

МЕТОД СИНТЕЗА ПОЛНОГО КЛАССА БЕНТ-ФУНКЦИЙ ШЕСТИ ПЕРЕМЕННЫХ

А.В. Соколов

Одесский национальный политехнический университет

SYNTHESIS METHOD OF A COMPLETE CLASS OF BENT-FUNCTIONS OF SIX VARIABLES

A.V. Sokolov

Odessa National Polytechnic University

Предложен метод построения полного класса бент-функций шести переменных на основе знакокодирующих матриц, структурных, асинхронных и синхронных перестановок применительно к теории бент-квадратов Агиевича. Полученный полный класс бент-функций может быть использован при решении многих проблем теории передачи информации, помехоустойчивого кодирования, криптографии и криптоанализа.

Ключевые слова: бент-функция, бент-квадрат Агиевича, знакокодирующая матрица, структурная перестановка, синхронная и асинхронная перестановка, преобразование Уолша-Адамара.

The synthesis method for constructing full class of bent-functions of six variables based on the sign coding matrices, structural, synchronous and asynchronous permutations applied to the theory of Agievich bent-squares is proposed. The resulting full class of bent-functions can be used to solve many problems in the theory of information transmission, error-correcting coding, cryptography and cryptanalysis.

Keywords: bent-function, Agievich bent-square, sign coding matrix, structure permutation, synchronous and asynchronous permutation, Walsh-Hadamard transform.

*Памяти д.т.н., профессора
Михаила Ивановича Мазуркова*

Введение

Бент-функции со времени своего введения О. Ротхаусом [1] представляют интерес для многих исследователей в виду своей огромной области применения в современных информационных технологиях, в частности, в криптологии. Бент-функции также находят свое применение в задачах построения сигналов с расширенным спектром, в теории кодирования и в комбинаторике [2]. Бент-функции, будучи максимально удаленными от аффинных булевых функций, являются сложным комбинаторным объектом: в настоящее время нет даже оценок их количества для числа переменных $k > 8$. Тем не менее, основной задачей теории бент-функций является построение методов синтеза их полных классов.

Булевы бент-функции чаще всего определяют через их таблицы истинности, называемые бент-последовательностями. В соответствии с определением [3], бинарная последовательность $B = [b_0, b_1, \dots, b_i, \dots, b_{n-1}]$ длины $n = 2^{2l} = N^2$, где $b_i \in \{\pm 1\}$, $i = 0, n-1$ – коэффициенты, называется бент-последовательностью, если она имеет равномерный по модулю спектр Уолша – Адамара $W_B(\omega)$, который представим в матричной форме $W_B(\omega) = BA$, $\omega = 0, n-1$, где A – матрица Уолша – Адамара порядка n .

Исходя из определения бент-функций, каждый спектральный коэффициент бент-последовательности $W_B(\omega = 0), W_B(\omega = 1), \dots, W_B(\omega = n-1)$ принимает значение из множества $\{\pm N\}$.

Одним из наиболее универсальных методов построения бент-последовательностей длины n является конструкция Майорана-МакФарланда, которая основана на конкатенации строк матрицы Адамара A порядка N , а также всех возможных $N!$ перестановок её строк и 2^N знаковых кодирований, в свою очередь, матрица Адамара A каждого следующего порядка 2^l строится в соответствии с рекуррентным правилом [4]

$$A_{2^l} = \begin{bmatrix} A_{2^{l-1}} & A_{2^{l-1}} \\ A_{2^{l-1}} & -A_{2^{l-1}} \end{bmatrix}, \text{ где } A_1 = 1. \quad (0.1)$$

Очевидно, число бент-последовательностей, которые могут быть получены таким образом, определяется выражением $J = 2^N N!$.

Известен также регулярный метод синтеза полных классов бент-функций от $k = 4$ переменных [5], основанный на четырех специальных обобщённых опорных матрицах, для которых определены правила заполнения, что позволяет строить бент-функции, минуя перебор. Тем не менее, оказывается, что для большего числа переменных число подобных опорных конструкций становится велико, что затрудняет дальнейшее развитие подобного метода.

Для синтеза полных классов бент-функций следующей длины $n = 64$ был разработан конструктивный метод, основанный на свойствах преобразования Рида-Маллера [6], однако, его применение связано с вычислительными затруднениями, что диктует необходимость более строгого математического описания полного класса бент-функций этой длины путем создания соответствующих методов синтеза.

Как показали исследования, лучшим математическим базисом для разработки подобных методов синтеза является теория бент-квадратов (БК), разработанная С. Агиевичем [7].

Для каждой бент-функции может быть найден соответствующий ей бент-квадрат. Бент-квадратом назовем матрицу S порядка N , каждой строкой и каждым столбцом которой является спектральный вектор (коэффициенты преобразования Уолша – Адамара бинарной последовательности). Строки бент-квадрата получаются в результате умножения сегмента бент-последовательности длины N на матрицу Адамара порядка N $S_i = B_i \cdot A_N$, где S_i – i -я строка бент-квадрата S ; B_i – i -й сегмент бент-последовательности.

В работе [7] показано, что для длины бент-последовательностей $n = 64$ существует 8 структур, неэквивалентных с точки зрения перестановок по строкам и столбцам и знаковых кодирований бент-квадратов:

$$\begin{aligned}
 S^1 &= \begin{bmatrix} 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 8 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 8 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 8 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 8 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 8 \end{bmatrix}, \\
 S^2 &= \begin{bmatrix} -4 & 4 & 4 & 4 & 0 & 0 & 0 & 0 \\ 4 & -4 & 4 & 4 & 0 & 0 & 0 & 0 \\ 4 & 4 & -4 & 4 & 0 & 0 & 0 & 0 \\ 4 & 4 & 4 & -4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 8 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 8 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 8 \end{bmatrix}, \quad (0.2) \\
 S^3 &= \begin{bmatrix} -4 & 4 & 4 & 4 & 0 & 0 & 0 & 0 \\ 4 & -4 & 4 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & -4 & 4 & 4 & 4 & 0 & 0 \\ 0 & 0 & 4 & -4 & 4 & 4 & 0 & 0 \\ 4 & 4 & 0 & 0 & -4 & 4 & 0 & 0 \\ 4 & 4 & 0 & 0 & 4 & -4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 8 \end{bmatrix}, \\
 S^4 &= \begin{bmatrix} -4 & 4 & 4 & 4 & 0 & 0 & 0 & 0 \\ 4 & -4 & 0 & 0 & 4 & 4 & 0 & 0 \\ 4 & 0 & -4 & 0 & 4 & 0 & 4 & 0 \\ 4 & 0 & 0 & -4 & 0 & 4 & 4 & 0 \\ 0 & 4 & 4 & 0 & 0 & 4 & -4 & 0 \\ 0 & 4 & 0 & 4 & -4 & 0 & 4 & 0 \\ 0 & 0 & 4 & 4 & 4 & -4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 8 \end{bmatrix},
 \end{aligned}$$

