструкций особый интерес представляет разработка метода синтеза троичных бент-квадратов Агиевича произвольного порядка $\sqrt{N}$.

Целью настоящей статьи является разработка метода синтеза троичных бент-квадратов Агиевича на основе регулярного оператора триадного сдвига.

Рассмотрим множество корней третьей степени из единицы

$$z_k = e^{j\frac{2\pi}{3}k}, \quad k \in \{0, 1, 2\}, \tag{1}$$

тогда алфавит рассматриваемых векторов будет состоять из следующих значений

$$z_0 = e^{j\frac{2\pi}{3}0} = 1; \quad z_1 = e^{j\frac{2\pi}{3}}; \quad z_2 = e^{j\frac{4\pi}{3}} = z_1^{\,2}. \tag{2}$$

Рассмотрим матрицу Виленкина-Крестенсона третьего порядка:

$$V_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & z_1 & z_2 \\ 1 & z_2 & z_1 \end{pmatrix}. \tag{3}$$

Построение матриц Виленкина-Крестенсона порядков 3^L, $L \in \mathbb{N}$ может быть выполнено на основе следующего рекуррентного правила

$$V_{3^L} = \begin{bmatrix} V_{3^{L-1}} & V_{3^{L-1}} & V_{3^{L-1}} \\ V_{3^{L-1}} & \left(V_{3^{L-1}}+1\right)\bmod 3 & \left(V_{3^{L-1}}+2\right)\bmod 3 \\ V_{3^{L-1}} & \left(V_{3^{L-1}}+2\right)\bmod 3 & \left(V_{3^{L-1}}+1\right)\bmod 3 \end{bmatrix}, \tag{4}$$

где $\left(V_{3^{L-1}}+1\right)\bmod 3$ – матрица, у которой индексы всех элементов увеличены на 1 по модулю 3.

Например, матрица V_9 будет иметь следующий вид

$$V_9 = \left[\begin{array}{ccc:ccc:ccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & z_1 & z_2 & 1 & z_1 & z_2 & 1 & z_1 & z_2 \\ 1 & z_2 & z_1 & 1 & z_2 & z_1 & 1 & z_2 & z_1 \\ \hdashline 1 & 1 & 1 & z_1 & z_1 & z_1 & z_2 & z_2 & z_2 \\ 1 & z_1 & z_2 & z_1 & z_2 & 1 & z_2 & 1 & z_1 \\ 1 & z_2 & z_1 & z_1 & 1 & z_2 & z_2 & z_1 & 1 \\ \hdashline 1 & 1 & 1 & z_2 & z_2 & z_2 & z_1 & z_1 & z_1 \\ 1 & z_1 & z_2 & z_2 & 1 & z_1 & z_1 & z_2 & 1 \\ 1 & z_2 & z_1 & z_2 & z_1 & 1 & z_1 & 1 & z_2 \end{array}\right] \tag{5}$$

1. Спектральная классификация последовательностей длины $N = 3$

Рассмотрим сначала последовательности длины $N = 3$. Каждый вектор из данного множества может быть представлен в виде

$$A = \{a_1 \quad a_2 \quad a_3\}, \quad a_i = z_k = e^{j\frac{2\pi}{3}k}, \quad k \in \{0,1,2\}. \tag{6}$$

Для данного вектора определено преобразование Виленкина-Крестенсона как новый вектор $S = A \cdot \overline{V_3}$, где $\overline{V_3}$ – матрица из элементов, комплексно сопряженных к элементам матрицы V_3, вектор S имеет вид

$$S = \{s_1 \quad s_2 \quad s_3\}, \; s_i \in \mathbb{Z}. \tag{7}$$

Для каждого вектора A однозначно определен вектор S. Заметим, что обратное неверно, т. е. не для каждого вектора S, $s_i \in \mathbb{Z}$ существует соответствующий ему вектор с координатами $a_i \in \{1, z_1, z_2\}$, такой что справедливо равенство $S = A \cdot V_3$.

Определение 1 [3]. Троичная последовательность $H = [h_0, h_1, \cdots, h_i, \cdots, h_{N-1}]$ длины $N = 3^{2m}$, $m \in \mathbb{N}$, где коэффициенты $h_i \in \pm 1\{1, z_1, z_2\}$, называется бент-последовательностью в базисе Виленкина-Крестенсона, если она имеет равномерный по модулю спектр Виленкина-Крестенсона, который представим в матричной форме

$$\left|\Omega_B(\omega)\right| = \left|H \cdot \overline{V}_N\right| = const, \quad \omega = \overline{0, N-1}, \tag{8}$$

где V_N – матрица Виленкина-Крестенсона порядка N.

В общем случае, задача поиска бент-функций является задачей поиска последовательностей, обладающих заданными спектральными свойствами, что требует детального изучения области допустимых значений $s_i \in \mathbb{Z}$, для которых существуют векторы A во временной области, т.е. проведение спектральной классификации полного множества векторов длины $N = 3$.

Спектральную классификацию векторов $\{a_i\}$ длины $N = 9$ будем проводить в соответствии с подходом [8], основанным на наборах абсолютных значений спектральных векторов.

