УДК 004.622.612

М.И. Мазурков, д-р техн. наук, проф.,
А.В. Соколов, магистр,
Одес. нац. политехн. ун-т

РЕГУЛЯРНЫЕ ПРАВИЛА ПОСТРОЕНИЯ ПОЛНОГО КЛАССА БЕНТ-ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛИНЫ 16

М.І. Мазурков, А.В. Соколов. **Регулярні правила побудови повного класу бент-послідовностей довжини 16**. Запропоновано алгебраїчні конструкції опорних матриць в символьному вигляді та розроблено регулярні правила побудови повного класу бент-послідовностей (БП) довжини $n = 16$ і об'єму $J = 896$. Показано, що нелінійні двійкові коди на основі повного класу БП є найкращими коригуючими кодами з мінімальною надмірністю.

Ключові слова: бент-послідовності, синтез, криптографія, коригувальні коди.

М.И. Мазурков, А.В. Соколов. **Регулярные правила построения полного класса бент-последовательностей длины 16.** Предложены алгебраические конструкции опорных матриц в символьном виде и разработаны регулярные правила построения полного класса бент-последовательностей (БП) длины $n = 16$ и объема $J = 896$. Показано, что нелинейные двоичные коды на основе полного класса БП являются наилучшими корректирующими кодами с минимальной избыточностью.

Ключевые слова: бент-последовательности, синтез, криптография, корректирующие коды.

M.I. Mazurkov, A.V. Sokolov. **The regular rules of constructing the complete class of bent-sequences of length 16.** The algebraic constructions of basic matrices in a symbolical representation are offered, and regular rules of constructing a complete class of bent-sequences (BS) of length $n = 16$ and volume $J = 896$ are developed. It is shown that nonlinear binary codes on the basis of the complete class of BS are the best error-correcting codes with the minimum redundancy.

Keywords: bent-sequences, synthesis, cryptography, error-correcting codes.

Одной из важнейших характеристик булевых функций, применяемых как в криптографии, криптоанализе, так и в теории кодирования, является их нелинейность. Линейность булевой функции является свидетельством ее простой реализации и источником информации о многих ее свойствах, что диктует задачу построения высоконелинейных булевых функций. Булевы функции, нелинейность которых достигает экстремально больших значений, были введены и названы бент-функциями, таблицы истинности которых соответственно называются бент-последовательностями (БП) [1].

Основным в теории бент-функций является описание полного класса БП соответствующей длины регулярными правилами синтеза. До сих пор данный вопрос не получил своего решения даже для малых значений длины БП, более того, не существует приемлемых верхних и нижних оценок мощности класса БП от m переменных.

Лучшие предложенные методы построения БП, например, конструкция Мэйорана-МакФарланда, конструкция Диллона, правила Ротхауса [2] позволяют получить регулярными методами лишь некоторые БП из полного класса. Такая ситуация существенно затрудняет полномасштабное использование всех практически ценных свойств БП в современных информационных технологиях.

Целью статьи является построение регулярных правил синтеза полного класса БП длины $n = 16$ путем расширения и существенного дополнения конструкции Мэйорана-МакФарланда [2] после разработки обобщенных форм опорных матриц в символьном виде; установление взаимосвязи класса БП с классом совершенных двоичных решеток (СДР) [3], а также построение нелинейного двоичного корректирующего кода на основе полного класса БП, определение его минимальной избыточности [4].

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

В соответствии с определением [1] бинарная последовательность $\mathbf{B}=[b_0,b_1,\cdots,b_i,\cdots,b_{n-1}]$, где $b_i\in\{\pm1\}$ — коэффициенты четной длины $n=2^{2m}=N^2$, $i=\overline{0,n-1}$; N — порядок матрицы Уолша-Адамара, называется бент-последовательностью, если она имеет равномерный по модулю спектр Уолша-Адамара $\mathbf{W}_B(\omega)$, который представим в матричной форме

$$\mathbf{W}_B(\omega)=\mathbf{BA},\ \omega=\overline{0,n-1}, \tag{1}$$

где $\mathbf{A}$ — матрица Уолша-Адамара порядка $N^2=16$.

