

С. Ю. М е л ь н и к о в (Москва, ООО «Стэл-КС»). **О статистических характеристиках обработки двоичных последовательностей регистром сдвига с последовательным суммированием.**

В [1] рассматривались многогранники, характеризующие статистические свойства конечных сильносвязных автоматов. В случае двоичных входного и выходного алфавитов и значковых статистик этот многогранник является многоугольником в квадрате $[0, 1] \times [0, 1]$. Его можно трактовать как геометрическое место точек на плоскости, координаты которых образованы всевозможными пределами пар относительных частот встречаемости единиц во входной и выходной последовательностях.

Пусть $f(x_1, x_2, \dots, x_n)$ — булева функция от n двоичных переменных, $n = 1, 2, \dots$. Пусть A_f — регистр сдвига с последовательным суммированием, т. е. автомат Мили, множество состояний которого есть множество всех n -мерных двоичных векторов, входной и выходной алфавиты — множества $[0, 1]$. Автомат A_f под действием входного символа $\alpha \in \{0, 1\}$ из состояния $(\alpha_1, \alpha_2, \dots, \alpha_n)$ переходит в состояние $(\alpha, \alpha_1 \oplus \alpha_2, \dots, \alpha_{n-1} \oplus \alpha_n)$. Выходом автомата является значение функции f от текущего состояния. Многоугольник автомата A_f обозначим R_f .

Утверждение 1.

$$R_f = \text{Conv} \left\langle \left(\frac{\|c\|}{l_c} \right), \frac{\|f/c\|}{l_c}, c \in C(G) \right\rangle,$$

где G — граф автомата A_f , $C(G)$ — множество всех его циклов, l_c — длина цикла c , $\|c\|$ — число единиц во входной разметке цикла c , $\|f/c\|$ — вес функции на векторах цикла c , Conv — взятие выпуклой оболочки на плоскости.

Утверждение 2. $R_{f(x_1, x_2, \dots, x_n)} = R_{f(x_1, x_2, \dots, \bar{x}_n)}$, многоугольники $R_{f(x_1, x_2, \dots, x_n)}$ и $R_{\overline{f(x_1, x_2, \dots, x_n)}}$ симметричны относительно горизонтальной оси симметрии квадрата $[0, 1] \times [0, 1]$.

Пусть M_n — число таких булевых функций f от n переменных, для которых $R_f = [0, 1] \times [0, 1]$.

Утверждение 3. $M_n > 2^{2^n - 4n}$, $n = 5, 6, \dots$

СПИСОК ЛИТЕРАТУРЫ

1. Мельников С. Ю. Многогранники, характеризующие статистические свойства конечных автоматов. — Труды по дискретной математике, т. 7. М.: Физматлит, 2003, с. 126–137.