Определение 2. Элементарной структурой спектрального вектора S назовем набор абсолютных значений его спектральных компонент.

Выясним, какие значения могут принимать элементы s_i. Рассмотрим, например, первый

спектральный коэффициент s_1, который является результатом произведения последовательности A на первый столбец матрицы преобразования Виленкина-Крестенсона. Элементы последовательности A принадлежат алфавиту $\{z_0, z_1, z_2\}$, который представим в алгебраической форме

$$z_0 = 1,\ z_1 = -0{,}5 + j\frac{\sqrt{3}}{2},\ z_2 = -0{,}5 - j\frac{\sqrt{3}}{2}. \quad (9)$$

Обозначим через α_0, α_1, α_2 количество элементов z_0, z_1, z_2 в последовательности A соответственно. Тогда коэффициент s_1 будет принимать значение

$$s_1 = \left[\alpha_0 + (\alpha_1 + \alpha_2)(-0{,}5)\right] + j\left[\alpha_1\frac{\sqrt{3}}{2} + a_2\left(-\frac{\sqrt{3}}{2}\right)\right], \quad (10)$$

причем

$$\begin{cases} \alpha_0 + \alpha_1 + \alpha_2 = 3, \\ \alpha_0, \alpha_1, \alpha_2 \in \{0,1,2,3\}. \end{cases} \quad (11)$$

Полное рассмотрение всех возможных вариантов показало: существует всего 10 троек чисел α_0, α_1, α_2, удовлетворяющих условию (11)

$$\begin{bmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \alpha_0 & \alpha_1 & \alpha_2 \\ 0 & 0 & 3 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 & 2 & 0 \\ 0 & 2 & 1 & 2 & 0 & 1 \\ 0 & 3 & 0 & 2 & 1 & 0 \\ 1 & 0 & 2 & 3 & 0 & 0 \end{bmatrix}. \quad (12)$$

Для нахождения возможных значений модуля коэффициента s_1 подставим решения (12) в (10), после чего, находя модуль комплексного числа, получим:

$$|s_1| = \sqrt{\left[\alpha_0 + (\alpha_1 + \alpha_2)(-0{,}5)\right]^2 + \left[\alpha_1\frac{\sqrt{3}}{2} + a_2\left(-\frac{\sqrt{3}}{2}\right)\right]^2} \in \{0, \sqrt{3}, 3\}. \quad (13)$$

Утверждение. Множество значений (13), и только они, являются возможными значениями всех модулей коэффициентов преобразования Виленкина-Крестенсона векторов длины $N = 3$.

Действительно, выразим значения первого коэффициента преобразования Виленкина-Крестенсона через элементы исходной последовательности

$$s_1 = [a_1\ a_2\ a_3][\overline{z_0}\ \overline{z_0}\ \overline{z_0}]^T = [a_1\ a_2\ a_3][1\ 1\ 1]^T = a_1 + a_2 + a_3,\quad a_i \in \{1, z_1, z_2\}. \quad (14)$$

Аналогично, рассмотрим i-й коэффициент преобразования Виленкина-Крестенсона

$$s_i = [a_1\ a_2\ a_3][\overline{z_0}\ \overline{z_0}\ \overline{z_0}]^T = \left[e^{j\beta_1}\ e^{j\beta_2}\ e^{j\beta_3}\right]\left[e^{j\gamma_1}\ e^{j\gamma_2}\ e^{j\gamma_3}\right]^T = \left[e^{j(\beta_1+\gamma_1)}\ e^{j(\beta_2+\gamma_2)}\ e^{j(\beta_3+\gamma_3)}\right]. \quad (15)$$

Так как $в_i, г_i \in \{1, z_1, z_2\}$, то для каждого s_i существует последовательность $A' = [a_1'\ a_2'\ a_3']$, преобразование Виленкина-Крестенсона которой имеет коэффициент s_1, равный заданному s_i.

Проведенные вычисления показывают, что для векторов длины $N = 9$ существуют десять спектральных классов векторов (табл. 1). В табл. 1 для краткости приняты следующие обозначения: {9(1), 0(8)}. Смысл обозначений данного примера следующий: элемент 9 встречается один раз, элемент 0 повторяется восемь раз.

Таблица 1. **Классы векторов длины $N = 3$**

№	Спектральный класс в виде иррациональностей	Мощность класса	Последовательность-представитель
1	{3(1), 0(2)}	9	{0 0 0}
2	{$\sqrt{3}$(3)}	18	{0 0 1}

Анализ данных табл. 1 показывает, что существует всего 18 последовательностей длины $N = 3^1 = 3$, обладающих равномерным по модулю спектром Виленкина-Крестенсона. Данное обстоятельство позволяет обобщить определение бент-последовательности для многозначного случая.