Каждый спектральный коэффициент $\mathbf{W}_B(0),\mathbf{W}_B(1),...,\mathbf{W}_B(n-1)$ принимает значения из множества $\{\pm2^{N/2}\}$.

Установлено, что полный класс БП длины $n=16$ можно получить на основе четырех специальных опорных матриц, определяющих правила конкатенации элементов множества всех бинарных векторов длины $m=4$

$$V_4=\begin{matrix}\{++++,\ +++-,\ ++-+,\ ++--,\ +-++,\ +-+-,\ +--+,\ +---,\\ -+++,\ -++-,\ -+-+,\ -+--,\ --++,\ --+-,\ ---+,\ ----\}.\end{matrix} \tag{2}$$

Экспериментально, в обобщенной форме, с точностью до порядка следования и инверсии строк установлен символьный вид специальных четырех опорных матриц:

$$\mathbf{S}_1(4)=\begin{bmatrix}\boldsymbol{\alpha}\\ \boldsymbol{\beta}\\ \boldsymbol{\gamma}\\ \boldsymbol{\delta}\end{bmatrix},\quad \mathbf{S}_2(4)=\begin{bmatrix}\mathbf{a}\\ \mathbf{b}\\ \mathbf{c}\\ \mathbf{d}\end{bmatrix},\quad \mathbf{S}_3(4)=\begin{bmatrix}\mathbf{q}\\ \mathbf{q}\\ \mathbf{s}\\ \overline{\mathbf{s}}\end{bmatrix},\quad \mathbf{S}_4(4)=\begin{bmatrix}\mathbf{r}\\ \mathbf{r}\\ \mathbf{r}\\ \overline{\mathbf{r}}\end{bmatrix}, \tag{3}$$

где векторы $\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma},\boldsymbol{\delta},\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d},\mathbf{q},\mathbf{s},\mathbf{r}$ в соответствии с V_4 (2) определим с помощью правил П1…П4.

Сформулируем некоторые свойства полученных матриц (3) в виде утверждений.

Утверждение 1. Каждая матрица (3) удовлетворяет необходимому условию существования опорных матриц для построения БП, если разбаланс Δ каждой соответствующей бинарной матрицы удовлетворяет условию

$$\Delta=K^+-K^-=\pm N, \tag{4}$$

где K^+ и K^- — число символов соответственно “+1” и “–1” в бинарной матрице.

Действительно, только в этом случае спектральный коэффициент $\mathbf{W}_B(0)$ будет равняться N либо $-N$.

Достаточные условия определяются набором следующих правил построения бинарных матриц на основе опорных (3).

Правило П1. $\mathbf{S}_1(4)$ — матрица Уолша-Адамара [1] с произвольным порядком следования строк (векторов) $\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma},\boldsymbol{\delta}$ и произвольным способом их инверсии, которая отражает конструкцию Мэйорана-МакФарланда [2] и путем конкатенации строк порождает первый подкласс БП объема $J_1=4!\cdot2^4=384$, представляющий собой известную [2] нижнюю границу количества БП.

Правило П2. $\mathbf{S}_2(4)$ — матрица, все строки (векторы) $\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d}$ которой различны и имеют нечетный вес, т.е. нечетное число символов “–1”. В матрице $\mathbf{S}_2(4)$ допускается перестановка строк и знаковое кодирование строк векторами из V_4 (2) только четного веса, для соблюдения условия разбаланса (4). Данное правило порождает второй подкласс БП объема $J_2=4!\cdot2^{N-1}=192$.

