УДК 004.622.612

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 1, pp. 5-13

БЫСТРЫЕ ОРТОГОНАЛЬНЫЕ ПРЕОБРАЗОВАНИЯ НА ОСНОВЕ БЕНТ-ПОСЛЕДОВАТЕЛЬНОСТЕЙ

М.И. Мазурков, А.В. Соколов

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: alart@stream.com.ua

Разработан метод построения ортогональных преобразований на основе бент-последовательностей, для которого предложена экономичная схема вычисления коэффициентов преобразования. Найдены все минимаксные с точки зрения автокорреляционных свойств бент-последовательности длины $N = 16$.

Ключевые слова: бент-последовательность, ортогональное преобразование, экономичная схема, CDMA.

Введение

Важнейшим классом бинарных сигналов, интенсивно изучающихся в последние десятилетия, стали бент-последовательности, обладающие равномерным спектром Уошла-Адамара, и, соответственно, максимально возможным расстоянием нелинейности в смысле расстояния Хэмминга до кода Рида-Маллера первого порядка [1]. Вышеуказанные последовательности нашли применение во многих областях науки и техники, в том числе в теории передачи информации, криптографии, криптоанализе. Так, благодаря своему равномерному спектру амплитуд, бент-последовательности нашли свое применение в технологиях CDMA (англ. Code Division Multiple Access — множественный доступ с кодовым разделением), где они позволяют существенно уменьшить отношение пиковой и средней мощностей сигнала — пик-фактор, что приводит к более рациональному использованию мощности передатчика [2]. Высокое расстояние нелинейности бент-последовательностей приводит к существенному затруднению их аппроксимации классом аффинных функций, что позволяет наилучшим образом противостоять атакам линейного криптоанализа [3].

Целью настоящей статьи является разработка метода синтеза бинарных матриц Ψ ортогонального преобразования на основе бент-последовательностей и построение быстрого алгоритма вычисления коэффициентов преобразований.

Основная часть

В соответствии с определением [4,5] бинарная последовательность $B = [b_0, b_1, \ldots, b_i, \ldots, b_{n-1}]$, где $b_i \in \{\pm 1\}$ — коэффициенты, четной длины $N = 2^k$, $i = 0,1,\ldots,k-1$, называется бент-последовательностью, если она имеет равномерный по модулю спектр Уолша-Адамара $W_B(\omega)$, который представим в матричной форме

$$W_B(\omega) = BA,\ \omega = 0,1,\ldots,N, \qquad (1)$$

где A — матрица Уолша-Адамара порядка N.

Исходя из определения бент-последовательности, каждый спектральный коэффициент последовательности $W_B(\omega=0), W_B(\omega=1),\ldots,W_B(\omega=n-1)$ принимает значения из множества $\{\pm 2^{k/2}\}$.

В настоящее время, для произвольного значения длины N не существует конструктивного алгоритма, позволяющего построить полный класс бент-последовательностей, и даже асимптотических оценок количества существующих в природе бент-последовательностей [1]. Тем не менее, регулярные методы синтеза созданы для некоторых значений N, например, для $N=16$. Так в [5] предложен регулярный метод, позволяющий синтезировать полный класс бент-последовательностей на основе 4-х структур опорных матриц:

$$S_1(4)=\begin{bmatrix}\alpha\\ \beta\\ \gamma\\ \delta\end{bmatrix},\quad S_2(4)=\begin{bmatrix}a\\ b\\ c\\ d\end{bmatrix},\quad S_3(4)=\begin{bmatrix}q\\ q\\ s\\ \bar{s}\end{bmatrix},\quad S_4(4)=\begin{bmatrix}r\\ r\\ r\\ \bar{r}\end{bmatrix}, \tag{2}$$

где $\alpha,\beta,\gamma,\delta,a,b,c,d,q,s,r$ — векторы-элементы линейного векторного пространства V_4 векторов длины 4, где

$$V_4=\begin{matrix}\{++++,\ +++-,\ ++-+,\ ++--,\ +-++,\ +-+-,\ +--+,\ +---,\\ -+++,\ -++-,\ -+-+,\ -+--,\ --++,\ --+-,\ ---+,\ ----\}.\end{matrix}$$

Для каждой из матриц (2) существует определенное правило построения подкласса бент-последовательностей.