Определение 3. Для матрицы Виленкина-Крестенсона порядка $N = p^k$, p – простое число, $k \in \mathbb{N}$ бент-последовательностью называется последовательность $H = [h_0, h_1, \cdots, h_i, \cdots, h_{N-1}]$ над алфавитом

$$h_i \in \left\{ e^{j\frac{2\pi}{m}\nu} \right\},\ \nu = 0, 1, ..., m-1,$$

если она имеет равномерный по модулю спектр Виленкина-Крестенсона, который представим в матричной форме

$$\left|\Omega_B(\omega)\right| = \left|H \cdot \overline{V}_N\right| = const,\quad \omega = \overline{0, N-1}, \quad (16)$$

где V_N – матрица Виленкина-Крестенсона порядка N над алфавитом

$$h_i \in \left\{ e^{j\frac{2\pi}{m}\nu} \right\},\ \nu = 0,\ 1,\ ...,\ m-1.$$

Актуальной является задача описания множества значений m, для которых существуют бент-последовательности.

2. Спектральная классификация последовательностей длины $N = 9$

Рассмотрим полное множество троичных векторов длины $N = 9$. Каждый вектор из данного множества может быть представлен в общем виде

$$A = \{a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8\ a_9\},\ a_i \in \{1, z_1, z_2\}. \quad (17)$$

Аналогично случаю $N = 3$, определяем преобразование Виленкина-Крестенсона как вектор $S = A \cdot \overline{V}$, где S имеет координаты

$$S = \{s_1\ \ s_2\ \ s_3\ \ s_4\ \ s_5\ \ s_6\ \ s_7\ \ s_8\ \ s_9\},\ s_i \in \mathbb{Z}, \quad (18)$$

а V – матрица Виленкина-Крестенсона порядка $N = 9$.

Обозначим через α_0, α_1, α_2 число элементов 1, z_1, z_2 в последовательности A, соответственно. Тогда коэффициент s_1 будет принимать значение

$$s_1 = \left[\alpha_0 + (\alpha_1 + \alpha_2)(-0{,}5)\right] + j\left[\alpha_1\frac{\sqrt{3}}{2} + a_2\left(-\frac{\sqrt{3}}{2}\right)\right], \quad (19)$$

причем

$$\begin{cases} \alpha_0 + \alpha_1 + \alpha_2 = 9, \\ \alpha_0, \alpha_1, \alpha_2 \in \{0, 1, 2, ..., 9\}. \end{cases} \quad (20)$$

Полное рассмотрение всех вариантов показало: существует всего 55 троек чисел α_0, α_1, α_2, удовлетворяющих условию (20)

$\alpha_0\alpha_1\alpha_2$	$\alpha_0\alpha_1\alpha_2$	$\alpha_0\alpha_1\alpha_2$	$\alpha_0\alpha_1\alpha_2$	$\alpha_0\alpha_1\alpha_2$
0 0 9	1 1 7	2 3 4	3 6 0	5 4 0
0 1 8	1 2 6	2 4 3	4 0 5	6 0 3
0 2 7	1 3 5	2 5 2	4 1 4	6 1 2
0 3 6	1 4 4	2 6 1	4 2 3	6 2 1
0 4 5	1 5 3	2 7 0	4 3 2	6 3 0
0 5 4	1 6 2	3 0 6	4 4 1	7 0 2
0 6 3	1 7 1	3 1 5	4 5 0	7 1 1
0 7 2	1 8 0	3 2 4	5 0 4	7 2 0
0 8 1	2 0 7	3 3 3	5 1 3	8 0 1
0 9 0	2 1 6	3 4 2	5 2 2	8 1 0
1 0 8	2 2 5	3 5 1	5 3 1	9 0 0

(21)

Для нахождения возможных значений модуля коэффициента s_1 подставим решения (21) в (19), после чего воспользуемся формулой нахождения модуля комплексного числа

$$|s_1| = \sqrt{\left[\alpha_0 + (\alpha_1 + \alpha_2)(-0{,}5)\right]^2 + \left[\alpha_1\frac{\sqrt{3}}{2} + a_2\left(-\frac{\sqrt{3}}{2}\right)\right]^2} \in$$

$$\in \{0, \sqrt{3},\ 3, \sqrt{12}, \sqrt{21}, \sqrt{27}, 6,\ \sqrt{39}, \sqrt{57}, 9\}. \quad (22)$$

Поскольку умножение вектора A на любой другой столбец матрицы Виленкина-Крестенсона $V_{:,j}$, по сути, эквивалентно следующей записи $s_i = \left(A \cdot V_{:,j}\right) \cdot V_{:,1} = B \cdot V_{:,1}$, а последовательность $B = A \cdot V_{:,j}$ принадлежит линейному векторному пространству векторов длины над алфавитом $\{1, z_1, z_2\}$, то значения, полученные в (22), будут такими же для всех коэффициентов преобразования Виленкина-Крестенсона s_i, $i = 1, 2, \ldots, 9$.

Проведенные исследования показывают, что для векторов длины $N = 9$ существуют десять спектральных классов векторов (табл. 2).

