УДК 519.713

Т.А. ВАЛУЕВА

ОЦЕНКА ВЕРОЯТНОСТНЫХ ХАРАКТЕРИСТИК ОДНОГО КЛАССА АВТОНОМНЫХ АВТОМАТОВ

We consider an autonomous automaton, which consists of linear feedback shift registers, and obtain the tight upper bounds for the probability that initial state of such automaton repeats at first after n steps.

Математическая модель

Рассмотрим конечный автономный автомат U, состоящий из $m \geq 1$ двоичных линейных регистров сдвига $R_1, R_2, ..., R_m$ [1, 2]. В момент времени $t \in N$ регистр R_i сдвигается на $v_i(t)$ шагов, где $v_i(1), v_i(2), ...$ – независимые в совокупности случайные величины с заданным распределением вероятностей на множестве $K_i = \{L_{i,1}, L_{i,2}, ..., L_{i,k_i}\}$, $L_{i,j} \in N_0 = N \cup \{0\}$, $0 \leq L_{i,1} < L_{i,2} < ... < L_{i,k_i}$, $\mathrm{P}\left\{v_i(t) = L_{i,j}\right\} = p_{i,j} > 0$, $\sum_{j=1}^{k_i} p_{i,j} = 1$.

Рассмотрим случай, когда полином обратной связи регистра R_i является неприводимым полиномом степени n_i, порядка T_i, $T_i \ge \max\left\{L_{i,k_i}, 3\right\}$, $i=\overline{1,m}$ (см. [2]). Обозначим: $V=\{0,1\}$ – множество выходов автомата U; $S=S_1\times S_2\times\ldots\times S_m$ – множество состояний U, где $S_i=V_{n_i}\setminus\{0_{n_i}\}$ – множество ненулевых состояний R_i; $S(t)=(S_1(t),S_2(t),\ldots,S_m(t))$ – состояние U в момент t, где $S_i(t)=(s_{i,1}(t),s_{i,2}(t),\ldots,s_{i,n_i}(t))$ – состояние R_i в момент t, $s_{i,j}(t)\in V$. Функция переходов состояний имеет вид: $S_i(t+1)=S_i(t)\cdot A_i^{v_i(t)}$, $i=\overline{1,m}$, где A_i – характеристическая матрица порядка n_i полинома обратной связи R_i.

В [3] рассмотрен случай, когда в момент t R_i сдвигается на $\tilde{v}_i(S(t))$ шагов, где $\tilde{v}_i: S\to K_i=\{1,2,\ldots,k_i\}$ – некоторая функция. Всевозможные функции $\tilde{v}_i$ определяют класс автоматов мощности $\left(\prod_{i=1}^m k_i\right)^{T_1T_2\ldots T_m}$; в работе [3] вычислена вероятность события $D(n)=\{$начальное состояние автомата, выбранного случайно и равновероятно из указанного класса, лежит на цикле длины $n\}$. В данной статье рассмотрен общий случай задания множества K_i, включая особый случай $L_{i,1}=0$, когда регистр может простаивать, а также получено наиболее вероятное время первого возвращения автомата в начальное состояние, в ситуации, когда $K_i=\{1,2\}$, $p_{i,1}\in\{1/4,1/2\}$.

Вероятность возвращения автомата в начальное состояние

Определим время первого возвращения τ как число шагов, за которое автомат впервые возвращается в начальное состояние $S(1)$. Обозначим: $p(n)=\mathrm{P}\left\{\tau=n\right\}$; $T_+=\max_{1\le i\le m}T_i$ ($T_-=\min_{1\le i\le m}T_i$) – наибольший (наименьший) порядок полинома обратной связи, $n_0=\min_{1\le i\le m}\{T_i/L_{i,k_i}\}$, $B_i(n,r)=n!\sum(p_{i,1})^{x_{i,1}}(p_{i,2})^{x_{i,2}}\ldots(p_{i,k_i})^{x_{i,k_i}}/(x_{i,1}!x_{i,2}!\ldots x_{i,k_i}!)$, где суммирование проводится по всем наборам $x_{i,1},x_{i,2},\ldots,x_{i,k_i}$, $x_{i,j}\in N_0$, удовлетворяющим соотношениям: $x_{i,1}+x_{i,2}+..+x_{i,k_i}=n$, $L_{i,1}x_{i,1}+L_{i,2}x_{i,2}+\ldots+L_{i,k_i}x_{i,k_i}=r$. В случае, когда данные уравнения не имеют решений в N_0, положим $B_i(n,r)=0$. Кроме того, обозначим $M_i=\sum_{j=2}^{k_i}p_{i,j}B_i(n-1,T_i-L_{i,j})$.

Теорема. Пусть $S(1)$ – случайное начальное состояние автомата U, равномерно распределенное на множестве S, тогда справедлива оценка сверху:

$$p(n)\le f(n)=\mathrm{P}\left\{S(1)=S(1+n)\right\}=\prod_{i=1}^m\left(\sum_{L_{i,1}n\le d_iT_i\le L_{i,k_i}n}B_i(n,d_iT_i)\right),\quad n\ge 1, \tag{1}$$

причем (1) обращается в равенство в следующих случаях:

1) $n=1$;
2) $\min_{1\le i\le m}L_{i,1}>0$; $1<n<2\max_{1\le i\le m}\{T_i/L_{i,k_i}\}$;
3) $\min_{1\le i\le m}L_{i,1}=0$, $\max_{1\le i\le m}L_{i,1}>0$; $1<n<2n_0$.

