УДК 681.3.06

МАЗУРКОВ М.И., СОКОЛОВ А.В.

КОНСТРУКТИВНЫЙ МЕТОД СИНТЕЗА ПОЛНЫХ КЛАССОВ МНОГОУРОВНЕВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЕ БРЕЙНА

Одесский национальный политехнический университет.
Украина, Одесса, 65044, пр. Шевченко 1

Аннотация. Введены две новые формы представления многоуровневых последовательностей де Брейна (ПБ) в виде геометрической и алгебраической структуры, найдены практически привлекательные свойства этих структур, и на этой основе предложен конструктивный метод синтеза образующих и полных классов ПБ. Показано приложение найденных классов четверичных ПБ в задачах шифрования, с целью уменьшения в 2 раза объема памяти для хранения криптографических таблиц замен.

Abstract. Two new submission forms of multilevel de Bruijn sequences (BS) as geometric and algebraic structure are introduced, the practically useful properties of these structures are determined, and on this basis a constructive synthesis method of forming and full BS classes is offered. The practical usage of the found BS classes in problems of encoding is revealed, which allow a reduction of cryptographic substitution boxes storage memory size by a factor of 2.

Ключевые слова: многоуровневые числовые последовательности, свойство серий, геометрическая структура, алгебраическая структура, кортеж, образующие классы, полные классы, циклический сдвиг, зеркальное отображение, шифрование, криптографические таблицы замен, multilevel numerical sequences, property of a series, geometric structure, algebraic structure, tuple, forming classes, full classes, circular shift, mirror map, encoding, cryptographic S-boxes.

Последовательности де Брейна (кратко ПБ) [1-3] нашли многочисленные применения в задачах радиолокации и связи, а также в задачах криптографии, в частности, в качестве гамм или ключевых потоков в поточных шифрах. Характерной особенностью ПБ является то, что они в максимальной степени приближаются к случайным последовательностям, имеют нормальное распределение серий, сбалансированы, обладают высокой непредсказуемостью.

Хорошо известна оценка объема $W_{\text{обр}}$ образующих классов ПБ произвольной длины $N = m^n$, над алфавитом из m элементов (чисел), для произвольного натурального n [4]

$$W_{\text{обр}} = [(m-1)!]^{m^n-1} m^{m^{n-1}-n}. \qquad (1)$$

Заметим однако, что оценка (1) показывает только существование образующего класса ПБ и не дает конструктивного метода их построения (подобно известным теоремам К.Э. Шеннона существования хороших корректирующих кодов). Таким образом, вопросы конструктивного построения образующих и полных классов многоуровневых ПБ не получили удовлетворительного решения и требуют дальнейшего исследования.

В данной статье выбран новый подход к решению проблемы синтеза полных классов многоуровневых ПБ, сущность которого состоит в том, что каждая ПБ описывается с помощью двух форм: геометрической структуры и алгебраической структуры. На основе учета свойств этих структур предложен конструктивный метод синтеза полных классов многоуровневых ПБ, что, по-сути, является основной целью работы. Далее рассматриваются вопросы применения построенных классов ПБ для построения экономичных схем S-блоков подстановки и криптографических таблиц замен блочных шифров.

Перейдем непосредственно к изложению материала статьи. По определению, каждая m-ичная последовательность де Брейна (ПБ), длины $N = m^n$, где m-основание ПБ, n-разрядность состояния (число ячеек памяти условного генератора), должна отображать на замкнутом цикле точно N различных между собой состояний. Например, если основание

$m=4$ (элементы $\{0,1,2,3\}$), а $n=2$, то все $N=4^2=16$ состояний ПБ разместим в $m=4$ хранилищах и представим их в виде следующей алгебраической конструкции

Состояния	Хранилище	Состояния	Хранилище
[00] 01 02 03	№1	20 21 [22] 23	№3
10 [11] 12 13	№2	30 31 32 [33]	№4

. (2)

Конструкция (2) представляет собой достаточно удобный объект для конструктивного построения различных множеств ПБ, даже ручным способом. Состояния ПБ с одинаковыми числами в каждой из n ячеек памяти условно назовем стационарными. В конструкции (2) стационарные состояния отмечены в прямоугольниках.