Так, например, конструкция $S_1(4)$ представляет из себя вертикальную конкатенацию векторов $\alpha,\beta,\gamma,\delta$ — всех четного веса, что отображает конструкцию Мэйорана-МакФарланда [1] и позволяет построить класс из $J_1=384$ бент-последовательностей, которые можем привести в виде 12-ти полиномов Жегалкина [3] с точностью до аффинных термов $\{1,x_1,x_2,x_3,x_4\}$

$$\begin{bmatrix}x_1x_3\oplus x_2x_3\oplus x_1x_4\oplus x_3x_4;\\ x_1x_3\oplus x_2x_3\oplus x_1x_4;\\ x_1x_3\oplus x_2x_3\oplus x_2x_4\oplus x_3x_4;\\ x_1x_3\oplus x_2x_3\oplus x_2x_4;\\ x_1x_3\oplus x_1x_4\oplus x_2x_4\oplus x_3x_4;\\ x_1x_3\oplus x_1x_4\oplus x_2x_4;\end{bmatrix}\quad\begin{bmatrix}x_1x_3\oplus x_2x_4;\\ x_1x_3\oplus x_2x_4\oplus x_3x_4;\\ x_2x_3\oplus x_1x_4\oplus x_2x_4\oplus x_3x_4;\\ x_2x_3\oplus x_1x_4\oplus x_2x_4;\\ x_2x_3\oplus x_1x_4;\\ x_2x_3\oplus x_1x_4\oplus x_3x_4.\end{bmatrix} \tag{3}$$

Аналогичным образом, на основе конструкций $S_2(4)$, $S_3(4)$, $S_4(4)$, где вектора a,b,c,d,q,s,r являются векторами нечетного веса, может быть получено $J_2+J_3+J_4=192+288+32=512$ бент-последовательностей, которые также представим в виде 16-ти полиномов Жегалкина с точностью до аффинных термов

$$\begin{bmatrix} x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_3x_4; \\ x_1x_2 \oplus x_1x_3 \oplus x_2x_4; \\ x_1x_2 \oplus x_1x_3 \oplus x_3x_4; \\ x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_4; \\ x_1x_2 \oplus x_2x_3 \oplus x_1x_4; \\ x_1x_2 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4; \\ x_1x_2 \oplus x_2x_3 \oplus x_3x_4; \\ x_1x_2 \oplus x_2x_3 \oplus x_1x_4 \oplus x_2x_4; \end{bmatrix} \quad \begin{bmatrix} x_1x_2 \oplus x_1x_4 \oplus x_3x_4; \\ x_1x_2 \oplus x_2x_4 \oplus x_3x_4; \\ x_1x_2 \oplus x_3x_4; \\ x_1x_2 \oplus x_1x_4 \oplus x_2x_4 \oplus x_3x_4; \\ x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_4; \\ x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2x_4; \\ x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3x_4; \\ x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_4 \oplus x_2x_4 \oplus x_3x_4. \end{bmatrix} \tag{4}$$

Таким образом, 28 полиномов Жегалкина (3) и (4) полностью определяют полный класс бент-последовательностей мощности $J = 896$.

Данные [6, 7] и проведенные исследования позволили установить, что на основе каждой из существующих бент-последовательностей может быть построена бинарная ортогональная матрица преобразования, путем выполнения операции диадного сдвига.

