

УСЛОВНЫЕ РАСПРЕДЕЛЕНИЯ TV-ГРАММ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ОДНОГО КЛАССА АВТОМАТОВ МУРА

We investigate the probabilistic dependence of the output sequence of the Moore automaton on the input sequence which elements are arbitrarily distributed.

Рассмотрим класс автоматов Мура, определяемый каноническими уравнениями:

$$S(t+1) = \varphi(S(t), x_{t+n}), \quad y(t) = f(S(t)), \quad t = 0, 1, 2, \dots,$$

где $S(t) = (S_0(t), S_1(t), \dots, S_{n-1}(t))$ - состояние автомата, x_{t+n} - элемент входной последовательности автомата, $\varphi: \{0,1\}^n \times \{0,1\} \rightarrow \{0,1\}^n$ - функция переходов, $f: \{0,1\}^n \rightarrow \{0,1\}$ - функция выходов, $y(t)$ - элемент выходной последовательности автомата.

Функция переходов $\varphi(S(t), x_{t+n})$, $t \geq 0$, имеет вид: $S(t+1) = (S_0(t+1), \dots, S_{n-1}(t+1)) = \varphi(S(t), x_{t+n}) = (S_1(t), \dots, S_{n-1}(t), x_{t+n})$, $S(0) = (x_0, \dots, x_{n-1})$.

Функция выходов $f(S(t))$, $t \geq 0$, имеет вид: $y(t) = f(S(t)) = f(S_0(t), \dots, S_{n-1}(t)) = f(x_t, \dots, x_{t+n-1})$.

Исходя из предположения [1, 2], что входы x_t - независимые одинаковые распределенные случайные величины с распределением вероятностей $P\{x_t = 1\} = p$, $P\{x_t = 0\} = 1 - p$, $t \geq 0$, а выходы $y(t)$ имеют распределение $p_y = P\{y(t) = f(x(t)) = y\}$, $y \in \{0, 1\}$, были рассмотрены задачи нахождения условных вероятностей

$$p_y(k) = P\{y(t) = f(x(t)) = y \mid \omega(x(t)) = k\},$$

$$p_{y^0, y^1}^{t, t+1}(k) = P\{(y(t), y(t+1)) = (y^0, y^1) \mid \omega(\bar{x}(t)) = k\},$$

где $\omega(x(t))$, $\omega(\bar{x}(t))$ - число единиц в векторах $x(t) = (x_t, \dots, x_{t+n-1})$ и $\bar{x}(t) = (x_t, \dots, x_{t+n})$ соответственно.

Отметим, что результаты [1, 2] применимы на практике для векторов $x(t)$ произвольной длины.

В данной статье найдены условные распределения N -грамм ($N \geq 1$) выходной последовательности рассматриваемого автомата при следующих условиях:

- 1) x_t , $t \geq 0$, имеют произвольные распределения:

$$P\{x_t = y\} = p_t(y) = \begin{cases} p_t, & y = 1, \\ 1 - p_t, & y = 0, \end{cases}$$

$$0 < p_t < 1, \quad t \geq 0;$$

- 2) входная последовательность автомата является последовательностью независимых случайных величин:

$$P\{x_{i_1} = y^{i_1}, \dots, x_{i_m} = y^{i_m}\} = \prod_{k=1}^m P\{x_{i_k} = y^{i_k}\},$$

$$0 \leq i_1 < \dots < i_m, \quad \forall m \geq 1, \quad y^{i_1}, \dots, y^{i_m} \in \{0, 1\}.$$

Полученные соотношения для условных распределений N -грамм имеют экспоненциальную вычислительную сложность относительно длины n вектора $x(t)$ и применимы на практике для малых значений n .