Определение 1. Геометрической структурой ПБ, длины $N=m^n$, назовем такой вектор $T=[\tau_1,\tau_2,\cdots,\tau_m]$, у которого координаты τ_i определяют расстояния (число элементов) между каждыми двумя соседними стационарными состояниями на замкнутом цикле ПБ, при этом сумма координат вектора T

$$\sum_{i=1}^{m}\tau_i=m^n-mn. \tag{3}$$

Например, общий вид геометрической структуры произвольной ПБ, длины $N=4^2=16$, на замкнутом цикле, представим в виде следующей конструкции

$$00 \overset{\tau_1}{\longleftrightarrow} 11 \overset{\tau_2}{\longleftrightarrow} 22 \overset{\tau_3}{\longleftrightarrow} 33 \overset{\tau_4}{\longleftrightarrow} 00, \tag{4}$$

которая определена с точностью до места и порядка расположения стационарных состояний. Проведенные исследования позволили установить ряд свойств геометрических структур:

Утверждение 1. Полное множество геометрических структур объема Γ_{Π}, всех ПБ, длины $N=m^n$, представляет собой всевозможные наборы векторов $T_i=\{\tau_{i,k}\}$, $k=\overline{1,m}$, каждый из которых удовлетворяет единственному ограничению (3), и, следовательно, полное множество геометрических структур строится конструктивно. Для ПБ, длины $N=4^2=16$, находим $\Gamma_{\Pi}=165$.

Утверждение 2. Пусть заданная геометрическая структура $T_i=\{\tau_{i,k}\}$, $k=\overline{1,m}$, определяет подмножество ПБ объема J, тогда каждый циклический сдвиг и каждое непоглащенное циклическим сдвигом зеркальное отображение заданной структуры T_i определяет новое подмножество ПБ, такого же объема J, при этом новое подмножество ПБ нетрудно сформировать на основе ранее построенного подмножества ПБ.

Заметим, что для ряда геометрических структур операция циклического сдвига поглощает операцию зеркального отображения, существуют также геометрические структуры с меньшим, чем m периодом цикличности. Определим эквивалентный класс геометрических структур как множество $\{T_i\}$, объема $J_{\text{экв}}$, полученных из заданной T_i, путем операций циклического сдвига и зеркального отображения. Очевидно, что каждый эквивалентный класс строится конструктивно. Выберем из каждого эквивалентного класса по одной геометрической структуре, в результате получим образующий класс геометрических структур, который обозначим через $\Gamma_{\text{обр}}$, а его объем $J_{\text{обр}}$. Для ПБ, длины $N=4^2=16$, находим значения $\Gamma_{\text{обр}}$

и $J_{\text{экв}}$, которые представлены в табл.1. Из анализа данных табл.1 устанавливаем, что объем множества образующих структур $J_{\text{обр}} = 29$.

Таблица 1

$\Gamma_{\text{обр}}$	$J_{\text{экв}}$	$w_{\text{обр}}$	$\Gamma_{\text{обр}}$	$J_{\text{экв}}$	$w_{\text{обр}}$	$\Gamma_{\text{обр}}$	$J_{\text{экв}}$	$w_{\text{обр}}$
0008	4	216	0152	8	102	1115	4	36
0017	8	204	0161	4	72	1124	8	48
0026	8	162	0206	4	156	1133	4	60
0035	8	186	0215	8	120	1214	4	72
0044	4	192	0224	8	126	1223	8	66
0107	4	144	0233	8	114	1313	2	24
0116	8	114	0305	4	192	0323	4	156
0125	8	126	0241	4	168	1232	4	120
0134	8	96	0404	2	120	2222	1	96
0143	8	150	0314	8	138	–	–	–

Каждый фиксированный вектор T_i, при фиксированном порядке следования стационарных состояний, определяет собой подмножество точно из $w_{\text{обр}}$ ПБ (табл.1). Рассмотрим этот вопрос более полно. Методика и пример конструктивного построения подмножеств ПБ, объема $w_{\text{обр}}$, машинным или ручным способом, состоит в следующем:

Шаг 1. Выбираем вид геометрической структуры ПБ и фиксируем порядок следования стационарных состояний. Например, пусть $T_1 = [0,0,0,8]$, а порядок следования стационарных состояний – $[0,0,1,1,2,2,3,3]$.