Нетрудно показать, что матрица $Diad(N)$ диадного сдвига (диадной перестановки) строится по рекуррентному правилу

$$Diad(N) = \begin{bmatrix} Diad(N/2) & Diad(N/2) + N/2 \\ Diad(N/2) + N/2 & Diad(N/2) \end{bmatrix}, \tag{5}$$

где $Diad(2) = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$. Например, для значения $N = 16$, получаем

$$Diad(16) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 & 10 & 9 & 12 & 11 & 14 & 13 & 16 & 15 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 & 11 & 12 & 9 & 10 & 15 & 16 & 13 & 14 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 & 12 & 11 & 10 & 9 & 16 & 15 & 14 & 13 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 & 13 & 14 & 15 & 16 & 9 & 10 & 11 & 12 \\ 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 & 14 & 13 & 16 & 15 & 10 & 9 & 12 & 11 \\ 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 & 15 & 16 & 13 & 14 & 11 & 12 & 9 & 10 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 16 & 15 & 14 & 13 & 12 & 11 & 10 & 9 \\ 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 10 & 9 & 12 & 11 & 14 & 13 & 16 & 15 & 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \\ 11 & 12 & 9 & 10 & 15 & 16 & 13 & 14 & 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\ 12 & 11 & 10 & 9 & 16 & 15 & 14 & 13 & 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \\ 13 & 14 & 15 & 16 & 9 & 10 & 11 & 12 & 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \\ 14 & 13 & 16 & 15 & 10 & 9 & 12 & 11 & 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 \\ 15 & 16 & 13 & 14 & 11 & 12 & 9 & 10 & 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 \\ 16 & 15 & 14 & 13 & 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix}. \tag{6}$$

Осуществляя перестановку элементов бент-последовательности в соответствии с правилами (строками) построения матрицы диадного сдвига $Diad$ получаем бинарную матрицу Ψ ортогонального преобразования.

Например, пусть задан первый полином Жегалкина из (3), полностью определяющий структуру бинарной бент-последовательности

$$B = \{11111-1-111-11-1-1-111\}, \tag{7}$$

тогда с учетом выражения (6) можем построить бинарную матрицу ортогонального преобразования

$$\Psi = \left[\begin{array}{cccc|cccc|cccc|cccc}
+ & + & + & + & + & - & - & + & + & - & + & - & - & - & + & + \\
+ & + & + & + & - & + & + & - & - & + & - & + & - & - & + & + \\
+ & + & + & + & - & + & + & - & + & - & + & - & + & + & - & - \\
+ & + & + & + & + & - & - & + & - & + & - & + & + & + & - & - \\
\hline
+ & - & - & + & + & + & + & + & - & - & + & + & + & - & + & - \\
- & + & + & - & + & + & + & + & - & - & + & + & - & + & - & + \\
- & + & + & - & + & + & + & + & + & + & - & - & + & - & + & - \\
+ & - & - & + & + & + & + & + & + & + & - & - & - & + & - & + \\
\hline
+ & - & + & - & - & - & + & + & + & + & + & + & + & - & - & + \\
- & + & - & + & - & - & + & + & + & + & + & + & - & + & + & - \\
+ & - & + & - & + & + & - & - & + & + & + & + & - & + & + & - \\
- & + & - & + & + & + & - & - & + & + & + & + & + & - & - & + \\
\hline
- & - & + & + & + & - & + & - & + & - & - & + & + & + & + & + \\
- & - & + & + & - & + & - & + & - & + & + & - & + & + & + & + \\
+ & + & - & - & + & - & + & - & - & + & + & - & + & + & + & + \\
+ & + & - & - & - & + & - & + & + & - & - & + & + & + & + & +
\end{array}\right], \tag{8}$$

В общем случае, матрица Ψ является симметричной ортогональной матрицей [6], т.е.

$$\Psi \cdot \Psi^T = \Psi * \Psi = NI, \tag{9}$$

где T — оператор транспонирования, I — единичная матрица порядка N.

В [7] разработана экономичная схема вычисления коэффициентов ортогональных преобразований на основе совершенных двоичных решеток. Данная схема основана на учете свойств двухпетлевого циклического сдвига, который используются для построения матриц таких преобразований. В настоящей работе установлено, что подобная экономичная схема вычисления коэффициентов ортогонального преобразования может быть построена и для случая произвольной структуры бент-последовательности. Функционирующая модель данной схемы была собрана с помощью интерактивного инструмента имитации и анализа динамических систем Matlab Simulink.