$$\begin{aligned}
 S^5 &= \begin{bmatrix} -4 & 4 & 4 & 4 & 0 & 0 & 0 & 0 \\ 4 & -4 & 4 & 4 & 0 & 0 & 0 & 0 \\ 4 & 4 & -4 & 4 & 0 & 0 & 0 & 0 \\ 4 & 4 & 4 & -4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -4 & 4 & 4 & 4 \\ 0 & 0 & 0 & 0 & 4 & -4 & 4 & 4 \\ 0 & 0 & 0 & 0 & 4 & 4 & -4 & 4 \\ 0 & 0 & 0 & 0 & 4 & 4 & 4 & -4 \end{bmatrix}, \\
 S^6 &= \begin{bmatrix} -4 & 4 & 4 & 4 & 0 & 0 & 0 & 0 \\ 4 & -4 & 4 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & -4 & 4 & 4 & 4 & 0 & 0 \\ 0 & 0 & 4 & -4 & 4 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & -4 & 4 & 4 & 4 \\ 0 & 0 & 0 & 0 & 4 & -4 & 4 & 4 \\ 4 & 4 & 0 & 0 & 0 & 0 & -4 & 4 \\ 4 & 4 & 0 & 0 & 0 & 0 & 4 & -4 \end{bmatrix}, \\
 S^7 &= \begin{bmatrix} -4 & 4 & 4 & 4 & 0 & 0 & 0 & 0 \\ 4 & -4 & 0 & 0 & 4 & 4 & 0 & 0 \\ 4 & 0 & -4 & 0 & 4 & 0 & 4 & 0 \\ 4 & 0 & 0 & -4 & 0 & 4 & 4 & 0 \\ 0 & 4 & 4 & 0 & -4 & 0 & 0 & 4 \\ 0 & 4 & 0 & 4 & 0 & -4 & 0 & 4 \\ 0 & 0 & 4 & 4 & 0 & 0 & -4 & 4 \\ 0 & 0 & 0 & 0 & 4 & 4 & 4 & -4 \end{bmatrix}, \\
 S^8 &= \begin{bmatrix} -6 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & -6 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & -6 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & -6 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & -6 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & -6 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & -6 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & -6 \end{bmatrix}.
 \end{aligned}$$

С. Агиевичем была указана возможность построения бент-последовательностей длины $n = 64$ с помощью операций перестановок по строкам и столбцам и знакового кодирования бент-квадратов (0.2), однако, конкретные правила перестановок и знаковых кодирований показаны не были.

Целью настоящей статьи является разработка регулярных правил перестановок и знаковых кодирований строк и столбцов бент-квадратов Агиевича для построения полного класса бент-последовательностей длины $n = 64$.

1 Основные принципы выполнения операций перестановок и кодирований

Рассмотрим основные принципы выполнения операций перестановок по строкам и столбцам, а также знаковых кодирований, для чего введем несколько базовых определений.

Определение 1.1. Знакокодирующей бинарной матрицей назовем такую матрицу Z порядка N , у которой каждая строка и столбец представляют собой функцию Уолша [4] длины N .

Очевидно, для $N = 2$ все существующие бинарные матрицы являются знакокодирующими

$$\begin{aligned}
 & \begin{bmatrix} + & + \\ + & + \end{bmatrix} \begin{bmatrix} + & + \\ - & + \end{bmatrix} \begin{bmatrix} + & - \\ + & + \end{bmatrix} \begin{bmatrix} + & - \\ - & + \end{bmatrix} \\
 & \begin{bmatrix} - & + \\ + & + \end{bmatrix} \begin{bmatrix} - & + \\ - & + \end{bmatrix} \begin{bmatrix} - & - \\ + & + \end{bmatrix} \begin{bmatrix} - & - \\ - & + \end{bmatrix}
 \end{aligned}$$

$$\begin{bmatrix} + & + \\ + & - \end{bmatrix} \begin{bmatrix} + & + \\ - & - \end{bmatrix} \begin{bmatrix} + & - \\ + & - \end{bmatrix} \begin{bmatrix} + & - \\ - & - \end{bmatrix}, \quad (1.1)$$

где, для краткости, под символом «+» понимается +1, а под символом «-» – значение -1.

Для построения всех знакокодирующих матриц 4×4 представим их в общем виде

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \quad (1.2)$$

где $\alpha, \beta, \gamma, \delta$ – знакокодирующие матрицы из (1.1).

Выбор такого вида матриц $\alpha, \beta, \gamma, \delta$, чтобы конструкция (1.2) была знакокодирующей матрицей, должен происходить таким образом, чтобы все строки и столбцы (1.2) были функциями Уолша длины $N = 4$, т. е. совпадали бы с одной из следующих строк

$$\begin{bmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \\ - & - & - & - \\ - & + & - & + \\ - & - & + & + \\ - & + & + & - \end{bmatrix}.$$

Получить выполнение этого условия возможно в том случае, если в качестве матрицы β использовать знаковые кодирования функциями Уолша строк матрицы α , тогда как в качестве матрицы γ использовать знаковые кодирования функциями Уолша столбцов матрицы α , следя за выполнением определения знакокодирующей матрицы.

В качестве матрицы δ можно взять поэлементное произведение остальных матриц $\delta = \alpha \cdot \beta \cdot \gamma$ или его инверсию. В соответствии с приведенными выше выкладками, оценивается число возможных комбинаций матриц $\alpha, \beta, \gamma, \delta$ в конструкции (1.2)

$$\begin{bmatrix} 16 & 4 \\ 4 & 2 \end{bmatrix},$$

таким образом, знакокодирующих матриц порядка $N = 4$ существует $J_4 = 16 \cdot 4 \cdot 4 \cdot 2 = 512$. Аналогичным образом $J_8 = 512 \cdot 8 \cdot 8 \cdot 2 = 65536$, $J_{16} = 2^{16} \cdot 2^4 \cdot 2^4 \cdot 2 = 2^{25}$.

Рассмотрим базовые принципы проведения перестановок строк и столбцов бент-квадратов. Пусть V_8 – линейное векторное пространство $J = 2^k = 2^8 = 256$ векторов v_i длины $k = 8$. Тогда элементы этого пространства в бинарном виде

$$V_8 = \left\{ \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & + & + & + & + & + & + & - \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ - & - & - & - & - & - & - & - \end{bmatrix} \right\}.$$

Для каждого элемента данного пространства единственным образом определяется спектральный вектор (коэффициенты преобразования Уолша – Адамара) как произведение

$$W_i = v_i \cdot A,$$

где A – матрица Уолша – Адамара порядка $N = 8$, построенная в соответствии с (0.1).