Таблица 2. **Классы векторов длины $N = 9$**

№	Спектральный класс в виде иррациональностей	Мощность класса	Последовательность-представитель
1	{9(1), 0(8)}	27	{0 0 0 0 0 0 0 0 0}
2	$\{\sqrt{57}(1), \sqrt{3}(8)\}$	486	{0 0 0 0 0 0 0 0 1}
3	$\{\sqrt{39}(1), \sqrt{12}(2), \sqrt{3}(6)\}$	1944	{0 0 0 0 0 0 0 1 1}
4	{6(1), 3(5), 0(3)}	1944	{0 0 0 0 0 0 0 1 2}
5	$\{\sqrt{27}(3), 0(6)\}$	216	{0 0 0 0 0 0 1 1 1}
6	$\{\sqrt{27}(1), 3(6), 0(2)\}$	3888	{0 0 0 0 0 1 0 1 1}
7	$\{\sqrt{21}(3), \sqrt{3}(6)\}$	1944	{0 0 0 0 0 0 1 1 2}
8	$\{\sqrt{21}(2), \sqrt{12}(2), \sqrt{3}(5)\}$	5832	{0 0 0 0 0 1 0 1 2}
9	$\{\sqrt{21}(1), \sqrt{12}(4), \sqrt{3}(4)\}$	2916	{0 0 0 0 0 1 1 1 2}
10	{3(9)}	486	{0 0 0 0 1 2 0 2 1}
∑		19683	

3. Метод синтеза бент-квадратов на основе произвольного набора коэффициентов преобразования Виленкина-Крестенсона

Рассмотрим процесс формирования бент-квадратов порядка $N = 9$ на основе каждого из

приведенных классов спектральных векторов длины $N = 9$ с помощью регулярного оператора триадного сдвига.

Определение 2 [9]. Оператором m-сдвига числа a на величину b называется поразрядное сложение чисел a и b, представленных в m-ичной системе счисления по модулю m.

Хорошо известен оператор диадного сдвига [10], который используется для построения матриц ортогонального преобразования, а также бент-квадратов [7].

В нашем случае, для получения оператора триадного сдвига положим $m = 3$. Например, рассмотрим тривиальную монотонно возрастающую последовательность чисел от 0 до 8, каждый элемент которой представим в виде двухразрядного троичного числа

$$\begin{array}{cccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline 00 & 01 & 02 & 10 & 11 & 12 & 20 & 21 & 22 \end{array}. \qquad (23)$$

Последовательно проводем 3-сдвиг данной последовательности на величины от 00_3 до 22_3, представляя результат в виде последовательности десятичных чисел

сдвиг	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	0	4	5	3	7	8	6
2	2	0	1	5	3	4	8	6	7
3	3	4	5	6	7	8	0	1	2
4	4	5	3	7	8	6	1	2	0
5	5	3	4	8	6	7	2	0	1
6	6	7	8	0	1	2	3	4	5
7	7	8	6	1	2	0	4	5	3
8	8	6	7	2	0	1	5	3	4

(24)

Рассмотрим процесс построения бент-квадрата с помощью конкретных шагов, которые прокомментированы примером на основе последовательностей четвертого класса.

Шаг 1. Выберем временную троичную последовательность и её спектр Виленкина-Крестенсона

$$\begin{aligned} t_4 &= \{0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 2\}; \\ S_4 &= \{6\ 3\ 0\ 3e^{-\pi/3}\ \ 3e^{2\pi/3}\ \ 0\ 3e^{\pi/3}\ \ 3e^{-2\pi/3}\ \ 0\}. \end{aligned} \qquad (25)$$

Шаг 2. Применим к выбранной на Шаге 1 троичной последовательности оператор триадного сдвига (24).

В результате получаем бент-квадрат

$$BS_4 = \begin{bmatrix} 6 & 3 & 0 & 3e^{-\pi/3} & 3e^{2\pi/3} & 0 & 3e^{\pi/3} & 3e^{-2\pi/3} & 0 \\ 3 & 0 & 6 & 3e^{2\pi/3} & 0 & 3e^{-\pi/3} & 3e^{-2\pi/3} & 0 & 3e^{\pi/3} \\ 0 & 6 & 3 & 0 & 3e^{-\pi/3} & 3e^{2\pi/3} & 0 & 3e^{\pi/3} & 3e^{-2\pi/3} \\ 3e^{-\pi/3} & 3e^{2\pi/3} & 0 & 3e^{\pi/3} & 3e^{-2\pi/3} & 0 & 6 & 3 & 0 \\ 3e^{2\pi/3} & 0 & 3e^{-\pi/3} & 3e^{-2\pi/3} & 0 & 3e^{\pi/3} & 3 & 0 & 6 \\ 0 & 3e^{-\pi/3} & 3e^{2\pi/3} & 0 & 3e^{\pi/3} & 3e^{-2\pi/3} & 0 & 6 & 3 \\ 3e^{\pi/3} & 3e^{-2\pi/3} & 0 & 6 & 3 & 0 & 3e^{-\pi/3} & 3e^{2\pi/3} & 0 \\ 3e^{-2\pi/3} & 0 & 3e^{\pi/3} & 3 & 0 & 6 & 3e^{2\pi/3} & 0 & 3e^{-\pi/3} \\ 0 & 3e^{\pi/3} & 3e^{-2\pi/3} & 0 & 6 & 3 & 0 & 3e^{-\pi/3} & 3e^{2\pi/3} \end{bmatrix}. \qquad (26)$$