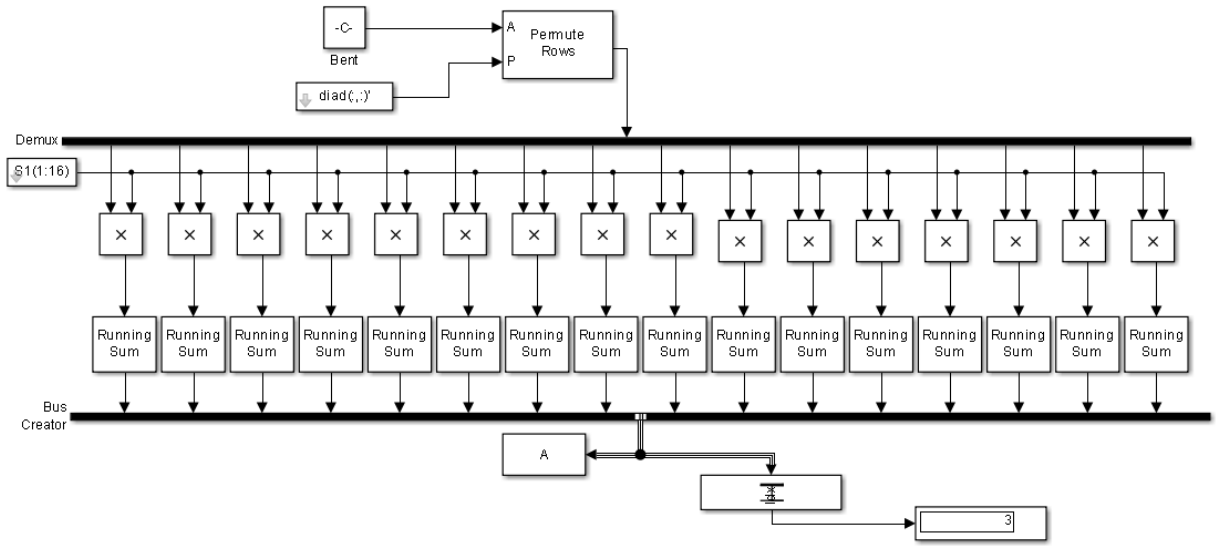

Рис. 1. Экономичная схема вычисления коэффициентов ортогональных преобразований на основе бент-последовательностей длины $N = 16$

На рис. 1 приняты следующие условные обозначения, расшифрованные в табл. 1.

Таблица 1.

Расшифровка условных обозначений схемы (рис. 1)

×	— умножитель;		— дисплей, вывод результата.
Running Sum	— накопительный сумматор;	A	— вывод массива, содержащего результат;
-C- Bent1	— ввод исходной бент-последовательности;	diad(:,:)'	— ввод диадной синхропоследовательности;
A Permute Rows P	— коммутатор входов по правилу диадного сдвига;		— нахождение индекса максимального элемента;

Опишем принцип функционирования экономичной схемы вычисления коэффициентов ортогонального преобразования на основе бент-последовательностей. На вход коммутатора входов по правилу диадных сдвигов подаются элементы исходной бент-последовательности, например (7), а также диадная синхропоследовательность, сформированная в соответствии с (8), которая может храниться в накопителе, либо же формироваться на каждом такте работы схемы. Элементы преобразованной в соответствии с правилом диадной синхропоследовательности бент-последовательности на каждом такте схемы перемножаются с отсчетом сигнала, соответствующим номеру такту, и подаются на вход накопительного сумматора, после чего мультиплексируются. Результирующий вектор подается на решающее устройство, определяющее наиболее правдоподобный переданный сигнал как индекс максимального элемента результирующего вектора преобразования.

Пусть, например, передавался один из ортогональных сигналов, соответствующей 3-й строке матрицы (8), т.е.

$$S(t) = \{1111-111-11-11-111-1-1\}, \quad (10)$$

который под воздействием некоторой помехи в канале связи был искажен, в результате чего на приемник поступила последовательность

$$Y(t) = \{00-22-102-31-11-101-10\}, \quad (11)$$

тогда на выходе схемы мы получим последовательность - корреляционный вектор

$$Z(\tau) = Y \cdot \Psi = \{-408-44-80-4-444-4-444-4\}, \tau = 0,1,\ldots,15, \quad (12)$$

соответственно схема (рис. 1) приняла решение о том, что максимально правдоподобно был передан сигнал соответствующей 3-й строке матрицы (8), что соответствует действительности.