Среди всего полученного множества спектральных векторов W_i можно выделить три класса (где в круглых скобках указано количество позиций, в которых число перед скобками встречается среди элементов вектора):

- 1) векторы, компонентами которых являются числа $\{\pm 6(1), \pm 2(7)\}$, которых существует 128 штук;
- 2) векторы, компонентами которых являются числа $\{\pm 8(1), 0(7)\}$, которых существует 16 штук;
- 3) векторы, компонентами которых являются числа $\{\pm 4(4), 0(4)\}$, которых существует 112 штук.

Определение 1.2. *Позиционной структурой спектрального вектора называются номера позиций, на которых расположены ненулевые компоненты.*

Найдены множества таких векторов из третьего класса, каждый вектор внутри которого имел бы различную позиционную структуру. Эти векторы представлены в матрице слева, позиционные структуры – в матрице справа

$$\begin{bmatrix} -4 & 4 & 4 & 4 & 0 & 0 & 0 & 0 \\ -4 & 4 & 0 & 0 & 4 & 4 & 0 & 0 \\ -4 & 4 & 0 & 0 & 0 & 0 & -4 & -4 \\ -4 & 0 & 4 & 0 & 4 & 0 & 4 & 0 \\ -4 & 0 & 4 & 0 & 0 & -4 & 0 & -4 \\ -4 & 0 & 0 & -4 & 4 & 0 & 0 & -4 \\ -4 & 0 & 0 & 4 & 0 & -4 & -4 & 0 \\ 0 & 4 & 4 & 0 & 4 & 0 & 0 & -4 \\ 0 & 4 & 4 & 0 & 0 & 4 & -4 & 0 \\ 0 & 4 & 0 & 4 & 4 & 0 & -4 & 0 \\ 0 & 4 & 0 & -4 & 0 & -4 & 0 & -4 \\ 0 & 0 & 4 & 4 & 4 & -4 & 0 & 0 \\ 0 & 0 & 4 & -4 & 0 & 0 & -4 & -4 \\ 0 & 0 & 0 & 0 & 4 & -4 & -4 & -4 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 5 & 6 \\ 1 & 2 & 7 & 8 \\ 1 & 3 & 5 & 7 \\ 1 & 3 & 5 & 8 \\ 1 & 4 & 6 & 8 \\ 1 & 4 & 6 & 7 \\ 2 & 3 & 5 & 8 \\ 2 & 3 & 6 & 7 \\ 2 & 4 & 5 & 7 \\ 2 & 4 & 6 & 8 \\ 3 & 4 & 5 & 6 \\ 3 & 4 & 7 & 8 \\ 5 & 6 & 7 & 8 \end{bmatrix}.$$

Например, для первой структуры выписаны все четырнадцать правил структурных перестановок

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 5 & 6 & 3 & 4 & 7 & 8 \\ 1 & 2 & 5 & 6 & 7 & 8 & 3 & 4 \\ 1 & 5 & 2 & 6 & 3 & 7 & 4 & 8 \\ 1 & 5 & 2 & 6 & 7 & 3 & 8 & 4 \\ 1 & 5 & 6 & 2 & 3 & 7 & 8 & 4 \\ 1 & 5 & 6 & 2 & 7 & 3 & 4 & 8 \end{bmatrix} \quad (1.3)$$

$$\begin{bmatrix} 5 & 1 & 2 & 6 & 3 & 7 & 8 & 4 \\ 5 & 1 & 2 & 6 & 7 & 3 & 4 & 8 \\ 5 & 1 & 6 & 2 & 3 & 7 & 4 & 8 \\ 5 & 1 & 6 & 2 & 7 & 3 & 8 & 4 \\ 5 & 6 & 1 & 2 & 3 & 4 & 7 & 8 \\ 5 & 6 & 1 & 2 & 7 & 8 & 3 & 4 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \end{bmatrix}.$$

Определение 1.3. Синхронные и асинхронные перестановки. Для столбцов или строк матрицы размера 4×4 существует всего $4! = 24$ различных способов перестановок строк и столбцов

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 1 & 2 & 4 & 3 & 1 & 3 & 2 & 4 & 1 & 3 & 4 & 2 & 1 & 4 & 2 & 3 & 1 & 4 & 3 & 2 \\ 2 & 1 & 3 & 4 & 2 & 1 & 4 & 3 & 2 & 3 & 1 & 4 & 2 & 3 & 4 & 1 & 2 & 4 & 1 & 3 & 2 & 4 & 3 & 1 \\ 3 & 1 & 2 & 4 & 3 & 1 & 4 & 2 & 3 & 2 & 1 & 4 & 3 & 2 & 4 & 1 & 3 & 4 & 1 & 2 & 3 & 4 & 2 & 1 \\ 4 & 1 & 2 & 3 & 4 & 1 & 3 & 2 & 4 & 2 & 1 & 3 & 4 & 2 & 3 & 1 & 4 & 3 & 1 & 2 & 4 & 3 & 2 & 1 \end{bmatrix} \quad (1.4)$$

Перестановку строк или столбцов матрицы порядка 8 мы можем представить как суперпозицию двух перестановок из (1.4)

$$\left[\begin{array}{cccc|cccc} c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_8 \end{array} \right], \quad (1.5)$$

где столбцы $c_1 \dots c_4$ могут быть переставлены, соответственно, $4!$ различными способами из (1.4), тогда как столбцы $c_5 \dots c_8$ должны переставляться синхронно со столбцами $c_1 \dots c_4$, т. е. для каждой перестановки $c_1 \dots c_4$, соответствующие номера старших столбцов определяются как

$$\begin{cases} c_5 = c_1 + 4; \\ c_6 = c_2 + 4; \\ c_7 = c_3 + 4; \\ c_8 = c_4 + 4, \end{cases}$$

такую перестановку будем называть **синхронной**.

Исследования показали, что также возможны и **асинхронные** перестановки столбцов, когда первые столбцы $c_1 \dots c_4$ выбираются из $4!$ различных перестановок, тогда как старшие столбцы $c_5 \dots c_8$ могут быть подвергнуты диадному сдвигу [8], т. е. одной из 4-х комбинаций

$$\begin{cases} c_5 & c_6 & c_7 & c_8 \\ c_6 & c_5 & c_8 & c_7 \\ c_7 & c_8 & c_5 & c_6 \\ c_8 & c_7 & c_6 & c_5 \end{cases} \quad (1.6)$$

Далее, последовательно рассмотрены все восемь бент-квадратов (0.2) и для каждого представлены свои специфические правила перестановок строк и столбцов, а также знаковых кодирований, основанные на ранее введенных основных определениях.

