ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
МАТЕМАТИКИ
Том 19 **Выпуск 3**
2012

Ф. К. Алиев, **А. В. Зайцева**, **В. А. Киселенко**, **А. Г. Сенцов** (Москва, ТВП, МГТУ, ИНМЭ РАН). **О возможности генерации подстановок с использованием генераторов скользящих перестановок.**

Пусть r и n – такие натуральные числа, что $n \geqslant r$. Обозначим E_r множество всех таких n мерных двоичных векторов $\mathbf{e}_k = (e_{1k}, e_{2k}, \ldots, e_{nk})$, что $e_{1k} = 1$, $S_j = e_{1k} + e_{2k} + \cdots + e_{jk}$, $S_n = r$.

Определим на этом множестве совокупность отображений $\{h_i \,|\, i = 0, 1, \ldots, r-1\}$ следующим образом:

$$h_i(\mathbf{e}_k) = \begin{cases} (1, e_{1k}, e_{2k}, \ldots, e_{n-1,k}), & \text{если} \quad e_{nk} = 1, \\ (1, e_{1k}, e_{2k}, \ldots, e_{j-1,k}, 0, e_{j+1,k}, \ldots, e_{n-1,k}), & \text{если} \quad e_{nk} = 0,\ e_{jk} = 1 \\ & \text{и} \quad S_j = i + 1. \end{cases}$$

Определим также совокупность отображений $\{f_i \,|\, i = 0, 1, \ldots, r-1\}$, $f_i : E_r \to \mathbf{Z}/n$, где $\mathbf{Z}/n$ – кольцо вычетов целых чисел по модулю n, следующим образом:

$$f_i(\mathbf{e}_k) = \begin{cases} n-1, & \text{если} \quad e_{nk} = 1, \\ j-1, & \text{если} \quad e_{nk} = 0,\ S_j = i+1,\ e_{jk} = 1. \end{cases}$$

Пусть $A(n, r) = (X, Q, Y, h, f)$ — такой автомат Мили [5], что входной алфавит $X = \mathbf{Z}/r$ — кольцо вычетов целых чисел по модулю r, множество состояний $Q = E_r$, выходной алфавит $Y = \mathbf{Z}/n$ — кольцо вычетов целых чисел по модулю n, функция переходов $h : X \times Q \to Q$, $h(i, q) = h_i(q)$ для любых $i \in X$, $q \in Q$, функция выходов $f : X \times Q \to Y$, $f(i, q) = f_i(q)$ для любых $i \in X$, $q \in Q$.

В работах [1] и [2] автомат $A(n, r)$ используется как теоретико-автоматная модель генератора скользящих перестановок, применяемых в криптографических приложениях. В работах [3] и [4] рассматриваются вопросы, связанные с использованием автомата $A(n, r)$ в стеганографических приложениях.

Далее при проведении арифметических вычислений элементы выходного алфавита Y автомата $A(n, r)$ считаем целыми числами из множества $\{0, 1, \ldots, n-1\}$.

Если $\{y_i\}_{i=1}^t$ — выходная последовательность длины $t \in \mathbf{N}$ ($\mathbf{N}$ – множество натуральных чисел) автомата $A(n, r)$ с начальным состоянием $q_1 = (\underbrace{11\ldots1}_{r}\underbrace{00\ldots0}_{n-r})$, соответствующая входной последовательности $\{x_i\}_{i=1}^t$, то определим отображение $\varphi_{\{x_i\}_{i=1}^t} : \{1, 2, \ldots, t\} \to \mathbf{Z}$ ($\mathbf{Z}$ — множество целых чисел), положив $\varphi_{\{x_i\}_{i=1}^t}(k) = k + (r-1) - y_k$, $k \in \{1, 2, \ldots, t\}$.

Утверждение. *Отображение $\varphi_{\{x_i\}_{i=1}^t}$ является подстановкой на множестве $\{1, 2, \ldots, t\}$ тогда и только тогда, когда отображение $h_{x_1} h_{x_2} \cdots h_{x_t}$ принадлежит стабилизатору элемента q_1 в полугруппе $S_{A(n,r)}$ автомата $A(n, r)$.*

СПИСОК ЛИТЕРАТУРЫ

1. *Алиев Ф. К.* О сходимости матриц переходных вероятностей автоматов, определяющих преобразования скользящей перестановки. – В сб.: Третья Всероссийская школа-коллоквиум по стохастическим методам. М.: ТВП, 1996, с. 13–14.
2. *Алиев Ф. К.* О реализуемости вероятностных автоматов, определяющих скользящие перестановки, автоматами Мили со случайным входом. — В сб.: Третья Всероссийская школа-коллоквиум по стохастическим методам. М.: ТВП, 1996, с. 14–15.
3. *Киселенко В. А.* О периодических свойствах преобразований скользящей перестановки в связи со стеганографическими приложениями. — Обозрение прикл. и промышл. матем., 2005, т. 12, в. 4, с. 985–986.
4. *Киселенко В. А.* Об удельной энтропии выходных последовательностей автомата, определяющего преобразования скользящей перестановки, в связи со стеганографическими приложениями. — Обозрение прикл. и промышл. матем., 2006, т. 13, в. 5, с. 865–866.
5. *Фомичев В. М.* Дискретная математика и криптология. М.: ДИАЛОГ-МИФИ, 2003, 400 с.