Учитывая определение Дж. фон Неймана [8], будем оценивать сложность реализации предложенной экономичной схемы вычисления коэффициентов ортогональных преобразований на основе бент-последовательностей как число умножителей, как самых сложнореализуемых её компонентов. Очевидно, сложность реализации прямой схемы вычисления коэффициентов ортогонального преобразования на основе бент-последовательностей как матричного произведения можно оценить как $O(N^2)$, тогда как сложность предлагаемой схемы $O(N)$, т.е. имеем выигрыш

$$\gamma = \frac{N^2}{N} = N, \quad (13)$$

что является даже более значительным, чем выигрыш при использовании алгоритмов быстрого преобразования Уолша-Адамара, где сложность оценивается как $O(N \cdot \log_2(N))$. Не вызывает сомнений также тот факт, что предложенная схема может быть легко масштабирована для любых N.

Отметим, что все остальные компоненты схемы, в том числе коммутатор и накопительные сумматоры имеют низкую сложность реализации, и обычно входят в состав современных микросхем PLD (англ. Programmable Logic Device — программируемая логическая интегральная схема) [9].

Вопрос выбора исходной бент-последовательности зависит от конкретных приложений, в которых могут быть использованы предложенные ортогональные преобразования. Например, использование полного класса бент-последовательностей может быть оправдано для реализации концепции оперативной смены ансамбля используемых сигналов для решения задач защиты информации. В задачах же повышения помехоустойчивости могут быть использованы минимаксные [10] бент-последовательности с точки зрения ААКФ (апериодической автокорреляционной функции)

$$r_{ААКФ}(n) = \sum_{l=0}^{2N-2} B(l)B(n+l), n = 0,1,\ldots,2N-2, \quad (14)$$

а также ПАКФ (периодической автокорреляционной функции)

$$r_{ПАКФ}(n) = \sum_{l=0}^{N-1} B(l)B(n+l),\ n = 0,1,\ldots,N-1. \qquad (15)$$

Результаты проведенных исследований позволили установить значения максимумов побочных лепестков автокорреляционных функций сигналов из класса бент-последовательностей, которые, для наглядности, представим в виде таблицы 2.

Таблица 2.

Значения максимумов побочных лепестков автокорреляционных функций класса бент-последовательностей

$\max\limits_{2,3,\ldots,16}\{r_{ААКФ}\}$	3	4	5	7	8	9
Количество бент-последовательностей	344	152	328	56	8	8
$\max\limits_{2,3,\ldots,16}\{r_{ПАКФ}\}$	—	4	—	—	8	—
Количество бент-последовательностей	—	832	—	—	64	—

Отметим, что все минимаксные с точки зрения ААКФ бент-последовательности являются также минимаксными и с точки зрения ПАКФ. Например, минимаксная бент-последовательность может быть представлена в бинарном, двоичном и шестнадцатеричном видах

$$B = [1\,1\,1\,1\,1 - 1\,1 - 1\,1 - 1 - 1\,1\,1\,1 - 1 - 1] \Rightarrow [0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,1\,0\,0\,0\,1\,1]_2 \Rightarrow [0563]_h \qquad (16)$$

обладает ААКФ

$$r_{ААКФ} = \begin{Bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 16 & -1 & 4 & 1 & 0 & 1 & -4 & 3 & 0 & -3 & 0 & -1 & 0 & -1 & 0 & 1 \end{Bmatrix}, \qquad (17)$$

и ПАКФ

$$r_{ПАКФ} = \begin{Bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 16 & 0 & 4 & 0 & 0 & 0 & -4 & 0 & 0 & 0 & -4 & 0 & 0 & 0 & 4 & 0 \end{Bmatrix}, \qquad (18)$$

которые можно представить в виде графиков (рис. 2).