2 Бент-квадраты Агиевича

Первый бент-квадрат Агиевича S_1 представляет собой известную ранее конструкцию Майорана-МакФарланда, где матрица S_1 является матрицей циркулянта. Полное множество бент-функций, соответствующих структуре S_1 , может быть получено путем всех возможных знаковых кодирований строк (или столбцов), которых существует $J_{Z1} = 256 = 2^8$, а также всех возможных перестановок по строкам (или по столбцам), которых может быть выполнено $J_{P1} = 8! = 40320 = 2^7 \cdot 3^2 \cdot 5 \cdot 7$. Отметим, что, поскольку

структура S_1 является матрицей циркулянта, все перестановки по строкам эквиваленты перестановкам по столбцам.

Итого, количество бент-функций, соответствующих первой структуре, достигает

$$J_1 = 2^{15} \cdot 3^2 \cdot 5 \cdot 7.$$

Второй бент-квадрат Агиевича S_2 . Для выполнения операции знакового кодирования используем знакокодирующие матрицы. Бент-квадрат структуры S_2 может быть представлен в виде обобщенной структуры

$$\begin{bmatrix} \alpha_2 & \beta_2 \\ \gamma_2 & \delta_2 \end{bmatrix},$$

где $\alpha_2, \beta_2, \gamma_2, \delta_2$ – матрицы четвертого порядка.

Знаковые кодирования допускают только структуры α_2 и δ_2 . В соответствии с правилами построения знакокодирующих матриц, структура α_2 допускает $512 = 2^9$ различных вариантов знаковых кодирований, тогда как структура δ_2 допускает только 2^4 вариантов знаковых кодирований по строкам (или по столбцам). Таким образом, с помощью знаковых кодирований получаем $J_{Z2} = 2^{13}$ различных бент-последовательностей.

Рассмотрим алгоритм выполнения перестановок бент-квадрата структуры S_2 . Структура δ_2 допускает $24 = 2^3 \cdot 3$ перестановок по строкам или по столбцам, тогда как перестановки в структуре α_2 не требуются исходя из того, что все они поглощаются знаковыми кодированиями. Перестановки между структурами $\alpha_2, \beta_2, \gamma_2, \delta_2$ выполняются в соответствии с найденными четырнадцатью правилами

$$\left[\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 5 & 6 & 3 & 4 & 7 & 8 \\ 1 & 2 & 5 & 6 & 7 & 8 & 3 & 4 \\ 1 & 5 & 2 & 6 & 3 & 7 & 4 & 8 \\ 1 & 5 & 2 & 6 & 7 & 3 & 8 & 4 \\ 1 & 5 & 6 & 2 & 3 & 7 & 8 & 4 \\ 1 & 5 & 6 & 2 & 7 & 3 & 4 & 8 \end{array} \right] \left[\begin{array}{cccccccc} 5 & 1 & 6 & 2 & 7 & 3 & 8 & 4 \\ 5 & 1 & 6 & 2 & 3 & 7 & 4 & 8 \\ 5 & 6 & 1 & 2 & 7 & 8 & 3 & 4 \\ 5 & 6 & 1 & 2 & 3 & 4 & 7 & 8 \\ 5 & 1 & 2 & 6 & 7 & 3 & 4 & 8 \\ 5 & 1 & 2 & 6 & 3 & 7 & 8 & 4 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \end{array} \right],$$

которые используются как для перестановок по строкам, так и для перестановок по столбцам, причем пересечения структур при этом не происходит. Объем возможных перестановок составляет $J_{P2} = 24 \cdot 14^2$. Таким образом, полный объем бент-функций, которые могут быть получены на основе бент-квадрата S_2 , равняется $J_2 = 2^9 \cdot 2^4 \cdot 24 \cdot 14^2 = 2^{18} \cdot 3 \cdot 7^2$.

Третий бент-квадрат Агиевича S_3 . Для использования подхода к знаковому кодированию, основанному на знакокодирующих матрицах, рассмотрим бент-квадрат структуры S_3 в виде следующей обобщенной матрицы

$$\left[\begin{array}{cc|cc} a_3 & b_3 & 0 & 0 \\ 0 & c_3 & d_3 & 0 \\ \hline e_3 & 0 & f_3 & 0 \\ 0 & 0 & 0 & g_3 \end{array} \right],$$

где $a_3, b_3, c_3, d_3, e_3, f_3, g_3$ – матрицы второго порядка.

В соответствии с правилом построения знакокодирующих матриц, a_3 допускает 16 различных вариантов, тогда как b_3 должно быть всеми возможными знаковыми кодированиями матрицы a_3 , т. е. допускает только 4 варианта. Матрица c_3 должна быть знаковыми кодированиями столбцов матрицы b_3 , что также допускает 4 варианта её выбора. В соответствии с правилом построения знакокодирующих матриц правый верхний квадрант должен быть всеми возможными знаковыми кодированиями строк левого верхнего. Т. е., матрица d_3 может принимать значения всех возможных построчных знаковых кодирований матрицы c_3 . Аналогично, матрица f_3 должна быть знаковыми кодированиями столбцов матрицы d_3 , тогда как матрица e_3 допускает только 2 значения – прямое и инверсное. Матрица g_3 , имеет всего 4 возможных варианта знакового кодирования. Итого, мы имеем

$$\left[\begin{array}{cc|cc} 2^4 & 2^2 & 0 & 0 \\ 0 & 2^2 & 2^2 & 0 \\ \hline 2 & 0 & 2^2 & 0 \\ 0 & 0 & 0 & 2^2 \end{array} \right],$$

или всего $J_{23} = 2^{15}$ знаковых кодирований.

Рассмотрим алгоритм выполнения перестановок по строкам и столбцам в виде конкретных шагов:

Шаг 1. Перестановки по строкам.