Условные распределения выходных N-грамм при случайных входах

Найдем значения условных вероятностей $p_{y^0, \dots, y^{N-1}}^{t, \dots, t+N-1}(k)$:

$$p_{y^0, \dots, y^{N-1}}^{t, \dots, t+N-1}(k) = P\{(y(t), \dots, y(t+N-1)) = (y^0, \dots, y^{N-1}) \mid \omega(x'(t)) = k\}, \quad (1)$$

$$x'(t) = (x_t, \dots, x_{t+n+N-2}),$$

$$y(t+j) = f(x_{t+j}, \dots, x_{t+n+j-1}),$$

$$j = \overline{0, N-1}.$$

Для этого вычислим сначала следующие вспомогательные условные вероятности:

$$p_{l, \dots, l}^{j_1, \dots, j_m}(k) = P\{(y(j_1), \dots, y(j_m)) = (1, \dots, 1) \mid \omega(x'(t)) = k\},$$

где $x'(t) = (x_t, \dots, x_{t+n+N-2})$, $y(j_l) = f(x_{j_l}, \dots, x_{j_l+n-1})$, $l = \overline{1, m}$, $t \leq j_1 < j_2 < \dots < j_m \leq t+N-1$, $1 \leq m \leq N$.

Таблицу истинности функции $f(x(t))$ запишем в виде

$$f(x_t, \dots, x_{t+n-1}) = s_{2^{n-1}x_t + 2^{n-2}x_{t+1} + \dots + 2^0x_{t+n-1}} = s_{\sum_{j=0}^{n-1} 2^{n-j-1}x_{t+j}},$$

$$s_l \in \{0, 1\}, \quad l = \overline{0, 2^n - 1}.$$

Тогда условные вероятности $p_{l, \dots, l}^{j_1, \dots, j_m}(k)$ могут быть вычислены по следующей формуле:

$$\begin{aligned} p_{l, \dots, l}^{j_1, \dots, j_m}(k) &= P\left\{\prod_{l=1}^m f(x_{j_l}, \dots, x_{j_l+n-1}) = 1 \mid \omega(x'(t)) = k\right\} = \\ &= \frac{P\left\{\prod_{l=1}^m f(x_{j_l}, \dots, x_{j_l+n-1}) = 1, \omega(x'(t)) = k\right\}}{P\{\omega(x'(t)) = k\}} = \\ &= \frac{P\{f(x_{j_1}, \dots, x_{j_1+n-1}) \cdot \dots \cdot f(x_{j_m}, \dots, x_{j_m+n-1}) = 1, \omega(x'(t)) = k\}}{P\{\omega(x'(t)) = k\}} = \\ &= \frac{\sum_{\substack{i_1, \dots, i_{t+n+N-2} \in \{0,1\} \\ \sum_{j=t}^{t+n+N-2} i_j = k}} \left(\prod_{l=0}^{n-1} 2^{n-l-1} x_{j_1+l} \prod_{l=0}^{n-1} 2^{n-l-1} x_{j_2+l} \cdot \dots \cdot \prod_{l=0}^{n-1} 2^{n-l-1} x_{j_m+l} \prod_{l=t}^{t+n+N-2} p_l(i_l) \right)}{\sum_{\substack{i_1, \dots, i_{t+n+N-2} \in \{0,1\} \\ \sum_{j=t}^{t+n+N-2} i_j = k}} \prod_{l=t}^{t+n+N-2} p_l(i_l)} = \\ &= \frac{\sum_{\substack{i_1, \dots, i_{t+n+N-2} \in \{0,1\} \\ \sum_{j=t}^{t+n+N-2} i_j = k}} \left(\prod_{u=0}^m \prod_{l=0}^{n-1} 2^{n-l-1} x_{j_u+l} \prod_{l=t}^{t+n+N-2} p_l(i_l) \right)}{\sum_{\substack{i_1, \dots, i_{t+n+N-2} \in \{0,1\} \\ \sum_{j=t}^{t+n+N-2} i_j = k}} \prod_{l=t}^{t+n+N-2} p_l(i_l)}. \end{aligned} \quad (2)$$

При $m = N-1$ из формулы (2) получаем искомое значение для условной вероятности $p_{l, \dots, l}^{t, \dots, t+N-1}(k)$