Для краткости приведем все минимаксные бент-последовательности в виде их шестнадцатеричных эквивалентов (жирным шрифтом выделены шестнадцатеричные эквиваленты, соответствующие совершенным двоичным решеткам [5, 10]).

Анализ данных табл. 2 свидетельствует о достаточно большом количестве бент-последовательностей, обладающих хорошими автокорреляционными свойствами.

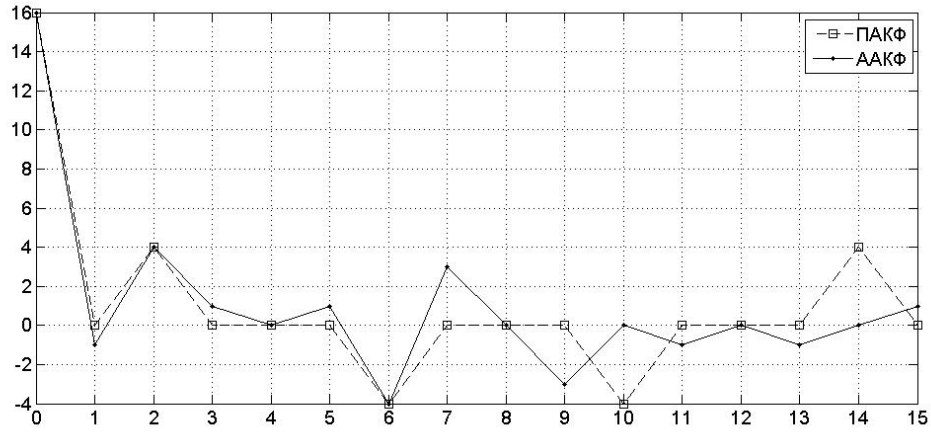

Рис.2. ААКФ и ПАКФ минимаксной бент-последовательности (16)

Таблица 2.

Шестнадцатеричные эквиваленты всех минимаксных бент-последовательностей

0563	059C	**0653**	093A	**095C**	09C5	0A93	**0C56**	**0CA9**	1178
11D2	**12B8**	1427	**14E4**	**1B14**	1BD7	**1D48**	**1DB7**	1E88	1EDD
2147	**218B**	221E	**2287**	2714	**27D7**	281B	**28D8**	**2BDB**	2D11
2D88	**2E7B**	**2EDE**	30A9	**356F**	3650	36AF	395F	39FA	**3A6F**
3AF6	**3F65**	3FA6	4172	**41B1**	442D	**44E1**	**47ED**	482E	**4B11**
4BDD	4D7E	4E7D	**4EBE**	5039	50C9	**53F9**	**5903**	**59FC**	**5C09**
5C90	5F39	5FC6	**603A**	6305	63F5	6503	6A0C	**6ACF**	6C0A
6CF5	6F5C	**6FC5**	7241	**7282**	7412	**747B**	**74DE**	774B	**7822**
78DD	**7B74**	**7BD1**	**7D72**	7DB1	7EB2	**8171**	**8272**	82B1	**8474**
84D1	87BB	**882D**	**88D2**	**8B7B**	**8BDE**	8D41	**8D82**	**8E81**	905C
90C5	9350	950C	**95CF**	9A03	9C05	9C5F	**9F35**	**9FCA**	A063
A309	A390	**A3F9**	A63F	A930	**ACF9**	AF6C	AFC9	B17D	**B1BE**
B411	B477	**B71D**	**B7E2**	**B8ED**	BB78	**BBE1**	BE72	**BEB1**	**C065**
C0A6	**C56F**	C5F6	C65F	C90A	C95F	**CA60**	**CA9F**	CFA9	**D17B**
D1DE	**D288**	D418	D71B	**D7D8**	D814	**D8D7**	**DBD4**	**DD87**	**DE2E**
DE8B	**DED1**	**E144**	**E1BB**	E284	**E414**	E4D7	E7D4	EB27	**EBE4**
EDB8	**EE4B**	**EEB4**	F36A	F536	F593	**F65C**	**F6AC**	**F953**	FA39
FA93	FC65	—	—	—	—	—	—	—	—

Вывод

В заключении отметим основные результаты проведенных исследований:

1. Получила дальнейшее развитие теория синтеза бинарных матриц ортогональных преобразований, в рамках чего разработан метод формирования бинарных матриц ортогональных преобразований на основе бент-последовательностей, которые могут найти свое применение в технологиях передачи информации, таких как CDMA, а также в криптографии и криптоанализе.