Шаг 3. Выполняя обратное преобразование каждой строки, получаем троичный бент-квадрат во временной области

$$BKT_4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 2 & 1 & 0 & 2 & 1 & 1 & 2 & 0 \\ 0 & 1 & 2 & 0 & 1 & 2 & 1 & 1 & 1 \\ 0 & 0 & 0 & 2 & 2 & 2 & 2 & 1 & 0 \\ 0 & 2 & 1 & 2 & 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 2 & 2 & 0 & 1 & 2 & 2 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 2 & 1 \\ 0 & 2 & 1 & 1 & 0 & 2 & 0 & 1 & 2 \\ 0 & 1 & 2 & 1 & 2 & 0 & 0 & 0 & 0 \end{bmatrix}. \qquad (27)$$

Шаг 4. Путем последовательной конкатенации строк временного бент-квадрата (27) получаем бент-функцию длины $N = 81$

$$\begin{aligned} B = \{&0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 2\ 0\ 2\ 1\ 0\ 2\ 1\ 1\ 2\ 0\ 0\ 1 \\ &2\ 0\ 1\ 2\ 1\ 1\ 1\ 0\ 0\ 0\ 2\ 2\ 2\ 2\ 1\ 0\ 0\ 2\ 1\ 2\ 1\ 0\ 2 \\ &0\ 1\ 0\ 1\ 2\ 2\ 0\ 1\ 2\ 2\ 2\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 2\ 1\ 0\ 2\ 1 \\ &1\ 0\ 2\ 0\ 1\ 2\ 0\ 1\ 2\ 1\ 2\ 0\ 0\ 0\ 0\}. \end{aligned} \qquad (28)$$

Отметим, что для получения троичного бент-квадрата на основе оператора триадного сдвига может быть использован любой троичный вектор длины $N = 9$, принадлежащий любому спектральному классу.

В отличие от двоичных бент-квадратов Агиевича, спектральное представление троичных бент-квадратов является весьма громоздким, поэтому для краткости приведем по одному представителю временных бент-квадратов для каждого класса (табл. 2)

$$BKT_1=\begin{bmatrix}0&0&0&0&0&0&0&0&0\\0&2&1&0&2&1&0&2&1\\0&1&2&0&1&2&0&1&2\\0&0&0&2&2&2&1&1&1\\0&2&1&2&1&0&1&0&2\\0&1&2&2&0&1&1&2&0\\0&0&0&1&1&1&2&2&2\\0&2&1&1&0&2&2&1&0\\0&1&2&1&2&0&2&0&1\end{bmatrix};\quad BKT_2=\begin{bmatrix}0&0&0&0&0&0&0&0&1\\0&2&1&0&2&1&0&2&2\\0&1&2&0&1&2&0&1&0\\0&0&0&2&2&2&1&1&2\\0&2&1&2&1&0&1&0&0\\0&1&2&2&0&1&1&2&1\\0&0&0&1&1&1&2&2&0\\0&2&1&1&0&2&2&1&1\\0&1&2&1&2&0&2&0&2\end{bmatrix};\quad BKT_3=\begin{bmatrix}0&0&0&0&0&0&0&1&1\\0&2&1&0&2&1&0&0&2\\0&1&2&0&1&2&0&2&0\\0&0&0&2&2&2&1&2&2\\0&2&1&2&1&0&1&1&0\\0&1&2&2&0&1&1&0&1\\0&0&0&1&1&1&2&0&0\\0&2&1&1&0&2&2&2&1\\0&1&2&1&2&0&2&1&2\end{bmatrix};$$

$$BKT_4=\begin{bmatrix}0&0&0&0&0&0&0&1&2\\0&2&1&0&2&1&0&0&0\\0&1&2&0&1&2&0&2&1\\0&0&0&2&2&2&1&2&0\\0&2&1&2&1&0&1&1&1\\0&1&2&2&0&1&1&0&2\\0&0&0&1&1&1&2&0&1\\0&2&1&1&0&2&2&2&2\\0&1&2&1&2&0&2&1&0\end{bmatrix};\quad BKT_5=\begin{bmatrix}0&0&0&0&0&0&1&1&1\\0&2&1&0&2&1&1&0&2\\0&1&2&0&1&2&1&2&0\\0&0&0&2&2&2&2&2&2\\0&2&1&2&1&0&2&1&0\\0&1&2&2&0&1&2&0&1\\0&0&0&1&1&1&0&0&0\\0&2&1&1&0&2&0&2&1\\0&1&2&1&2&0&0&1&2\end{bmatrix};\quad BKT_6=\begin{bmatrix}0&0&0&0&0&1&0&1&1\\0&2&1&0&2&2&0&0&2\\0&1&2&0&1&0&0&2&0\\0&0&0&2&2&0&1&2&2\\0&2&1&2&1&1&1&1&0\\0&1&2&2&0&2&1&0&1\\0&0&0&1&1&2&2&0&0\\0&2&1&1&0&0&2&2&1\\0&1&2&1&2&1&2&1&2\end{bmatrix};$$