Выполнение всех $8! = 40320$ перестановок по строкам показывает, что только 2688 перестановок исходной матрицы структуры S_3 приводят к новому бент-квадрату. Однако, только 336 имеют уникальные позиционные структуры. Из них можно выделить 26 базовых перестановок, на основе которых могут быть получены все остальные

$$\left[\begin{array}{cccccccc|cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 & 3 & 5 & 7 & 8 & 6 & 4 & 2 \\ 1 & 2 & 3 & 4 & 6 & 5 & 8 & 7 & 1 & 3 & 5 & 8 & 2 & 4 & 6 & 7 \\ 1 & 2 & 3 & 4 & 7 & 8 & 5 & 6 & 1 & 3 & 5 & 8 & 4 & 2 & 7 & 6 \\ 1 & 2 & 3 & 4 & 8 & 7 & 6 & 5 & 1 & 3 & 5 & 8 & 6 & 7 & 2 & 4 \\ 1 & 2 & 5 & 6 & 3 & 4 & 8 & 7 & 1 & 3 & 5 & 8 & 7 & 6 & 4 & 2 \\ 1 & 2 & 5 & 6 & 4 & 3 & 7 & 8 & 3 & 4 & 5 & 6 & 1 & 2 & 8 & 7 \\ 1 & 2 & 5 & 6 & 7 & 8 & 4 & 3 & 3 & 4 & 5 & 6 & 2 & 1 & 7 & 8 \\ 1 & 2 & 5 & 6 & 8 & 7 & 3 & 4 & 3 & 4 & 5 & 6 & 7 & 8 & 2 & 1 \\ 1 & 2 & 7 & 8 & 3 & 4 & 6 & 5 & 3 & 4 & 5 & 6 & 8 & 7 & 1 & 2 \\ 1 & 2 & 7 & 8 & 6 & 5 & 3 & 4 & 3 & 4 & 7 & 8 & 1 & 2 & 6 & 5 \\ 1 & 3 & 5 & 7 & 2 & 4 & 6 & 8 & 3 & 4 & 7 & 8 & 6 & 5 & 1 & 2 \\ 1 & 3 & 5 & 7 & 4 & 2 & 8 & 6 & 5 & 6 & 7 & 8 & 1 & 2 & 4 & 3 \\ 1 & 3 & 5 & 7 & 6 & 8 & 2 & 4 & 5 & 6 & 7 & 8 & 4 & 3 & 1 & 2 \end{array} \right]$$

Остальные перестановки могут быть получены из базовых перестановок путем синхронных перестановок, выполненных в соответствии с таблицей правил размножения опорных перестановок.

Таблица 2.1 – Правила размножения опорных перестановок бент-квадрата S_3

Опорные перестановки	Правила размножения	Получаемый объем
1, 2, 3, 4, 5, 6, 7, 8, 19, 20, 21, 22	1 2 3 4 1 3 2 4 1 3 4 2 3 1 2 4 3 1 4 2 3 4 1 2	$6 \cdot 12 = 72$
9, 10, 23, 24, 25, 26	1 2 3 4 1 2 4 3 1 3 2 4 1 3 4 2 1 4 2 3 1 4 3 2 3 1 2 4 3 1 4 2 3 4 1 2 4 1 2 3 4 1 3 2 4 3 1 2	$6 \cdot 12 = 72$
11, 12, 13, 14, 15, 16, 17, 18	Все возможные перестановки	$8 \cdot 24 = 192$
Сумма перестановок		336

Шаг 2. Нахождение перестановок по столбцам, которые не поглощаются перестановками по строкам. Очевидно, выполнив все полученные 336 перестановок по строкам и перестановок по столбцам, мы получаем 336^2 бент-квадратов, но только 9408 обладают уникальным набором позиционных структур. Итого, несовпадающие – каждая $336^2 / 9408 = 12$ -я.

Таким образом, существует 28 базовых перестановок по столбцам, которые при суперпозиции с каждой из перестановок по строкам не приводят к появлению эквивалентных позиционных структур

$$\left[\begin{array}{cccccccc|cccccccc} 7 & 8 & 1 & 2 & 3 & 4 & 5 & 6 & 1 & 3 & 7 & 5 & 6 & 8 & 4 & 2 \\ 7 & 1 & 8 & 2 & 3 & 5 & 4 & 6 & 1 & 3 & 7 & 5 & 4 & 2 & 6 & 8 \\ 7 & 1 & 3 & 5 & 8 & 2 & 4 & 6 & 1 & 3 & 7 & 5 & 2 & 4 & 8 & 6 \\ 7 & 1 & 3 & 5 & 6 & 4 & 2 & 8 & 1 & 3 & 5 & 7 & 8 & 6 & 4 & 2 \\ 7 & 1 & 3 & 5 & 4 & 6 & 8 & 2 & 1 & 3 & 5 & 7 & 6 & 8 & 2 & 4 \\ 7 & 1 & 3 & 5 & 2 & 8 & 6 & 4 & 1 & 3 & 5 & 7 & 4 & 2 & 8 & 6 \\ 7 & 1 & 2 & 8 & 3 & 5 & 6 & 4 & 1 & 3 & 5 & 7 & 2 & 4 & 6 & 8 \\ 1 & 7 & 8 & 2 & 3 & 5 & 6 & 4 & 1 & 3 & 4 & 2 & 7 & 5 & 6 & 8 \\ 1 & 7 & 3 & 5 & 8 & 2 & 6 & 4 & 1 & 3 & 4 & 2 & 5 & 7 & 8 & 6 \\ 1 & 7 & 3 & 5 & 6 & 4 & 8 & 2 & 1 & 3 & 2 & 4 & 7 & 5 & 8 & 6 \\ 1 & 7 & 3 & 5 & 4 & 6 & 2 & 8 & 1 & 3 & 2 & 4 & 5 & 7 & 6 & 8 \\ 1 & 7 & 3 & 5 & 2 & 8 & 4 & 6 & 1 & 2 & 7 & 8 & 3 & 4 & 5 & 6 \\ 1 & 7 & 2 & 8 & 3 & 5 & 4 & 6 & 1 & 2 & 3 & 4 & 7 & 8 & 5 & 6 \\ 1 & 3 & 7 & 5 & 8 & 6 & 2 & 4 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{array} \right] \cdot (2.1)$$

Итого, полный объем перестановок $J_{P3} = 336 \cdot 28 = 9408 = 2^6 \cdot 3 \cdot 7^2$, тогда как количество

всех бент-функций, которые могут быть построены на основе бент-квадрата структуры S_3 , составляет $J_3 = 2^{21} \cdot 3 \cdot 7^2$.

Четвертый бент-квадрат Агиевича S_4 . В соответствии с подходом, основанным на знакокодирующих матрицах, представим бент-квадрат S_4 в обобщенном виде

$$\begin{bmatrix} \alpha_4 & \beta_4 \\ \gamma_4 & \delta_4 \end{bmatrix},$$

где $\alpha_4, \beta_4, \gamma_4, \delta_4$ – матрицы четвертого порядка.

Определим возможные знаковые кодирования матрицы α_4 , для чего продолжим обобщение

$$\alpha_4 = \begin{bmatrix} -4 & 4 & 4 & 4 \\ 4 & -4 & 0 & 0 \\ 4 & 0 & -4 & 0 \\ 4 & 0 & 0 & -4 \end{bmatrix} = \begin{bmatrix} a_4 & b_4 \\ c_4 & d_4 \end{bmatrix} \Rightarrow \begin{bmatrix} 2^4 & 2 \\ 2 & 2^2 \end{bmatrix},$$

где a_4, b_4, c_4, d_4 – матрицы второго порядка.

