С. Ю. Мельников (Москва, ООО «Линфо»). **О статистической эквивалентности двоичных функций в схеме регистра сдвига с бернуллиевским и марковским входом.**

Пусть F_n — множество всех булевых функций от n аргументов, $n = 1, 2, \ldots$ Для булевой функции $f(x_1, x_2, \ldots, x_n) \in F_n$ обозначим $A_f = (X = \{0,1\}, \{0,1\}^n, Y = \{0,1\}, h, f)$ автомат Мура, являющийся двоичным регистром сдвига с накопителем размера n, множеством состояний $\{0,1\}^n$, функцией переходов h, определяемой по правилу $h((\alpha_1, \alpha_2, \ldots, \alpha_n), x) = (\alpha_2, \alpha_3, \ldots, \alpha_n, x)$, где $x, \alpha_i \in \{0,1\}$, $i = 1, 2, \ldots, n$, функцией выходов $f(x_1, x_2, \ldots, x_n)$.

Предположим, что на вход A_f поступает бернуллиевская последовательность независимых двоичных случайных величин $x^{(i)}$, $i = 1, 2, \ldots$, с распределением $\mathbf{P}\{x^{(i)} = 1\} = p$, $\mathbf{P}\{x^{(i)} = 0\} = 1 - p$, $0 < p < 1$. Последовательность случайных величин $f(x^{(i)}, x^{(i+1)}, \ldots, x^{(i+n-1)})$, $i = n+1, n+2, \ldots$, является стационарной и имеет смысл говорить о вероятности $P_f(p) = \mathbf{P}\{f(x^{(i)}, x^{(i+1)}, \ldots, x^{(i+n-1)}) = 1\}$ единицы в выходной последовательности. В [1, 2] показано, что $P_f(p) = \sum_{j=0}^{n} s_j p^j (1-p)^{n-j}$, где $s_k = \|f(x_1, x_2, \ldots, x_n)| \, \|(x_1, x_2, \ldots, x_n)\| = k\|$ $(k = 0, 1, \ldots, n)$ — веса функции f на подуровнях булевого куба. Функции f и g из F_n назовем *статистически эквивалентными при бернуллиевском входе*, приняв для такого случая обозначение $f \sim g$, если $P_f(p) = P_g(p)$ для $0 < p < 1$.

Пусть теперь на вход автомата A_f, $f \in F_n$, $1, 2, \ldots$, поступает последовательность двоичных случайных величин $x(i)$, $i = 1, 2, \ldots$, связанных в простую однородную стационарную цепь Маркова с матрицей переходных вероятностей

$$\Pi = \begin{pmatrix} 1-\lambda & \lambda \\ \xi & 1-\xi \end{pmatrix}, \quad \lambda, \xi \in (0,1).$$

При этом последовательность случайных величин $f(x^{(i)}, x^{(i+1)}, \ldots, x^{i=n-1})$, $i = n+1, n+2, \ldots$, является стационарной и имеет смысл говорить о вероятности $P_f(\lambda, \xi) = \mathbf{P}\{f(x^{(i)}, x^{(i+1)}, \ldots, x^{(i+n-1)} = 1\}$ единицы в выходной последовательности. Функции f и g из F_n назовем *статистически эквивалентными при марковской входной зависимости*, приняв для этого случая обозначение $f \approx g$, если $P_f(\lambda, \xi) = P + g(\lambda, \xi)$ при λ и ξ из $(0,1)$.

Утверждение 1. *Если $f \approx g$, то $f \sim g$.*

Утверждение 2. *Для количества классов эквивалентности при $n \to \infty$ справедливы соотношения*

$$|F_n/\sim| = \exp\left\{\frac{n^2}{2} + O(n \log n)\right\}, \quad |F_n/\approx| = \exp\left\{\frac{5}{4} n^2 \ln n + O(n^3)\right\}.$$

СПИСОК ЛИТЕРАТУРЫ

1. *Севастьянов Б. А.* Условное распределение выхода автоматов без памяти при заданных характеристиках входа. — Дискретн. матем., 1994, т. 6, в. 1, с. 34–39.
2. *Хохлов В. И.* Точные формулы для вторых моментов условных преобладаний по Севастьянову. — Обозрение прикл. и промышл. матем., 2003, т. 10, в. 3, с. 579–582.