Шаг 2. Представляем конструктивно каждую ПБ в виде объединения двух ее частей: стационарной части (3) и связывающего стационарную часть кортежа, длины (2). В нашем примере получаем следующую структуру: $\text{ПБ}_1 = [0,0,1,1,2,2,3,3,\text{кортеж}]$, в других случаях кортеж может быть распределенным, т.е. вложенным в стационарную часть.

Шаг 3. Построить первый подходящий кортеж длины (2), начиная с наименьших подходящих элементов из диапазона $\{0,1,2,\cdots,m-1\}$, при которых выполняется свойство серий ПБ. Здесь весьма удобно воспользоваться вспомогательной алгебраической конструкцией (2), где, переходя от хранилища к хранилищу, будут сформированы все N состояний ПБ, а все тупиковые кортежи будут отброшены по ходу их появления. Теперь легко получаем, что в нашем примере $\text{ПБ}_1 = [0,0,1,1,2,2,3,3,0,2,0,3,1,3,2,1]$. Нетрудно убедиться, что на замкнутом цикле ПБ_1 наблюдается точно $N = 16$ различных между собой состояний.

Продолжая построения других кортежей, устанавливаем, что при фиксированной геометрической структуре $T_1 = [0,0,0,8]$, и фиксированном порядке следования стационарных состояний – $[0,0,1,1,2,2,3,3]$, существует точно 36 ПБ, которые представлены в табл.2.

Таблица 2

0011223302031321	0011223303213102	0011223313032021	0011223320302131
0011223302032131	0011223310203213	0011223313032102	0011223320310213
0011223302103132	0011223310213032	0011223313202103	0011223320313021
0011223302131032	0011223310213203	0011223313203021	0011223321020313
0011223302132031	0011223310302132	0011223313210203	0011223321031302
0011223303102132	0011223310320213	0011223313210302	0011223321302031
0011223303132021	0011223310321302	0011223320210313	0011223321303102
0011223303132102	0011223313020321	0011223320213031	0011223321310203
0011223303202131	0011223313021032	0011223320213103	0011223321310302

На основе найденных 36 ПБ (табл.2), нетрудно построить точно по 36 новых структур ПБ для каждого из следующих пяти новых порядков следования стационарных состояний ПБ

$$\begin{bmatrix} 0,0,1,1,3,3,2,2 \\ 0,0,2,2,1,1,3,3 \\ 0,0,2,2,3,3,1,1 \\ 0,0,3,3,1,1,2,2 \\ 0,0,3,3,2,2,1,1 \end{bmatrix}.$$

Итак, при фиксированном векторе $T_1 = [0,0,0,8]$, и фиксированном вначале ПБ нулевом стационарном состоянии, построено всего $w_{\text{обр}} = 6 \cdot 36 = 216$ образующих ПБ. Подобным образом найдены значения $w_{\text{обр}}$ (табл.2) для всех других фиксированных векторов T_i, при фиксированном вначале ПБ нулевом стационарном состоянии. На основе данных табл.2 находим, что объем $W_{\text{обр}}$ образующего класса четверичных ПБ, длины $N = 4^2 = 16$, определяется соотношением

$$W_{\text{обр}} = \sum_{i=1}^{29} w_{\text{обр},i} J_{\text{экв},i} = 20736, \qquad (5)$$

что полностью соответствует оценке (1) существования объема образующего класса ПБ [4]. Для нахождения полного класса ПБ, на основе образующего класса ПБ, воспользуемся следующими свойствами ПБ:

Утверждение 3. Каждая образующая ПБ порождает, путем всех ее циклических сдвигов, точно $N = m^n$ ПБ из полного класса.

Утверждение 4. Полный класс ПБ обладает тем свойством, что операции циклических сдвигов образующих ПБ_i полностью поглощают операции зеркального отображения образующих ПБ_k, для соответствующих пар чисел (i,k).