Чтобы найти значения условных вероятностей $p_{y^0, \dots, y^{N-1}}^{t, \dots, t+N-1}(k)$ при $(y^0, \dots, y^{N-1}) \neq (1, \dots, 1)$, составим следующую систему, которая имеет единственное решение, так как матрица этой системы является невырожденной:

$$\begin{cases} p_1^{j_1}(k) = \sum_{\substack{i_1, \dots, i_{t+N-1} \in \{0,1\} \\ i_{j_1} = 1}} p_{i_1, \dots, i_{t+N-1}}^{t, \dots, t+N-1}(k), t \leq j_1 \leq t+N-1, \\ p_{1,1}^{j_1, j_2}(k) = \sum_{\substack{i_1, \dots, i_{t+N-1} \in \{0,1\} \\ i_{j_1} = 1, i_{j_2} = 1}} p_{i_1, \dots, i_{t+N-1}}^{t, \dots, t+N-1}(k), t \leq j_1 < j_2 \leq t+N-1, \\ \dots \\ p_{1, \dots, 1}^{j_1, \dots, j_{N-1}}(k) = \sum_{\substack{i_1, \dots, i_{t+N-1} \in \{0,1\} \\ i_{j_1} = 1, \dots, i_{j_{N-1}} = 1}} p_{i_1, \dots, i_{t+N-1}}^{t, \dots, t+N-1}(k), t \leq j_1 < j_2 < \dots < j_{N-1} \leq t+N-1. \end{cases} \quad (3)$$

Решая (3), получим значения условных вероятностей:

$$p_{y^0, \dots, y^{N-1}}^{t, \dots, t+N-1}(k) = \sum_{l=s}^N (-1)^{l-s} \left(\sum_{j_1=t}^{t+N-l} \dots \sum_{j_l=j_{l-1}+1}^{t+N-1} A(j_1, \dots, j_l) p_{1, \dots, 1}^{j_1, \dots, j_l}(k) \right), \quad (4)$$

$$A(j_1, \dots, j_l) = \sum_{u_1=1}^{l-s+1} \dots \sum_{u_s=j_{s-1}+1}^{j_s} \prod_{v=1}^s y^{j_v - u_v - t}, \quad s = \sum_{i=0}^{N-1} y^i, \\ (y^0, \dots, y^{N-1}) \neq (0, \dots, 0), \\ (y^0, \dots, y^{N-1}) \neq (1, \dots, 1),$$

где $p_{1, \dots, 1}^{j_1, \dots, j_l}(k)$, $t \leq j_1 < j_2 < \dots < j_l \leq t+N-1$, определяются с помощью формулы (2).

Используя (2) и (4), вычислим

$$p_{0, \dots, 0}^{t, \dots, t+N-1}(k) = 1 - \sum_{\substack{i_1, \dots, i_{t+N-1} \in \{0,1\} \\ i_{t+N-1} = 0 \\ \sum_{j=1}^{t+N-1} i_j \neq 0}} p_{i_1, \dots, i_{t+N-1}}^{t, \dots, t+N-1}(k). \quad (5)$$

Таким образом, была доказана следующая

Теорема 1. Пусть входная последовательность $\{x_i\}$ удовлетворяет условиям 1), 2), тогда условные $p_{y^0, \dots, y^{N-1}}^{t, \dots, t+N-1}(k)$ вероятности (1) определяются соотношениями (2), (4), (5).

В качестве примера рассмотрим систему (3) в случае $N = 3$:

$$\begin{cases} p_1^{j_1}(k) = \sum_{\substack{i_1, i_{t+1}, i_{t+2} \in \{0,1\} \\ i_{j_1} = 1}} p_{i_1, i_{t+1}, i_{t+2}}^{t, t+1, t+2}(k), \quad t \leq j_1 \leq t+2, \\ p_{1,1}^{j_1, j_2}(k) = \sum_{\substack{i_1, i_{t+1}, i_{t+2} \in \{0,1\} \\ i_{j_1} = 1, i_{j_2} = 1}} p_{i_1, i_{t+1}, i_{t+2}}^{t, t+1, t+2}(k), \quad t \leq j_1 < j_2 \leq t+2, \\ p_{1,1,1}^{j_1, j_2, j_3}(k) = p_{1,1,1}^{t, t+1, t+2}(k), \quad t \leq j_1 < j_2 < j_3 \leq t+2, \end{cases}$$