$$BKT_7=\begin{bmatrix}0&0&0&0&0&0&1&1&2\\0&2&1&0&2&1&1&0&0\\0&1&2&0&1&2&1&2&1\\0&0&0&2&2&2&2&2&0\\0&2&1&2&1&0&2&1&1\\0&1&2&2&0&1&2&0&2\\0&0&0&1&1&1&0&0&1\\0&2&1&1&0&2&0&2&2\\0&1&2&1&2&0&0&1&0\end{bmatrix};\quad BKT_8=\begin{bmatrix}0&0&0&0&0&1&0&1&2\\0&2&1&0&2&2&0&0&0\\0&1&2&0&1&0&0&2&1\\0&0&0&2&2&0&1&2&0\\0&2&1&2&1&1&1&1&1\\0&1&2&2&0&2&1&0&2\\0&0&0&1&1&2&2&0&1\\0&2&1&1&0&0&2&2&2\\0&1&2&1&2&1&2&1&0\end{bmatrix};\quad BKT_9=\begin{bmatrix}0&0&0&0&0&1&1&1&2\\0&2&1&0&2&2&1&0&0\\0&1&2&0&1&0&1&2&1\\0&0&0&2&2&0&2&2&0\\0&2&1&2&1&1&2&1&1\\0&1&2&2&0&2&2&0&2\\0&0&0&1&1&2&0&0&1\\0&2&1&1&0&0&0&2&2\\0&1&2&1&2&1&0&1&0\end{bmatrix};\qquad(29)$$

$$BKT_{10}=\begin{bmatrix}0&0&0&0&1&2&0&2&1\\0&2&1&0&0&0&0&1&2\\0&1&2&0&2&1&0&0&0\\0&0&0&2&0&1&1&0&2\\0&2&1&2&2&2&1&2&0\\0&1&2&2&1&0&1&1&1\\0&0&0&1&2&0&2&1&0\\0&2&1&1&1&1&2&0&1\\0&1&2&1&0&2&2&2&2\end{bmatrix}.$$

Полученные бент-квадраты (29) являются основой для построения классов троичных бент-последовательностей длины $N = 81$, а также для конструирования троичных бент-квадратов большего порядка.

Выводы

1. В статье разработан регулярный метод синтеза троичных бент-квадратов произвольного порядка на основе оператора триадного сдвига. Данный метод позволил получить полное множество базовых бент-квадратов девятого порядка, которые являются основой для построения троичных бент-функций длины $N = 81$.

2. Проведена спектральная классификация полного троичного кода длин $N = 3$ и $N = 9$, в результате чего выделены 10 спектральных подклассов векторов длины $N = 9$, обладающих уникальной элементарной структурой. Спектральная классификация векторов длины $N = 3$ позволила установить, что существуют троичные последовательности длины $N = 3$, обладающие равномерным по модулю спектром Виленкина-Крестенсона.

3. Уточнено определение многозначной бент-последовательности, в котором учтен феномен существования многозначных бент-последовательностей длин $N = p^k$, где p –простое число, $k \in \mathbb{N}$.

Литература

1. **Paterson K. G.** Sequences For OFDM and Multi-code CDMA: two problems in algebraic coding theory // K. G. Paterson. – Sequences and their applications. Seta 2001. Second Int. Conference (Bergen, Norway, May 13–17, 2001). Proc. Berlin: Springer, 2002. – P. 46–71.

2. **Петелин, Ю. В.** Перспективы использования сигнально-кодовых конструкций типа троичных М-последовательностей в спутниковых каналах связи / Ю. В. Петелин, М. А. Ковалев, А. А. Макаров // Информационно-управляющие системы. – 2006. – №. 5. – С. 32–35.

3. **Соколов, А. В.** Построение троичных бент-последовательностей / А.В. Соколов, О.Н. Жданов, Н.А. Барабанов // Материалы XIX международного молодежного форума «Радиоэлектроника и молодежь в XXI веке», Харьков. – Т. 3. – С. 131–132.

4. **Соколов, А. В.** Генератор псевдослучайных ключевых последовательностей на основе тройственных наборов бент-функций / А.В. Соколов, О.Н. Жданов, Н.А. Барабанов. – Проблемы физики, математики и техники, 2016. – №1(26). – С. 85–91.

5. **Agievich S. V.** «On the representation of bent functions by bent rectangles». – Probabilistic Methods in Discrete Mathematics: Proceedings of the Fifth International Petrozavodsk Conference (Petrozavodsk, June 1–6, 2000). Utrecht, Boston: VSP, 2002, P. 121–135.

6. **Agievich, S. V.** «Bent Rectangles», Proceedings of the NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security (Moscow, September 8–18, 2007). Amsterdam: IOS Press. – 2008.– p. 3–22.

7. **Соколов, А. В.** Регулярный метод синтеза базовых бент-квадратов произвольного порядка / А. В. Соколов // Наука и техника. – 2016. – № 4. – С. 345 – 352.