На основе (5), с учетом содержания *Утверждений 3* и *4*, построим полный класс четверичных ПБ длины $N = 4^2 = 16$, и найдем его объем

$$W_{\text{полн}} = NW_{\text{обр}} = 331776. \qquad (6)$$

Рассмотрим процесс построения S-блоков подстановки на основе четверичных ПБ. Основным этапом построения S-блока подстановки является задание кодирующей Q-последовательности, которая полностью описывает подстановочную конструкцию. Для нахождения Q-последовательности воспользуемся свойством серий ПБ. Подробная процедура получения, например, десятичной $Q = [15,13,6,10,8,1,5,4,0,2,11,12,3,14,9,7]$ кодирующей последовательности, на базе четверичной $\text{ПБ} = [3,3,1,2,2,0,1,1,0,0,2,3,0,3,2,1]$, проиллюстрирована с помощью рис.1.

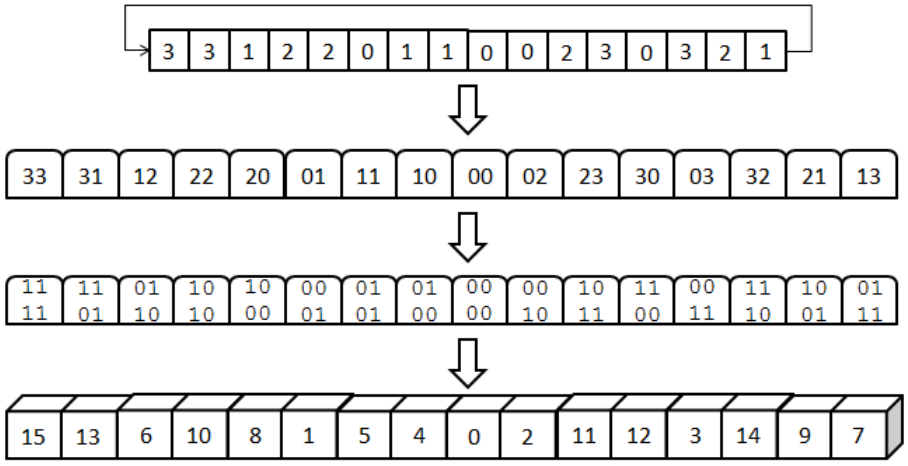

Рис.1

Анализ рис.1 показывает, что применение четверичных ПБ позволяет добиться экономии памяти, необходимой для хранения S-блока, в 2 раза. Так, в приведенном выше примере, для хранения десятичной кодирующей (шифрующей) последовательности Q, необходимо 64 бита памяти, тогда как для хранения четверичной ПБ достаточно всего 32 бита. Проведенный анализ показал, что в случае применения образующих классов двоичных ПБ, длины $N = 2^4 = 16$, можно добиться экономии памяти в 4 раза, однако при этом существенно уменьшается объем образующего класса двоичных ПБ, который составляет $W_{\text{обр}} = 256$.

Итак, получив кодирующую последовательность Q, запишем правило шифрования S-блока

$$\begin{bmatrix} \text{Вход} - X: 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ \text{Выход} - Y: 15 & 13 & 6 & 10 & 8 & 1 & 5 & 4 & 0 & 2 & 11 & 12 & 3 & 14 & 9 & 7 \end{bmatrix}. \tag{7}$$

Задачу количественной оценки криптографической стойкости [5,6,7] полученных S-блоков подстановки на основе четверичных ПБ сведем к исследованию, по крайней мере, следующих трех основных критериев качества:

1. Один из наиболее распространенных критериев качества S-блока подстановки состоит в том, чтобы каждый бит выходного вектора y_j являлся статистически независимым от каждого бита входного вектора x_i. Количественно степень линейной статистической (корреляционной) связи между выходными и входными битами описывают с помощью корреляционной матрицы $R = \| r_{i,j} \|$, $i, j = \overline{0, k-1}$, где коэффициенты корреляции

$$r_{i,j} = 1 - 2^{-(k-1)} \sum_{m=1}^{N} (x_{m,i} \oplus y_{m,j}), \quad i, j = \overline{0, k-1}. \tag{8}$$

Исследования подстановочной конструкции (7) показали, что её корреляционная матрица

$$R = \begin{bmatrix} -0.25 & 0 & 0.25 & 0 \\ 0 & 0 & -0.25 & 0.25 \\ 0.25 & 0.25 & 0 & -0.25 \\ 0 & 0 & -0.25 & 0 \end{bmatrix}. \tag{9}$$

2. Максимальное расстояние d_S нелинейности S-блока (7), которое определим как максимальное расстояние Хэмминга

$$d_S = \max(dist(Y_i, A_k)), \tag{10}$$

между булевыми функциями Y_i преобразования и всеми кодовыми словами A_k аффинного $A(N,k)$-кода, где, в общем случае, максимум отыскивается по всем видам преобразований.