Правило П3. $\mathbf{S}_3(4)$ — матрица, содержащая две совпадающие строки и две инверсные строки, все только нечетного веса, где строки (векторы) $\mathbf{q}$ и $\mathbf{s}$ принимают значения

$$\mathbf{q},\mathbf{s} \in \begin{array}{|c|c|c|c|}\hline \mathbf{a} & \mathbf{b} & \mathbf{c} & \mathbf{d} \\ \hline +++- & ++-+ & +-++ & +--- \\ \hline \end{array}. \quad (5)$$

Исследования показали, что на основе $\mathbf{S}_3(4)$ и с учетом (5) допускается построение следующих 24 комбинаций знакового кодирования БП:

$$\left.\begin{array}{llll} 1.\ \mathbf{a\bar{a}bb} & 7.\ \mathbf{b\bar{b}aa} & 13.\ \mathbf{c\bar{c}aa} & 19.\ \mathbf{d\bar{d}aa} \\ 2.\ \mathbf{a\bar{a}cc} & 8.\ \mathbf{b\bar{b}cc} & 14.\ \mathbf{c\bar{c}bb} & 20.\ \mathbf{d\bar{d}bb} \\ 3.\ \mathbf{a\bar{a}dd} & 9.\ \mathbf{b\bar{b}dd} & 15.\ \mathbf{c\bar{c}dd} & 21.\ \mathbf{d\bar{d}cc} \\ 4.\ \mathbf{a\bar{a}\bar{b}\bar{b}} & 10.\ \mathbf{b\bar{b}\bar{a}\bar{a}} & 16.\ \mathbf{c\bar{c}\bar{a}\bar{a}} & 22.\ \mathbf{d\bar{d}\bar{a}\bar{a}} \\ 5.\ \mathbf{a\bar{a}\bar{c}\bar{c}} & 11.\ \mathbf{b\bar{b}\bar{c}\bar{c}} & 17.\ \mathbf{c\bar{c}\bar{b}\bar{b}} & 23.\ \mathbf{d\bar{d}\bar{b}\bar{b}} \\ 6.\ \mathbf{a\bar{a}\bar{d}\bar{d}} & 12.\ \mathbf{b\bar{b}\bar{d}\bar{d}} & 18.\ \mathbf{c\bar{c}\bar{d}\bar{d}} & 24.\ \mathbf{d\bar{d}\bar{c}\bar{c}} \end{array}\right\}, \quad (6)$$

где черта сверху означает инверсный вектор (инверсную строку).

Каждая комбинация (6) порождает путем перестановок строк точно $4!/2! = 12$ новых БП. Таким образом, правило порождает третий подкласс БП объема $J_3 = 24 \cdot 12 = 288$.

Правило П4. $\mathbf{S}_4(4)$ — матрица, состоящая из трех совпадающих строк $\mathbf{r}$ нечетного веса и одной инверсной строки $\bar{\mathbf{r}}$.

Допускается выбор в качестве строки $\mathbf{r}$ любого из 2^{N-1} вектора нечетного веса, а также допускаются $N!/(N-1)! = 4$ перестановки строк в каждой бинарной матрице. Следовательно, порождается четвертый подкласс БП объема $J_4 = (4!/3!) \cdot 2^3 = 32$.

Таким образом, построен полный класс БП длины $n = 16$ и объема $J = J_1 + J_2 + J_3 + J_4 = 896$. Альтернативные эмпирические исследования полного класса последовательностей длины $n = 16$ приводят к получению того же класса БП.

Проведенные исследования структуры полного класса БП, записанных в виде матриц $\mathbf{h}$ размера 4×4, путем сегментации БП на элементы длины 4, каждый из которых представляет строку матрицы $\mathbf{h}$, показали, что полный класс БП длины $n = 16$ полностью поглощает полный класс совершенных двоичных решеток $H(4) = \left\| \mathbf{h}_{i,j} \right\|$ [3] с идеальной двумерной периодической автокорреляционной функцией (ДПАКФ)

$$\mathbf{R}(\tau_1, \tau_2) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \mathbf{h}_{i,j} \mathbf{h}_{i+\tau_1, j+\tau_2} = \begin{cases} N^2, & \text{если } \tau_1 = \tau_2 = 0, \\ 0, & \text{при других } \tau_1 \text{ и } \tau_2. \end{cases} \quad (7)$$

Например, для одной из БП вида $\mathbf{B} = [+++-+++-+++---+]$, определяемой правилом П4, построены соответствующая решетка и ее ДПАКФ

$$\mathbf{h} = \begin{bmatrix} + & + & + & - \\ + & + & + & - \\ + & + & + & - \\ - & - & - & + \end{bmatrix}, \quad \left\| \mathbf{R}(\tau_1, \tau_2) \right\| = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \quad (8)$$

Матрицы Уолша-Адамара, используемые конструкцией Майорана-МакФарланда, свойством ДПАКФ (7) не обладают.