8. **Соколов, А. В.** Алгоритм устранения спектральной эквивалентности компонентных булевых функций S-блоков конструкции Ниберг / А.В. Соколов, Н.А. Барабанов // Известия высших учебных заведений. Радиоэлектроника. – 2015. – Т. 58, N 5. – С. 41–49.

9. **Трахтман, А. М.** Основы теории дискретных сигналов на конечных интервалах / А. М. Трахтман, В. А. Трахтман. – М.: Советское радио, 1975. – 208 с.

10. **Мазурков, М. И.** Быстрые ортогональные преобразования на основе бент-последовательностей / М. И. Мазурков, А. В. Соколов // Інформатика та математичні методи в моделюванні. – Одеса, 2014. – № 1. – С.5–13.

References

1. **Paterson K. G.** Sequences For OFDM and Multi-code CDMA: two problems in algebraic coding theory // K. G. Paterson. – Sequences and their applications. Seta 2001. Second Int. Conference (Bergen, Norway, May 13–17, 2001). Proc. Berlin: Springer, 2002. – P. 46–71.

2. **Petelin, V.** The perspectives of usage of signal-code structures such as ternary M-sequences in the satellite communication channels / J. V. Petelin, M. A. Kovalev, A. A. Makarov // Information and Control Systems. – 2006. – №. 5. – P. 32–35.

3. **Sokolov, A. V.** Construction of ternary bent sequences / A. V. Sokolov, O. N. Zhdanov, N. A. Barabanov // Proceedings of the XIX International youth forum «Radioelectronics and youth in XXI century», Kharkiv. – V. 3. – P.131–132.

4. **Sokolov, A. V.** Pseudo-random key sequence generator based on triple sets of bent-functions / A. V. Sokolov, O. N. Zhdanov, N. A. Barabanov. – Problems of physics, mathematics and technology, 2016. – №1 (26). – P. 85–91.

5. **Agievich S. V.** «On the representation of bent functions by bent rectangles». – Probabilistic Methods in Discrete Mathematics: Proceedings of the Fifth International Petrozavodsk Conference (Petrozavodsk, June 1–6, 2000). Utrecht, Boston: VSP, 2002, P. 121–135.

6. **Agievich, S. V.** «Bent Rectangles», Proceedings of the NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security (Moscow, September 8–18, 2007) .Amsterdam: IOS Press. – 2008. – p. 3 – 22.

7. **Sokolov, A. V.** The regular synthesis method of bent-squares of any order / A.V. Sokolov // Science and Technology. – 2016. – № 4. – S. 345 – 352.

8. **Sokolov, A. V.** Algorithm for removing the spectral equivalence of component Boolean functions of Nyberg-design S-boxes / A. V. Sokolov, N. A. Barabanov // Proceedings of the higher educational institutions. Radioelectronics. – 2015. – T. 58, N 5. – P. 41–49.

9. **Trakhtman, A. M.** Fundamentals of the theory of discrete signals on finite intervals / A. M. Trakhtman, V. A. Trakhtman. – Moscow: Soviet Radio, 1975. – p. 208.

10. **Mazurkov, M. I.** Fast orthogonal transforms based on bent-sequences / M.I. Mazurkov, A. V. Sokolov // Informatics and mathematical methods in simulation. – Odesa, 2014. – №1. – P. 5–13.

Поступила	*После доработки*	*Принята к печати*
07.12.2016	*08.02.2017*	*06.03.2017*

Zhdanov O. N., Sokolov A. V.

A SYNTHESIS METHOD OF BASIC TERNARY BENT-SQUARES BASED ON THE TRIAD SHIFT OPERATOR

Practical application of advanced algebraic constructions in modern communication systems based on MC-CDMA (Multi Code Code Division Multiple Access) technology and in cryptography necessitates their further research. One of the most commonly used advanced algebraic construction is the binary bent-function having a uniform amplitude spectrum of the Walsh-Hadamard transform and, accordingly, having the maximal distance from the codewords of affine code. In addition to the binary bent-functions researchers are currently focuses on the development of synthesis methods of their many-valued analogues. In particular, one of the most effective methods for the synthesis of many-valued bent-functions is the method based on the Agievich bent-squares. In this paper, we developed a regular synthesis method of the ternary bent-squares on the basis of an arbitrary spectral vector and the regular operator of the triad shift. The classification of spectral vectors of lengths N = 3 and N = 9 is performed. On the basis of spectral classification more precise definition of many-valued bent-sequences is given, taking into account the existence of the phenomenon of many-valued bent-sequences for the length, determined by odd power of base. The paper results are valuable for practical use: the development of new constant amplitude codes for MC-CDMA technology, cryptographic primitives, data compression algorithms, signal structures, algorithms of block and stream encryption, based on advanced principles of many-valued logic. The developed bent-squares design method is also a basis for further theoretical research: development of methods of the permutation of rows and columns of basic bent-squares and their sign coding, synthesis of composite bent-squares. In addition, the data on the spectral classification of vectors give the task of constructing the synthesis methods of bent-functions of lengths $N = 3^{2k+1}$, $k \in \mathbb{N}$.