3. Максимальный период T_S возврата S-блока (7) в исходное состояние, который определяется как максимальная величина наименьшего общего кратного (НОК) длин всех циклов подстановки, где максимум ищется по всем видам подстановок

$$T_S = \text{НОК}(5, 7, 4) = 140. \tag{11}$$

Объемы S-блоков (четверичных ПБ) с наилучшими криптографическими свойствами представлены в табл.3.

Таблица 3

Оцениваемый параметр	$\lvert r_{i,j} \rvert_{\max}$	d_S	T_S
Наилучшие значения оцениваемых параметров	0.25	4	140
Количество S-блоков (четверичных ПБ)	23008	218688	2281

Анализ данных табл.3 показывает достаточно высокую перспективность применения класса четверичных ПБ для построения подстановочных конструкций современных экономичных криптографических систем.

В заключение отметим впервые полученные результаты настоящей работы:

1. Введены две формы представления произвольных последовательностей Де Брейна (ПБ): в виде геометрической и алгебраической структур, найдены практически привлекательные свойства этих структур, и на этой основе разработан конструктивный метод синтеза образующих и полных классов многоуровневых ПБ.

2. Синтезирован полный класс четверичных ПБ и разработана методология использования четверичных ПБ для получения шифрующих S-блоков подстановки, которые полностью определяют построение таблиц подстановки современных блочных шифров, в частности ГОСТ 28147-89. Показано, что применение данного класса ПБ позволяет уменьшить требуемый объёма памяти таблицы подстановок в 2 раза.

3. Получены основные количественные оценки криптографической стойкости S-блоков подстановки на основе четверичных ПБ, которые свидетельствуют о достаточно высокой перспективности применения класса четверичных ПБ для построения подстановочных конструкций современных экономичных криптографических систем.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Клименко Н.Н.* Сигналы с расширением спектра в системах передачи информации / Н.Н. Клименко, В.В. Кисель, А.И. Замарин // Зарубежная электроника. 1983. — № 11. — С. 45—59.

2. *Стельмашенко Б.Г.* Нелинейные псевдослучайные последовательности в широкополосных системах передачи информации / Б.Г. Стельмашенко, П.Г. Тараненко // Зарубежная радиоэлектроника. 1988.— № 9. — С. 3—17.

3. *Хачатрян Л.Г.* Методы построения последовательностей де Брейна / Л.Г. Хачатрян // Дискретная математика, Математический институт им. В. А. Стеклова РАН, — 1991. — Том 3. — Выпуск 4. — С. 62—78.

4. *De Bruijn N.G.* A combitorial problem // Nederl. Akad. Wetensch. Proc. – 1946. – V. 49. – P. 758–764.

5. *Горбенко І.Д.* Дослідження аналітичних і статистичних властивостей булевих функцій криптоалгоритму RIJNDAEL (FIPS 197) / Горбенко І.Д., Потій О.В., Ізбенко Ю.А. // Харків: Всеукраїнський міжвідомчий науково-технічний збірник "Радіотехніка". — 2004 . — Том 126. — С. 132-138.

6. *Сергиенко Р.В.* Исследование криптографических свойств нелинейных узлов замены алгоритма симметричного шифрования ГОСТ 28147-89 / Р.В. Сергиенко, И.В. Московченко.– Харьков: Системы обработки информации. 2007. — Выпуск 8. — С. 91-95.

7. *Долгов В.И.* Подстановочные конструкции современных симметричных блочных шифров / Долгов В.И., Олейников Р.В., Лисицкая И.В., Сергиенко Р.В., Дроботько Е.В. Мельничук Е.Д. // Радіоелектронні і компютерні системи, ХНУРЭ, – 2009, – №6.– С.89-93.