Верхняя строка b_4 принимает значения, являющиеся знаковым кодированием верхней строки a_4 . Левый столбец c_4 принимает значения, являющиеся знаковым кодированием левого столбца a_4 , а матрица d_4 допускает все возможные знаковые кодирования.

Матрица β_4 состоит из 3-х строк, каждая из которых является знаковым кодированием соответствующих строк α_4 , которых может быть 2^3 . Аналогично, матрица γ_4 является знаковым кодированием соответствующих столбцов α_4 . Их также может быть 2^3 . Матрица δ_4 допускает только инверсный или прямой вариант своих 3-х строк, а также отрицательный или положительный элемент 8, т.е. всего 2^2 значений. Итого $\begin{bmatrix} 2^8 & 2^3 \\ 2^3 & 2^2 \end{bmatrix}$, таким образом, $J_{Z_4} = 2^{16}$.

Выполнение всех возможных $8! = 40320$ перестановок по строкам показывает, что только 1344 из них приводят к формированию новых бент-квадратов. Экспериментальные данные по применению этих перестановок как по строкам, так и по столбцам приводят к выводу, что всего существуют $10752 = 2^9 \cdot 3 \cdot 7$ новых позиционных структур, т.е. каждая 168-я является уникальной.

Представим исходную структуру S_4 в виде двух структур, разделив матрицу на две равные части сначала по вертикали, а затем и по горизонтали $S_4 = [G_1 | H_1] = \begin{bmatrix} G_2 \\ H_2 \end{bmatrix}$.

Перестановки по строкам сначала матрицы G_1 , в соответствии с правилом синхронных и асинхронных перестановок, дают 96 различных

структур бент-квадратов, а затем выполнение 14 базовых для данной структуры перестановок

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 5 & 6 & 3 & 4 & 7 & 8 \\ 1 & 2 & 7 & 8 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 7 & 2 & 4 & 6 & 8 \\ 1 & 3 & 6 & 8 & 2 & 4 & 5 & 7 \\ 1 & 4 & 5 & 8 & 2 & 3 & 6 & 7 \\ 1 & 4 & 6 & 7 & 2 & 3 & 5 & 8 \end{bmatrix}, \begin{bmatrix} 2 & 3 & 5 & 8 & 1 & 4 & 6 & 7 \\ 2 & 3 & 6 & 7 & 1 & 4 & 5 & 8 \\ 2 & 4 & 5 & 7 & 1 & 3 & 6 & 8 \\ 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 \\ 3 & 4 & 5 & 6 & 1 & 2 & 7 & 8 \\ 3 & 4 & 7 & 8 & 1 & 2 & 5 & 6 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \end{bmatrix},$$

дает 1344 перестановки по строкам.

И далее, выписывая все перестановки по столбцам, которые не приводят к появлению повторяющихся позиционных структур, получаем

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 6 & 5 & 8 & 7 \\ 1 & 2 & 3 & 4 & 7 & 8 & 5 & 6 \\ 1 & 2 & 3 & 4 & 8 & 7 & 6 & 5 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 7 & 8 & 4 & 3 & 6 & 5 \\ 1 & 2 & 8 & 7 & 4 & 3 & 5 & 6 \\ 1 & 8 & 2 & 7 & 4 & 5 & 3 & 6 \\ 8 & 1 & 2 & 7 & 4 & 5 & 6 & 3 \end{bmatrix}.$$

Итого, объем допустимых перестановок составляет $J_{P_4} = 2^6 \cdot 3 \cdot 7 \cdot 2^3$, тогда как общий объем бент-функций, которые могут быть построены на основе бент-квадрата Агиевича структуры S_4 , составляет $J_4 = 2^{16} \cdot 2^6 \cdot 3 \cdot 7 \cdot 2^3 = 2^{25} \cdot 3 \cdot 7$.

Пятый бент-квадрат Агиевича S_5 . Для осуществления знакового кодирования матрицы S_5 представим её в обобщенном виде

$$\begin{bmatrix} \alpha_5 & 0 \\ 0 & \alpha_5 \end{bmatrix},$$

где α_5 – матрица четвертого порядка.

Все позиции в матрицах α_5 являются активными, что, в соответствии с определением знакокодирующих матриц, приводит к объему возможных знаковых кодирований

$$\begin{bmatrix} 2^9 & 0 \\ 0 & 2^9 \end{bmatrix}, \text{ т. е. } J_{Z_5} = 2^{18}.$$

Выполняя все $8! = 40320$ перестановок по строкам, устанавливаем, что только 8064 перестановки приводят к формированию нового бент-квадрата, но только 14 из них, приведенные в (1.3), приводят к формированию неповторяющихся структур бент-квадратов.

Для выполнения перестановок по столбцам может быть рассмотрена позиционная структура матрицы S_5

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 \end{bmatrix}.$$

Матрица S_5 состоит из двух различных позиционных структур. Ясно, что перестановка 5-го и 1-го столбца, а также 6-го и 2-го, 7-го и 3-го, 8-го и 4-го будут абсолютно эквивалентными некоторой другой перестановке столбцов и перестановке

строк. Например, применение одной из перестановок из (1.3) [5 1 2 6 3 7 8 4] приводит к формированию бент-квадрата

$$\begin{bmatrix} 0 & -4 & 4 & 0 & 4 & 0 & 0 & 4 \\ 0 & 4 & -4 & 0 & 4 & 0 & 0 & 4 \\ 0 & 4 & 4 & 0 & -4 & 0 & 0 & 4 \\ 0 & 4 & 4 & 0 & 4 & 0 & 0 & -4 \\ -4 & 0 & 0 & 4 & 0 & 4 & 4 & 0 \\ 4 & 0 & 0 & -4 & 0 & 4 & 4 & 0 \\ 4 & 0 & 0 & 4 & 0 & -4 & 4 & 0 \\ 4 & 0 & 0 & 4 & 0 & 4 & -4 & 0 \end{bmatrix},$$

что является эквивалентным применению перестановки по столбцам [1 5 6 2 7 3 4 8] и перестановки по строкам [5 6 7 8 1 2 3 4]. Аналогичным образом, не прибегая к перебору, можно показать, что все другие из вторых 7-ми перестановок из (1.3) эквивалентны одной из первых 7-ми перестановок из (1.3) и некоторой перестановке по строкам.