Рассмотрим некоторые криптографические свойства построенного полного класса БП. Известно, что расстояние нелинейности N_f БП определяется как минимальное расстояние Хэмминга между двоичной булевой функцией f, соответствующей БП, и всеми кодовыми словами аффинного кода [2], т.е.

$$N_f = \min(\mathrm{dist}(f, \varphi)) = 2^{N-1} - 2^{(N/2)-1} = 8 - 2 = 6, \quad (9)$$

где $\{\varphi\} \in < u, v > \oplus a$ — кодовые слова аффинного кода,

$u, v \in V_N$, $a \in \{0,1\}$.

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

Алгебраическая степень нелинейности любой БП от $m \geq 4$ переменных $\deg(f) \leq \frac{m}{2}$. Например, для функции $f = \{0001000100011110\}$, полученной путем отображения бинарной БП **B** по правилу "–" $\to 1$, "+" $\to 0$, определен конкретный вид полинома Жегалкина $\Phi(x_1, x_2, x_3, x_4)$ для функции f от четырех переменных [5]. По быстрой методике нахождения коэффициентов этого полинома находится $\Phi(x_1, x_2, x_3, x_4) = x_1 x_2 \oplus x_3 x_4$, т.е. полином действительно имеет алгебраическую степень нелинейности $\deg(f) = 2$.

Единственным недостатком любых БП, с точки зрения криптографии, является их несбалансированность, поскольку условие разбаланса $\Delta = \pm N$ (4) принципиально необходимо для построения БП.

Определим возможности построения корректирующих кодов на основе полных классов БП.

Утверждение 2. Двоичный нелинейный код (n, r, d), построенный на основе полного класса БП длины $n = 16$, имеет кодовое расстояние Хэмминга $d = N = |\Delta| = 4$, где $\Delta = K^{(+)} - K^{(-)}$ — разбаланс каждой опорной матрицы (3), а величина $r = n - \log_2 J = 6{,}1926$ — избыточность кода.

Таким образом, построен двоичный нелинейный код $(n, r, d) = (16; 6{,}1926; 4)$ соответствующий наилучшим кодам с минимальной избыточностью.

На основании изложенного можно сделать следующие выводы:

— впервые разработаны правила регулярного построения полного класса БП длины $n = 16$ на основе предложенных опорных матриц в символьной форме, которые могут быть использованы для разработки методов синтеза полных классов БП других длин, например, $n \geq 64$, а также для установления улучшенных нижних и верхних оценок их объема;

— установлено, что полный класс БП длины $n = 16$ и объема $J = 896$ полностью поглощает полный класс совершенных двоичных решеток порядка $N = 4$ и объема $J_{\text{СДР}} = 384$;

— показана практическая привлекательность полного класса БП для построения наилучших нелинейных двоичных корректирующих кодов с минимальной избыточностью.

Литература

1. Rothaus, O.S.: On "bent" functions / O.S. Rothaus // J. Comb. Theory Ser. A. — USA: Academic Press Inc, 1976. — №20(3). — P.300 — 305.
2. Токарева, Н.Н. Бент-функции: результаты и приложения. Обзор работ / Н.Н. Токарева // Прикклад. дискрет. математика. — Томск, 2009. — Сер. №1(3). — С. 15 — 37.
3. Мазурков, М.И. Системы широкополосной радиосвязи: учеб. пособие для студ. вузов / М.И. Мазурков. — Одесса: Наука и техника, 2010. — 340 с.
4. Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. — М.: Связь, 1979. — 745 с.
5. Ростовцев, А.Г. Теоретическая криптография / А.Г. Ростовцев, Е.Б. Маховенко. — СПб.: НПО "ПРОФЕССИОНАЛ". — 2004. — 478 с.

