О МНОЖЕСТВЕ ЛИНЕЙНЫХ И НЕЛИНЕЙНЫХ ТРОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ де БРЕЙНА ДЛИНОЙ $N = 9$

К. т. н. А. В. Соколов, О. И. Ефимов, А. И. Годунов

Одесский национальный политехнический университет
Украина, г. Одесса
radiosquid@gmail.com

С помощью регулярных правил синтезирован полный класс троичных последовательностей де Брейна длиной N=9. Проведены исследования его структурных свойств, которые показали, что он может быть порожден с помощью всего четырех исходных последовательностей: двух линейных и двух нелинейных. Синтезированные последовательности служат основой для построения экономичных S-блоков подстановки.

Ключевые слова: последовательность де Брейна, S-блок подстановки, многозначная логика.

Будучи известными еще в Древней Индии, последовательности де Брейна (ПБ) и сегодня являются важными совершенными алгебраическими конструкциями, которые нашли свое применение во многих задачах радиолокации и связи. В последнее время ПБ применяются также в качестве исходного материала для построения генераторов псевдослучайных ключевых последовательностей и экономичных схем *S*-блоков подстановки. Практическая ценность ПБ определила значительный интерес к ним со стороны современных исследователей.

Последовательность де Брейна длиной $N = q^k$ со свойством k-граммного распределения определим как такую, для которой полностью выполняется свойство серий, т. е. каждая серия из k элементов встречается на замкнутом цикле точно один раз [1]. Характерной особенностью ПБ является то, что они в максимальной степени приближаются к случайным последовательностям, имеют нормальное распределение серий, сбалансированы, обладают высокой непредсказуемостью.

Де Брейном была указана оценка мощностей $W_{\text{обр}}$ классов образующих последовательностей де Брейна

$$W_{\text{обр}} = (q!)^{q^{k-1}} \big/ q^k \,, \tag{1}$$

которая, тем не менее, показывает только существование образующего класса ПБ и не дает конструктивного метода их построения (подобно известным теоремам К. Э. Шеннона существования хороших корректирующих кодов).

В связи со стремительным развитием принципов многозначной логики и их имплементации в современных информационных технологиях особый интерес начали представлять, в частности, *S*-блоки подстановки, основанные на функциях многозначной логики и пригодные для построения полноценных криптографических алгоритмов. Так, для построения *S*-блоков подстановки длиной $N = 3^k$ в [2] предложено использование достаточно сложного математического аппарата конструкции Кима. Высококачественные *S*-блоки подстановки, однако, как показывает практика синтеза двоичных блоков замен, могут быть с успехом построены на основе ПБ. Более того, *S*-блоки, построенные на основе ПБ, характеризуются возможностями экономичного потребления используемой для их хранения памяти, что важно для мобильных платформ, а также при реализации параллельных вычислений. Тем не менее, для построения *S*-блоков подстановки первичной является задача синтеза полных классов последовательностей де Брейна, в данном случае троичных.

Единственной длиной троичных последовательностей де Брейна, для которой может быть применен переборный метод поиска, является длина $N = 3^k = 3^2 = 9$, поэтому особую важность представляет изучение свойств именно этого класса, чему и посвящена данная работа.

Отметим, что результаты работы [3] позволяют разделить полное множество последовательностей де Брейна на линейные и нелинейные. Линейную последовательность де Брейна можно постро-

ить на базе *M*-последовательности с генераторным полиномом $h(x)$ степени $k = \deg h(x)$ путем добавления одного нуля к серии, состоящей из $k-1$ нулей. Так, количество существующих первообразных полиномов определяется формулой

$$\left| f_q^k \right| = \varphi(q^k - 1)/k, \tag{2}$$

где φ — функция Эйлера.

В соответствии с выражением (2) число неприводимых полиномов для нашего случая $\left| f_3^2 \right| = 2$, каждый из которых порождает две соответствующие троичные ПБ:

$$\text{ПБ}_1 = \{001220211\}; \quad \text{ПБ}_2 = \{001120221\}. \tag{3}$$

Проведенные исследования показали, что размножение троичных последовательностей де Брейна подчиняется следующим правилам.

Правило 1. Представив исходные ПБ (3) в виде обобщенных структур, например $\text{ПБ}_1 = \{\beta_0\beta_0\beta_1\beta_2\beta_2\beta_0\beta_2\beta_1\beta_1\}$, и подставляя различные уникальные значения β_i из множества {0, 1, 2}, получаем новые ПБ. Перестановки значений β_i могут быть выполнены, соответственно, 3! = 6 способами.

Правило 2 [1]. Множество всех ПБ может быть получено из множества образующих ПБ путем их циклического сдвига. Данное правило создает *N* новых последовательностей де Брейна на основе каждой образующей.

Таким образом, используя *Правило 1*, на основе линейных последовательностей де Брейна (3) возможно построить множество из $W_{1\text{обр}} = 12$ образующих ПБ. Тем не менее, в соответствии с выражением (1), существует 24 образующие последовательности де Брейна, т. е. еще 12 нелинейных, которые могут быть построены на основе *Правила 1* из следующих двух нелинейных ПБ

$$\text{ПБ}_1 = \{001021122\}; \quad \text{ПБ}_2 = \{001102122\}. \tag{4}$$

На основе построенных 24 образующих ПБ путем применения *Правила 2* может быть построен полный класс троичных ПБ мощностью $J = 24 \cdot 9 = 216$.

Расчеты в соответствии с (1) и (3) позволяют сделать выводы о соотношении мощностей классов линейных и нелинейных ПБ с ростом их длины. Например, для длины ПБ $N = 27$ существует $J_{lin} = 4$ линейных ПБ и $J_{nl} = 373244$ нелинейных. Таким образом, с ростом длины *N* мощность класса нелинейных ПБ растет значительно быстрее, что обосновывает задачу усовершенствования методов синтеза нелинейных ПБ.

Таким образом, в настоящей работе проведено исследование полного класса ПБ длиной $N = 9$ и установлено, что он порождается двумя линейными и двумя нелинейными образующими ПБ, которые при использовании *Правила 1* порождают все остальные образующие ПБ.

Найденные троичные ПБ являются исходным материалом для конструирования криптографических конструкций, а также для использования в других телекоммуникационных приложениях. Использованный подход, при дальнейшем усовершенствовании, может быть адаптирован для описания классов троичных ПБ большей длины.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. De Bruijn N.G. A combinatorial problem // Nederl. Akad. Wetensch. Proc.— 1946.— Vol. 49.— P. 758–764.

2. Жданов О.Н., Соколов А.В. Алгоритм построения оптимальных по критерию нулевой корреляции недвоичных блоков замен // Проблемы физики, математики и техники.— 2015.— № 3(24). — С. 94–97.

3. Мазурков М.И., Соколов А.В. Методы синтеза двоичных псевдослучайных последовательностей со свойством *k*-граммного распределения // Труды ОНПУ.— 2012.— С. 188 — 198.

A. V. Sokolov, O. I. Efimov, A. I. Godunov

On the set of linear and nonlinear ternary de Bruijn sequences of length *N* = 9

This paper is devoted to the problem of development of regular synthesis rules of a complete class of de Bruijn ternary sequences. We performed classification of synthesized sequences according to their structural properties, which showed that they can be generated with the help of only four initial sequences: two linear sequences and two nonlinear ones. Synthesized sequences are the basis for building efficient S-boxes.

Keywords: de Bruijn sequence, S-box, many-valued logic.