Таким образом, выполняя перестановки по строкам и по столбцам, можем получить $J_{P_5} = 14 \cdot 7 = 98 = 2 \cdot 7^2$ новых бент-функций, соответствующих бент-квадрату структуры S_5 , тогда как общий объем всех бент-функций, соответствующих этой структуре, достигает $J_5 = 2^{18} \cdot 2 \cdot 7^2 = 2^{19} \cdot 7^2$.

Шестой бент-квадрат Агиевича S_6 . Для применения знакокодирующих матриц к структуре бент-квадрата S_6 удобно представить его в следующем обобщенном виде

$$\begin{bmatrix} \alpha_6 & \beta_6 \\ \gamma_6 & \delta_6 \end{bmatrix} = \begin{bmatrix} a_6 & b_6 & 0 & 0 \\ 0 & c_6 & d_6 & 0 \\ 0 & 0 & e_6 & f_6 \\ h_6 & 0 & 0 & g_6 \end{bmatrix},$$

где $\alpha_6, \beta_6, \gamma_6, \delta_6$ – матрицы четвертого порядка, $a_6, b_6, c_6, d_6, e_6, f_6, g_6, h_6$ – матрицы второго порядка.

Матрица a_6 допускает 16 значений, матрица b_6 – 4, знаковые кодирования строк матрицы a_6 . Матрица c_6 – знаковые кодирования столбцов матрицы b_6 . Матрица d_6 – знаковые кодирования строк матрицы c_6 . Матрица e_6 – знаковые кодирования столбцов матрицы d_6 . Матрица f_6 – знаковые кодирования строк матрицы e_6 . Матрица g_6 – знаковые кодирования столбцов матрицы f_6 . Матрица h_6 принимает только 2 варианта, прямой и инверсный. Таким образом, имеем

$$\begin{bmatrix} 2^4 & 2^2 & 0 & 0 \\ 0 & 2^2 & 2^2 & 0 \\ 0 & 0 & 2^2 & 2^2 \\ 2 & 0 & 0 & 2^2 \end{bmatrix},$$

т. е. общее число бент-функций, которые могут быть построены с помощью знаковых кодирований бент-квадрата структуры S_6 , составляет $J_{Z_6} = 2^{17}$.

Выполнение всех 40320 перестановок по строкам показывает, что 2688 перестановок приводят к формированию нового бент-квадрата, тогда как только $168 = 2^3 \cdot 3 \cdot 7$ из них имеют уникальные структуры. Данные перестановки могут быть сформированы регулярным способом, для чего исходный бент-квадрат S_6 может быть представлен в виде обобщенной структуры

$$\begin{bmatrix} a_6 \\ b_6 \\ c_6 \\ d_6 \end{bmatrix}, \tag{2.2}$$

где каждая из строк a_6, b_6, c_6, d_6 эквивалентна двум строкам исходного бент-квадрата S_6 . Для структуры (2.2) допустимы $4! = 24$ перестановки и 7 объединяющих перестановок для полученного множества бент-квадратов

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 7 & 6 & 8 \\ 1 & 2 & 3 & 4 & 5 & 7 & 8 & 6 \\ 1 & 2 & 3 & 5 & 4 & 6 & 7 & 8 \\ 1 & 2 & 3 & 5 & 4 & 7 & 6 & 8 \\ 1 & 2 & 3 & 5 & 4 & 7 & 8 & 6 \\ 1 & 2 & 3 & 5 & 6 & 4 & 7 & 8 \end{bmatrix},$$

что дает 168 искомым перестановок по строкам.

Правила перестановок по столбцам определяются несколькими из 28-ми базовых перестановок (2.1), а также правилами их размножения (таблица 2.2).

Таблица 2.2 – Правила перестановок по столбцам бент-квадрата S_6

Опорные перестановки	Правила размножения	Получаемый объем
1 2 3 4 5 6 7 8	Синхронные перестановки 4 3 2 1 4 2 3 1 4 2 1 3 Асинхронные перестановки 1 2 3 4 3 4 1 2	$2 \cdot 3 = 6$
1 2 5 6 3 4 8 7	Синхронные перестановки 4 3 2 1 4 2 3 1 4 2 1 3 Асинхронные перестановки 1 2 3 4	$3 \cdot 1 = 3$

Продолжение таблицы 2.2

Опорные перестановки	Правила размножения	Получаемый объем
1 3 5 7 4 2 8 6	Синхронные перестановки	12
	4 3 2 1	
	4 3 1 2	
	4 2 3 1	
	Асинхронные перестановки	
	1 2 3 4	
	2 1 4 3	
	3 4 1 2	
	4 3 2 1	

Таким образом, с помощью перестановок по строкам и столбцам можно получить $J_{P_6} = 168 \cdot 21 = 3528 = 2^3 \cdot 3^2 \cdot 7^2$ бент-функций, основанных на бент-квадрате структуры S_6 , тогда как общий объем бент-функций, основанных на бент-квадрате структуры S_6 , составляет $J_6 = 2^{20} \cdot 3^2 \cdot 7^2$.

Седьмой бент-квадрат Агиевича S_7 . Для применения подхода к знаковому кодированию бент-квадратов, основанного на закодирующих матрицах, удобно представить структуру S_7 в виде следующей обобщенной матрицы

$$\begin{bmatrix} a_7 & b_7 & c_7 & d_7 \\ e_7 & f_7 & g_7 & h_7 \\ i_7 & k_7 & l_7 & m_7 \\ n_7 & o_7 & p_7 & q_7 \end{bmatrix},$$

где $a_7, b_7, c_7, d_7, e_7, f_7, g_7, h_7, i_7, k_7, l_7, m_7, n_7, o_7, p_7, q_7$ – матрицы второго порядка.

Рассмотрим отдельно каждую структуру:

- 1) матрица a_7 допускает 16 вариантов знакового кодирования;
- 2) матрица b_7 – 2 варианта – прямая и инверсная первая строка матрицы a_7 ;
- 3) матрица e_7 – 2 варианта – прямой и инверсный первый столбец матрицы a_7 ;
- 4) матрица f_7 – все 4 доступных варианта;
- 5) матрица $\begin{bmatrix} c_7 & d_7 \\ g_7 & h_7 \end{bmatrix}$ – 8 вариантов знаковых кодирований последних 3-х строк матрицы $\begin{bmatrix} a_7 & b_7 \\ e_7 & f_7 \end{bmatrix}$;
- 6) матрица $\begin{bmatrix} i_7 & k_7 \\ n_7 & o_7 \end{bmatrix}$ – 8 вариантов знаковых кодирований последних 3-х столбцов матрицы $\begin{bmatrix} a_7 & b_7 \\ e_7 & f_7 \end{bmatrix}$;

$$7) \text{ матрица } \begin{bmatrix} l_7 & m_7 \\ p_7 & q_7 \end{bmatrix} = \begin{bmatrix} \overline{-4} & 0 & 0 & \overline{4} \\ 0 & \overline{-4} & 0 & \overline{4} \\ 0 & 0 & \overline{-4} & \overline{4} \\ \overline{4} & \overline{4} & \overline{4} & \overline{-4} \end{bmatrix}$$

является сложной, содержит 3 прямоугольника, которые допускают знаковые кодирования (представимы в прямом или инверсном виде), соответственно, допускает 2^3 знаковых кодирований.