Вдобавок, если $\max_{1\le i\le m}L_{i,1}=0$, то

$$p(n)=\begin{cases}0, & 1<n<n_0,\\ \prod_{i=1}^m(p_{i,1})^n\sum_{l=1}^m\sum_{\substack{s_1,s_2,\ldots,s_l\in\{1,m\}\\ s_1<s_2<\ldots<s_l}}\dfrac{M_{s_1}M_{s_2}\ldots M_{s_l}}{(p_{s_1,1}p_{s_2,1}\cdots p_{s_l,1})^n}, & n_0\le n<2n_0.\end{cases}$$

Схема доказательства данной теоремы аналогична схеме доказательства теоремы 1 из [3].

Замечание. Отметим, что в работе [1] показано, что в случае $K_i=\{1,2,\ldots,k_i\}$, $p_{i,j}=1/k_i$, справедливо равенство $p(n)=\mathrm{P}\left\{D(n)\right\}$, и, как следствие, результат теоремы в данном случае согласуется с теоремой 1 [3].

Следствие 1. Если $K_i=\{k,k+1\}$, $k\in N$, $\mathrm{P}\left\{v_i(t)=k\right\}=p_i$, $\mathrm{P}\left\{v_i(t)=k+1\right\}=1-p_i$ и $T_+/(k+1)\le n<T_-/k$, то

$$p(n)=f(n)=\prod_{i=1}^m\frac{n!(p_i)^{D_i}(1-p_i)^{(n-D_i)}}{D_i!(n-D_i)!},\ \text{где } D_i=(k+1)n-T_i. \tag{2}$$

Следствие 2. Если $K_i = \{0,1\}$, $\mathrm{P}\{v_i(t)=0\} = p_i$ и $T_+ \le n < 2T_-$, то

$$f(n) = \prod_{i=1}^{m}\left(\frac{n!(p_i)^{n-T_i}(1-p_i)^{T_i}}{(n-T_i)!T_i!} + p_i^n\right).$$

На отрезке $[N_1, N_2[$ наиболее вероятным временем *первого* возвращения автомата в начальное состояние назовем $n^* = \arg\max_{N_1 \le n < N_2} p(n)$, а наиболее вероятным временем возвращения автомата в начальное состояние назовем $n^{**} = \arg\max_{N_1 \le n < N_2} f(n)$.

Следствие 3. В условиях следствия 1, если $k=1$, $p_i \in \{1/4, 1/2\}$, $i=\overline{1,m}$, $T_1 = T_2 = \ldots = T_m = T > 1$, $N_1 = T/2$, $N_2 = T$, то $n^* \in [n_-, n_+]$, где

$$n_- = \begin{cases} \lfloor 4T/7 - 33/49 \rfloor, & p_i = 1/4, \\ \lfloor 2T/3 - 5/9 \rfloor, & p_i = 1/2, \end{cases} \qquad n_+ = \begin{cases} \lceil 4T/7 - 3/7 \rceil, & p_i = 1/4, \\ \lceil 2T/3 - 1/3 \rceil, & p_i = 1/2. \end{cases}$$

Доказательство. В силу следствия 1 для $p(n)$ верно (2). Пусть $r(n) = p(n+1)/p(n)$. Так как $n \in N$, максимум $p(n)$ доставляет такое n^*, что $r(n^*-1) > 1$ и $r(n^*) \le 1$. Решая уравнение $r(n) = 1$ относительно n, находим n^*. Отметим, что решение данного уравнения является вещественным числом, а значение n^* – натуральным, поэтому в следствии 3 приведены значения границ промежутка $[n_-, n_+]$, содержащего n^*.

Следствие 4. В условиях следствия 2, если $p_i \in \{1/4, 1/2\}$, $i=\overline{1,m}$, $T_1 = T_2 = \ldots = T_m = T > 1$, $N_1 = T$, $N_2 = 2T$, то

$$n^{**} = \begin{cases} \lceil 4T/3 \rceil - 1, & p_i = 1/4, \\ 2T - 1, & p_i = 1/2. \end{cases}$$

Схема доказательства аналогична схеме доказательства следствия 3.

Результаты теоремы и ее следствий могут быть использованы при анализе псевдослучайных последовательностей, порождаемых автоматом U.

Автор выражает благодарность Ю.С. Харину и А.С. Гурину за ценные замечания и рекомендации, высказанные при подготовке статьи.

1. Фомичев В.М. Дискретная математика и криптология. М., 2003. С. 176.
2. Лидл Р., Нидеррайтер Г. Конечные поля: в 2 т. М., 1988. Т. 2. С. 495.
3. Михайлов В.Г. // Тр. по дискрет. мат. 2002. Т. 5. С. 167.

Поступила в редакцию 20.03.08.

Татьяна Александровна Валуева – младший научный сотрудник НИИ прикладных проблем математики и информатики БГУ.