

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 структур. Найдены практически привлекательные свойства этих структур, и на этой основе предложен конструктивный метод синтеза образующих и полных классов ПБ. Показано применение найденных классов четверичных ПБ в задачах шифрования с целью уменьшения в 2 раза объема памяти для хранения криптографических таблиц замен

**Ключевые слова:** многоуровневая числовая последовательность, свойство серий, геометрическая структура, алгебраическая структура, кортеж, образующий класс, полный класс, циклический сдвиг, зеркальное отображение, шифрование, криптографическая таблица замен

**ВВЕДЕНИЕ**

Последовательности де Брейна (ПБ) [1–3] нашли применение 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, и обладают высокой непредсказуемостью.

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]

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

Однако оценка (1) показывает только существование образующего класса ПБ и не дает конструктивного метода их построения, по-

добно 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 предложен 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 создан конструктивный метод синтеза полных классов многоуровневых ПБ, что является основной целью работы. Рассмотрены вопросы применения построенных классов ПБ для построения экономических схем  $S$ -блоков подстановки и криптографических таблиц замен блочных шифров.

Электронный вариант статьи: <http://radio.kpi.ua/article/view/S0021347013010044>