Всего знаковых кодирований существует

$$\begin{bmatrix} 2^8 & 2^3 \\ 2^3 & 2^3 \end{bmatrix}, \text{ т. е. } J_{Z7} = 2^{17}.$$

Выполнение синхронных (1.5), а также асинхронных (1.6) перестановок по строкам позволяет сформировать $96 = 2^5 \cdot 3$ уникальных структур бент-квадратов структуры S_7 , к каждой из которых применимы перестановки (1.3), что дает $14 \cdot 96 = 1344$ уникальных бент-квадрата.

К каждой из полученных 1344-х перестановок могут быть применены базовые перестановки по столбцам, использование которых не приводит к появлению повторяющихся структур

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 8 & 7 & 6 & 5 & 4 & 3 \\ 3 & 2 & 8 & 5 & 7 & 6 & 4 & 1 \\ 4 & 5 & 1 & 8 & 2 & 7 & 3 & 6 \\ 5 & 6 & 1 & 2 & 4 & 3 & 8 & 7 \\ 6 & 7 & 3 & 2 & 4 & 1 & 5 & 8 \\ 7 & 8 & 5 & 6 & 4 & 3 & 2 & 1 \end{bmatrix}.$$

Таким образом, с помощью перестановок по строкам и столбцам можно получить $J_{P7} = 7 \cdot 1344 = 9408 = 2^6 \cdot 3 \cdot 7^2$ бент-функций, основанных на бент-квадрате структуры S_7 . Следовательно, общий объем бент-функций, основанных на бент-квадрате структуры S_7 , составляет $J_7 = 2^{17} \cdot 2^6 \cdot 3 \cdot 7^2 = 2^{23} \cdot 3 \cdot 7^2$.

Восьмой бент-квадрат Агиевича S_8 . Для выполнения операции знакового кодирования целесообразно использовать закодирующие матрицы порядка $N = 8$, которых существует $J_{Z8} = J_8 = 2^{16}$ штук. Для выполнения операций перестановок по строкам (или по столбцам) могут быть применены все $J_{P8} = 8! = 40320 = 2^7 \cdot 3^2 \cdot 5 \cdot 7$ существующих перестановок. Поскольку бент-квадрат структуры S_8 является матрицей циркулянтном, все перестановки по столбцам поглощаются перестановками по строкам.

Таким образом, общий объем бент-функций, основанных на бент-квадрате структуры S_8 , составляет $J_8 = 2^{23} \cdot 3^2 \cdot 5 \cdot 7$.

Таблица 2.3 суммирует результаты по разработанным правилам знакового кодирования и перестановкам строк и столбцов.

Анализируя результаты таблицы 2.3 нетрудно установить, что общее число синтезированных бент-функций

$$J_{bent64} = 5\,425\,430\,528,$$

что составляет полный класс всех бент-функций шести переменных.

Таблица 2.3 – Характеристики бент-квадратов

Номер бент-квадрата							
1	2	3	4	5	6	7	8
Количество знаковых кодирований							
2^8	2^{13}	2^{15}	2^{16}	2^{18}	2^{17}	2^{17}	2^{16}
Количество перестановок в виде множителей							
$2^7 \cdot 3^2 \cdot 5 \cdot 7$	$2^5 \cdot 3 \cdot 7^2$	$2^6 \cdot 3 \cdot 7^2$	$2^9 \cdot 3 \cdot 7$	$2 \cdot 7^2$	$2^3 \cdot 3^2 \cdot 7^2$	$2^6 \cdot 3 \cdot 7^2$	$2^7 \cdot 3^2 \cdot 5 \cdot 7$
Количество перестановок							
40320	4704	9408	10752	98	3528	9408	40320
Количество бент-последовательностей в эквивалентном классе							
$2^{15} \cdot 3^2 \cdot 5 \cdot 7$	$2^{18} \cdot 3 \cdot 7^2$	$2^{21} \cdot 3 \cdot 7^2$	$2^{25} \cdot 3 \cdot 7$	$2^{19} \cdot 7^2$	$2^{20} \cdot 3^2 \cdot 7^2$	$2^{23} \cdot 3 \cdot 7^2$	$2^{23} \cdot 3^2 \cdot 5 \cdot 7$

Заключение

Отметим основные результаты проведенных исследований:

– впервые предложены определения и разработаны методы синтеза знакокодирующих матриц, структурных перестановок, а также синхронных и асинхронных перестановок применительно к теории бент-квадратов Агиевича;

– получила дальнейшее развитие теория бент-квадратов Агиевича, в результате чего разработаны регулярные правила знаковых кодирований и перестановок по строкам и по столбцам всех восьми бент-квадратов Агиевича порядка $N = 8$;

– регулярными методами синтезирован полный класс бент-функций шести переменных.

Таким образом, разработанные методы, позволяющие синтез бент-функций, минуя переборные операции, являются существенным развитием теории бент-функций, могут быть применены в современных технологиях передачи информации, помехоустойчивом кодировании, а также в криптографии.

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. Соколов, А.В. Конструктивный метод синтеза нелинейных S-блоков подстановки, соответствующих строгому лавинному критерию / А.В. Соколов // Известия высших учебных заведений. Радиоэлектроника. – 2013. – Т. 56, № 8. – С. 43–52.

3. Токарева, Н.Н. Бент-функции: результаты и приложения. Обзор работ / Н.Н. Токарева // Приклад. дискрет. математика. – Томск, 2009. – Сер. № 1 (3). – С. 15–37.

4. Мазурков, М.И. Системы широкополосной радиосвязи / М.И. Мазурков // Одесса: Наука и Техника. – 2010. – 340 с.

5. Мазурков, М.И. Регулярные правила построения полного класса бент-последовательностей длины 16 / М.И. Мазурков, А.В. Соколов // Пр. Одес. політехн. ун-ту. – 2013. – № 2 (41). – С. 231–237.

6. Qingshu, Meng A novel algorithm enumerating bent functions / Qingshu Meng, Min Yang, Huanguo Zhang, Jingsong Cui // Discrete Mathematics. – 2008. – Vol. 308, № 23. – P. 5576–5584.

7. 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.

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

Поступила в редакцию 22.07.15.