2. Разработана экономичная схема вычисления коэффициентов ортогонального преобразования на основе бент-последовательностей, позволяющая существенно сократить необходимое для её реализации количество компонентов, что имеет

критическое значение при реализации разработанных технологий, например, на мобильных устройствах.

3. Найден полный класс минимаксных с точки зрения боковых лепестков автокорреляционных функций бент-последовательностей длины $N = 16$, который может быть рекомендован к использованию в системах связи.

Список литературы

1. Токарева, Н.Н. Бент-функции: результаты и приложения. Обзор работ / Н.Н. Токарева // Приклад. дискрет. математика. — Томск, 2009. — Сер. №1(3). — С. 15—37.
2. Peterson, K.G. Sequences For OFDM and Multi-code CDMA: two problems in algebraic Coding Theory // Sequences and their applications. Seta 2001. Second Int. Conference (Bergen, Norway, May 13—17, 2001). Proc. Berlin: Springer, 2002. P.46—71.
3. Логачев, О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. — М: Издательство МЦНМО. — 2004. — 472 с.
4. Rothaus, O.S. On “bent” functions / O.S. Rothaus // J. Comb. Theory Ser. A. — USA: Academic Press Inc, 1976. — №20(3). — P.300—305.
5. Мазурков, М.И. Регулярные правила построения полного класса бент-последовательностей длины 16 / М.И. Мазурков, А.В. Соколов. — Одесса: Труды ОНПУ, 2013. — С.227—230.
6. Дворников, В.Д. Ортогональные коды на основе бент-последовательностей / В.Д. Дворников. — Доклады БГУИР, Минск, 2003. — С. 110—113.
7. Мазурков, М.И. Быстрые ортогональные преобразования на основе совершенных двоичных решеток / М.И. Мазурков, М.Ю. Герасименко // Известия высших учебных заведений. Радиоэлектроника. – 2006. – Т. 49, N 9. - С. 54-60.
8. Блох, Э.Л. Обобщенные каскадные коды / Э.Л. Блох, В.В. Зяблов. — М.: Связь, 1976. — 240 с.
9. Попов, А.Ю. Проектирование цифровых устройств с использованием ПЛИС. — М.: Изд-во МГТУ им. Н.Э. Баумана, 2009. — 80 с.
10. Мазурков, М.И. Системы широкополосной радиосвязи: учеб. пособие для студ. вузов / М.И. Мазурков. — Одесса: Наука и техника, 2010. — 340 с.

ШВИДКІ ОРТОГОНАЛЬНІ ПЕРЕТВОРЕННЯ НА ОСНОВІ БЕНТ-ПОСЛІДОВНОСТЕЙ

М.І. Мазурков, А.В. Соколов

Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна, e-mail: alart@stream.com.ua

Розроблено метод побудови ортогональних перетворень на основі бент-послідовностей, для якого запропонована економічна схема обчислення коефіцієнтів перетворення. Знайдено всі мінімаксні з точки зору автокореляційних властивостей бент-послідовності довжини N=16.

Ключові слова: бент-послідовність, ортогональне перетворення, економічна схема, CDMA.

FAST ORTHOGONAL TRANSFORMATIONS BASED ON BENT-SEQUENCES

M.I. Mazurkov, A.V. Sokolov

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: alart@stream.com.ua

A method was developed to design orthogonal transformations based on bent sequences. The efficient scheme of computation of transformation coefficients was proposed for the above mentioned method as well. There were found all bent-sequences according to the minimax criterion in terms of autocorrelation properties with the length of $N = 16$

Keywords: bent sequence, orthogonal transformation, efficient scheme, CDMA