References

1. Rothaus, O.S.: On "bent" functions / O.S. Rothaus // J. Comb. Theory Ser. A. — USA: Academic Press Inc, 1976. — №20(3). — pp.300—305.
2. Tokareva, N.N. Bent-funktsii: rezul`taty i prilozheniya. Obzor rabot [Bent functions: results and applications. A review of works] / N.N. Tokareva // Priklad. diskret. Matematika [Applied Discr.Math.]. — Tomsk, 2009. — Ser. #1(3). — pp. 15 — 37.
3. Mazurkov, M.I. Sistemy shirokopolosnoy radiosvyazi: ucheb. posobie dlya stud. vuzov [Wideband Radio Systems: textbook for university students] / M.I. Mazurkov. — Odessa: Nauka i tekhnika, 2010. — 340 p.

4. Mak-Vil'yams, F. Dzh. Teoriya kodov ispravlyayushchikh oshibki [The theory of error-correcting codes] / F. Dzh. Mak-Vil'yams, N. Dzh. A. Sloehn. — Moscow, 1979. — 745 p.
5. Rostovtsev, A.G. Teoreticheskaya kriptografiya [Theoretical cryptography] / A.G. Rostovtsev, E.B. Makhovenko, — St. Petersburg — 2004. — 478 p.

Рецензент д-р техн. наук, проф. Одес. нац. политехн. ун-та Дмитришин Д.В.

Поступила в редакцию 20 февраля 2013 г.

УДК 004.056.55

Н.А. Барабанов, инженер,
А.В. Соколов, магистр,
Одес. нац. политехн. ун-т

СЛОЖНОСТЬ АППАРАТНОЙ РЕАЛИЗАЦИИ ПОЛНОГО КЛАССА БЕНТ-ФУНКЦИЙ ЧЕТЫРЕХ ПЕРЕМЕННЫХ

М.О. Барабанов, А.В. Соколов. **Складність апаратної реалізації повного класу бент-функцій чотирьох змінних.** Проведена оптимізація апаратної реалізації високонелінійних бент-функцій чотирьох змінних, в рамках чого знайдений клас бент-функцій, оптимальних з точки зору апаратної реалізації, який може бути використаний для завдань поточного шифрування. Розраховані основні криптографічні характеристики знайдених оптимальних бент-функцій, а також завадостійких кодів на їх основі.
Ключові слова: бент-функції, апаратна реалізація, поточне шифрування, коригувальні коди.

Н.А. Барабанов, А.В. Соколов. **Сложность аппаратной реализации полного класса бент-функций четырех переменных.** Проведена оптимизация аппаратной реализации высоконелинейных бент-функций четырех переменных, в рамках чего найден класс бент-функций, оптимальных с точки зрения аппаратной реализации, который может быть использован для задач поточного шифрования. Рассчитаны основные криптографические характеристики найденных оптимальных бент-функций, а также помехоустойчивых кодов на их основе.
Ключевые слова: бент-функции, аппаратная реализация, поточное шифрование, корректирующие коды.

N.A. Barabanov, A.V. Sokolov. **Hardware implementation complexity of a full class of bent functions of four variables.** In this paper the optimization of hardware implementation of highly nonlinear bent functions of 4 variables is proposed, within which we find a class of bent functions that are optimal in terms of hardware implementation, which can be used for tasks of stream encryption. The main cryptographic properties of the found optimal bent functions are estimated, as well as the error-correcting codes based on them are researched.
Keywords: Bent functions, hardware implementation, stream encryption, error-correcting codes.

Решающую роль, определяющую как криптографическую устойчивость, так и быстродействие большинства современных алгоритмов поточного шифрования (ПШ), играют булевы функции [1]. Такие системы обычно построены по принципу модифицированного шифра Вернама, где в качестве ключа используется псевдослучайная последовательность (гамма), которая по заранее оговоренному закону генерируется по определенному алгоритму. Данная гамма Г поразрядно складывается по модулю 2 с битами исходного сообщения p_i, в результате чего формируется криптограмма