ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 21 МАТЕМАТИКИ Выпуск 5
2014

Д. В. Шуваев (Москва, ТВП). **О подпоследовательностях цепей Маркова.**

Если из простой цепи Маркова вычеркнуть часть знаков, расположенных на заданных местах, то марковское свойство, очевидно, сохранится, хотя могут нарушится однородность и другие свойства. Если же места для вычеркивания выбираются случайно, то, как легко показать на примерах, может нарушится и марковское свойство. В докладе рассматривается один случай, когда после вычеркивания знаков на случайно выбранных местах в простой однородной цепи Маркова образуется опять же простая однородная цепь Маркова.

Рассмотрим две независимые случайные двоичные последовательности: простую однородную цепь Маркова $\mathbf{a} = (a_0, a_1, \ldots)$ и простую однородную цепь Маркова $\mathbf{s} = (s_0, s_1, \ldots)$ с состояниями 1 и 0 и матрицами переходных вероятностей

$$\begin{pmatrix} 1-\alpha & \alpha \\ \beta & 1-\beta \end{pmatrix}, \quad \begin{pmatrix} 1-p & p \\ q & 1-q \end{pmatrix}$$

соответственно. Уточним, что $q\,(p+q)^{-1}$ — вероятность единицы в стационарном распределении последовательности $\mathbf{s}$.

Образуем из последовательности $\mathbf{a}$ третью последовательность, вычеркнув знаки a_i при всех i таких, что $s_i = 0$.

Положим $R = (\alpha+\beta)+q\,(1-\alpha-\beta)$ и условимся, что $R > 0$ (иначе $\alpha = \beta = q = 0$ и построение не имеет смысла). Утверждается, что построенная последовательность — простая однородная цепь Маркова.

Теорема. *Матрица переходных вероятностей построенной цепи Маркова равна*

$$\begin{pmatrix} 1-\alpha & \alpha \\ \beta & 1-\beta \end{pmatrix} + \frac{p\,(1-\alpha-\beta)}{R} \begin{pmatrix} -\alpha & \alpha \\ \beta & -\beta \end{pmatrix}.$$

С прикладной точки зрения построенная последовательность — это выходная последовательность сжимающего генератора [1] с опорной последовательностью $\mathbf{a}$ и управляющей последовательностью $\mathbf{s}$.

Следствие. *Элементы построенной последовательности независимы тогда и только тогда, когда* $\alpha + \beta = 1$.

Замечание. Если $p + q = 1$, то элементы последовательности $\mathbf{s}$ независимы. Если $\alpha + \beta = 1$, то элементы последовательности $\mathbf{a}$ независимы.

Частный случай $\alpha = 1, \beta = 1$, когда $\mathbf{s}$ — знакопеременная последовательность $1, 0, 1, 0, \ldots$, рассматривался в [2]. Можно показать, что к этому случаю посредством подходящих переобозначений сводится задача из работы [3], в которой случайная последовательность строится несколько другим образом.

СПИСОК ЛИТЕРАТУРЫ

1. *Coppersmith D.*, *Krawczyk H.*, *Mansour Y.* The shrinking generator. — In: Advances in Cryptology — Crypto'93. 13th Annual International Cryptology Conference. (Santa Barbara, CA, August 22–26, 1993.) Proceedings./ Ed. by D.R. Stinson. N. Y. etc.: Springer, 1994, p. 22–39. (Ser. Lect. Notes Comput. Sci. V. 773.)
2. *Шуваев Д. В.* О некоторых вероятностных свойствах сжимающего генератора. — Обозрение прикл. и промышл. матем., 2012, т. 19, в. 3, с. 418–419.
3. *Максимов Ю. И.* Схема Бернулли с альтернирующими вставками. — В кн.: Труды по дискретной математике. Т. 2. М.: ТВП, 1998, с. 223–229.