Keywords: *bent-functions, many-valued logic, Agievich bent-square.*

Жданов Олег Николаевич родился 16 апреля 1964 года. В 1986 году окончил Красноярский Государственный Университет. Кандидатская диссертация по специальности «математический анализ» защищена в 1994 году. В настоящее время доцент кафедры безопасности информационных технологий Сибирского Государственного Аэрокосмического университета.

Читаемые лекционные курсы: «Криптографические методы защиты информации» (имеется удостоверение Института Криптографии, Связи и Информатики о соответствующем повышении квалификации), «Теоретико-числовые алгоритмы криптографии», «Теория надежности».

Общее количество публикаций 73, из них 7 – учебные пособия (в соавторстве с учениками).

Сфера научных интересов: системы дифференциальных уравнений в частных производных, являющиеся моделями процессов в механике сплошных сред. Получены точные решения уравнений пластичности плоского напряженного состояния, предложен новый подход к исследованию смешанной задачи для системы уравнений плоского напряженного состояния среды Мизеса, построен алгоритм нахождения решения задачи Коши для системы уравнений, описывающей одномерный поток гранулированного материала.

Еще одной областью научных интересов является защита информации: разработка реализации алгоритмов шифрования данных при передаче по открытому каналу с привлечением к этой работе студентов старших курсов для выполнения ими курсового и дипломного проектирования. Совместно с учениками разработал методику выбора ключевой информации для реализации алгоритмов блочного шифрования. Получено авторское свидетельство (совместно с Чалкиным Т.А.) на программный комплекс, реализующий выбор ключевой информации для шифрования данных по действующему стандарту России.

Два ученика стали лауреатами стипендии губернатора Красноярского края, а один – лауреат стипендии Правительства России и победитель конкурса на лучшую студенческую научную работу.

Награжден Благодарственным Письмом Законодательного Собрания Красноярского края. Награжден нагрудным знаком Министерства Образования и Науки РФ «За развитие научно-исследовательской работы студентов».

Zhdanov Oleg Nikolaevich was born on April 16, 1964. He graduated from Krasnoyarsk State University in 1986. The Ph. D. thesis in mathematical analysis was defended in 1994. At the moment

O. N. Zhdanov is Associate Professor of Informational Technologies subdepartment of Siberian State Space University and associate professor of Algebra and mathematical logic department of Siberian Federal university.

O. N. Zhdanov gives the following lecture courses: «Cryptographic methods of information security» (there is a certificate of Institute of Cryptography, Communication and Information Sciences of the corresponding advanced training), «Number-theoretic algorithms of cryptography», «Reliability theory».

The total number of his publications – 75. Eight of them are study guides.

Together with pupils, he developed a key information choice method for realization of block encryption algorithms. Together with Chalkin T. A. he received the copyright certificate on the program complex realizing the choice of key information for data encryption according to the current standard of Russia.

O. N. Zhanov was awarded by a letter of thanks from Legislative Assembly of Krasnoyarsk Krai, a breastplate of the Ministry of Education and Science of the Russian Federation «For development of students research activity».

Артем Викторович Соколов родился 15 апреля 1990 года в Одессе, УССР. Получил степень бакалавра (с отличием) по специальности «Системы технической защиты информации» в 2011 году, степень магистра (с отличием) по специальности «Системы технической защиты информации, автоматизация её обработки» в 2013 году и степень кандидата технических наук по специальности «Системы защиты информации» в 2014 году в Одесском национальном политехническом университете, г. Одесса, Украина.

С 2012 по 2014 работал младшим научным сотрудником кафедры Информационной безопасности в Одесском национальном политехническом университете. С 2014 года является старшим преподавателем кафедры Информационной безопасности Одесского национального политехнического университета. Является автором монографии и более 60 научных публикаций. Научные интересы включают в себя методы защиты информации на основе совершенных алгебраических конструкций, методы синтеза алгоритмов шифрования данных и нелинейных S-блоков.

Артем Соколов награжден Золотой медалью за высокие достижения в учебе, Дипломом победителя в конкурсе Магистров, 2013 год; Дипломом победителя Всеукраинского конкурса научно-исследовательских работ «Телекоммуникационные системы и сети», 2012 год; Дипломом за высокие академические и исследовательские достижения, 2010 год.

Artem V. Sokolov was born in Odessa, USSR, in 1990. He received a Bachelor (Hons) degree in systems of technical data protection in 2011, Master (Hons) degree in systems of technical data protection and automation of it's processing in 2013 and Ph. D. degree in data protection systems in 2014 from Odessa National Polytechnic University, Odessa, Ukraine.

From 2012 to 2014 he was a Junior Researcher of the Data Security department in Odessa National Polytechnic University. Since 2014 he has been a senior lecturer of the Data Security department in Odessa National Polytechnic University. He is the author of a book and more than 60 articles. His research interests include data protection methods based on perfect algebraic constructions, nonlinear S-box synthesis method, and stream encryption algorithms.

A. V. Sokolov awards and honors include: Gold medal for high achievements in education, Hons Diploma of Winner in Master Competition, 2013; winner of «Information and communication networks» Ukrainian competition of research papers, 2012; Diploma for excellent academic and research activities, 2010.