и представим ее в матричном виде $AX = B$, где:

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} p_{1,0,0}^{t, t+1, t+2}(k) \\ p_{0,1,0}^{t, t+1, t+2}(k) \\ p_{0,0,1}^{t, t+1, t+2}(k) \\ p_{1,1,0}^{t, t+1, t+2}(k) \\ p_{1,0,1}^{t, t+1, t+2}(k) \\ p_{0,1,1}^{t, t+1, t+2}(k) \\ p_{1,1,1}^{t, t+1, t+2}(k) \end{pmatrix}, \quad B = \begin{pmatrix} p_1^t(k) \\ p_1^{t+1}(k) \\ p_1^{t+2}(k) \\ p_{1,1}^{t, t+1}(k) \\ p_{1,1}^{t, t+2}(k) \\ p_{1,1}^{t+1, t+2}(k) \\ p_{1,1,1}^{t, t+1, t+2}(k) \end{pmatrix}.$$

Решение системы (3) для данного случая имеет вид:

$$\begin{aligned} p_{1,0,0}^{t,t+1,t+2}(k) &= p_1^{t+2}(k) - p_{1,1}^{t,t+2}(k) - p_{1,1}^{t+1,t+2}(k) + p_{1,1,1}^{t,t+1,t+2}(k), \\ p_{0,1,0}^{t,t+1,t+2}(k) &= p_1^{t+1}(k) - p_{1,1}^{t,t+1}(k) - p_{1,1}^{t+1,t+2}(k) + p_{1,1,1}^{t,t+1,t+2}(k), \\ p_{0,0,1}^{t,t+1,t+2}(k) &= p_1^{t+2}(k) - p_{1,1}^{t,t+2}(k) - p_{1,1}^{t+1,t+2}(k) + p_{1,1,1}^{t,t+1,t+2}(k), \\ p_{1,1,0}^{t,t+1,t+2}(k) &= p_{1,1}^{t,t+1}(k) - p_{1,1,1}^{t,t+1,t+2}(k), \\ p_{1,0,1}^{t,t+1,t+2}(k) &= p_{1,1}^{t,t+2}(k) - p_{1,1,1}^{t,t+1,t+2}(k), \\ p_{0,1,1}^{t,t+1,t+2}(k) &= p_{1,1}^{t+1,t+2}(k) - p_{1,1,1}^{t,t+1,t+2}(k), \end{aligned}$$

что совпадает с (4) при $N = 3$.

Следствие 1. В условиях теоремы 1 условные вероятности для биграмм

$p_{y^0, y^1}^{t,t+1}(k) = P\{(y(t), y(t+1)) = (y^0, y^1) | \omega(x'(t)) = k\}$ *определяются следующим образом:*

$$\begin{aligned} p_{1,0}^{t,t+1}(k) &= p_1^t(k) - p_{1,1}^{t,t+1}(k), \quad p_{0,1}^{t,t+1}(k) = p_1^{t+1}(k) - p_{1,1}^{t,t+1}(k), \\ p_{0,0}^{t,t+1}(k) &= 1 - p_1^t(k) - p_1^{t+1}(k) + p_{1,1}^{t,t+1}(k), \end{aligned} \quad (6)$$

где $p_1^t(k)$, $p_1^{t+1}(k)$, $p_{1,1}^{t,t+1}(k)$ *определяется с помощью формулы (2).*

В случае, когда $p_t = p$, $t \geq 1$, из (6) следуют результаты, полученные в работе [2].

1. Севастьянов Б. А. // Дискрет. мат. 1994. Т. 6. Вып. 1. С. 34.

2. Он же // Тр. по дискрет. мат. 2002. Т. 5. С. 219.

Поступила в редакцию 01.11.05.

Елизавета Владимировна Храмова - младший научный сотрудник НИЛ математических методов защиты информации НИИЦППМИ. Научный руководитель - кандидат физико-математических наук, заместитель директора НИИЦППМИ В.А. Галинский.