О СПОСОБАХ УЛУЧШЕНИЯ СТАТИСТИТЕСКИХ СВОЙСТВ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ФИЗИЧЕСКИХ ГЕНЕРАТОРОВ

Е.В. Храмова

Белгосуниверситет, НИИ прикладных проблем математики и информатики,
, Независимости 4, 220050 Минск, Беларусь
KhramovaEV@bsu.by

При использовании физических генераторов случайных последовательностей, для получения последовательности наиболее близкой по своим статистическим свойствам к чисто случайной, используется метод комбинирования нескольких последовательностей, полученных от разных физических источников [1, 2]. Обычно в качестве математической модели для данных последовательностей используется схема независимых испытаний. В данной работе рассматриваются $n \geqslant 2$ независимых последовательностей бинарных случайных величин $\{x_t^{(i)}, t = 0, 1, 2, \dots\}$ $(i = \overline{1, n})$, полученных от разных физических источников, являющихся однородными односвязными цепями Маркова (ОЦМ-1) с векторами начальных распределений вероятностей $\pi^{(i)}$ и симметрическими матрицами вероятностей одношаговых переходов $P^{(i)}$:

$$\pi^{(i)} = (\pi_j^{(i)}): \quad \pi_j^{(i)} = \mathsf{P}\left\{x_0^{(i)} = j\right\} > 0, \quad j = 0, 1, \tag{1}$$

$$P^{(i)} = (p_{j_1,j_2}^{(i)}): \quad p_{j_1,j_2}^{(i)} = \mathsf{P}\left\{x_{t+1}^{(i)} = j_2 | x_t^{(i)} = j_1\right\} = p_i + \delta_{j_1,j_2}(1 - 2p_i) > 0, \quad j_1, j_2 = 0, 1, \tag{2}$$

где $\delta_{i,j}$ — символ Кронекера: $\delta_{i,j} = \begin{cases} 1, & \text{если } i = j, \\ 0, & \text{если } i \neq j. \end{cases}$

В качестве комбинирующей функции для данных последовательностей рассматривается произвольная булева функция от n переменных. При такой постановке задачи было показано, что среди всех булевых функций от $n \geqslant 2$ переменных только линейная функция сохраняет марковское свойство. Сформулируем данный результат в виде следующей теоремы.

Теорема 1. *Пусть* $\{x_t^{(i)}, t = 0, 1, 2, \dots\}$ $(i = \overline{1,n})$ *— независимые последовательности бинарных случайных величин, образующие ОЦМ-1 с параметрами* (1), (2). *Последовательность* $y_t = f(x_t^{(1)}, \dots, x_t^{(n)})$ *является ОЦМ-1 тогда и только тогда, когда функция* $f : \{0,1\}^n \to \{0,1\}$ *имеет следующий вид:*

$$f(x_t^{(1)}, \dots, x_t^{(n)}) = x_t^{(1)} \oplus \dots \oplus x_t^{(n)} \oplus c, \quad c \in \{0,1\}.$$

В работе [3] было получено, что при суммировании по модулю 2 достаточно большого числа ОЦМ с симметрическими матрицами вероятностей одношаговых переходов распределение результирующей последовательности стремится к распределению чисто случайной последовательности. Откуда, можно сделать вывод, что используя основную комбинирующую функцию для физических генераторов — линейную [1, 2], можно получить последовательность, близкую по своим статистическим свойствам к чисто случайной, даже в случае, если в комбинируемых последовательностях существует марковская зависимость.

Литература

1. *Eastlake D., Crocker S., Schiller J.* Randomness Recommendations for Security, RFC 1750, 1994.
2. *Eastlake D., Crocker S., Schiller J.* Randomness Requirements for Security, RFC 4086, 2005.
3. Отчет о НИР / Белгосуниверситет, 2003.