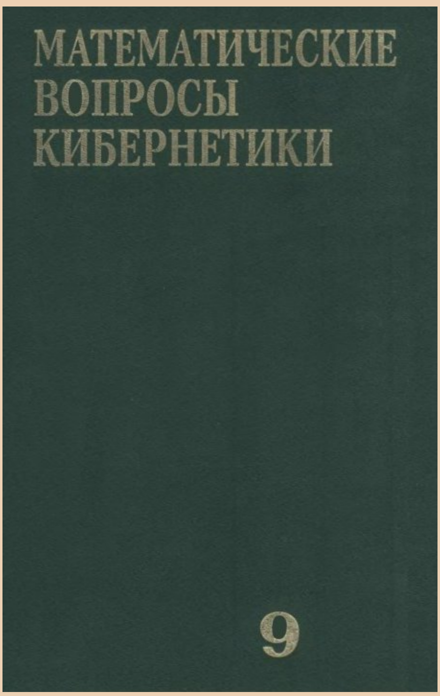

Р. Г. Бухараев

Автоматная методология исследования случайных последовательностей

АВТОМАТНАЯ МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Р. Г. БУХАРАЕВ

(КАЗАНЬ)

Введение

Теория последовательностей случайных кодов обычно строится в рамках классической теории вероятностей как ориентированная на формулировку и доказательство теорем существования. Структурный подход, ориентированный на синтез случайной последовательности с наперед заданными свойствами, применялся пока только для синтеза однородных конечных цепей Маркова. Однако, существует возможность развития структурного подхода по отношению к случайным последовательностям и в общем случае. А. С. Дэвис ([4], 1961) первым показал, что марковская цепь может быть получена как выходная последовательность детерминированного автомата со случайным входом. Этот факт был развит (Бухараев Р. Г., [1], 1985) в автоматную теорию функций цепей Маркова. В частности, было показано, что класс функций цепей Маркова (в том числе конечных) замкнут относительно (конечно-) автоматных преобразований.

Теория случайных последовательностей может строиться как частный случай теории многотактных каналов, имеющих входной алфавит, содержащий единственный символ. Благодаря этому многие результаты для случайных последовательностей получаются как частные случаи более общих теорем для вероятностных автоматов. Этот подход оказывается очень продуктивным для приложений, поскольку он выявляет структурные свойства случайных последовательностей и конструктивные пути их синтеза. Автоматный подход позволяет предложить новые пути классификации случайных последовательностей, исследовать их детерминированно-автоматные преобразования, выделить ряд специальных классов случайных последовательностей, в частности, такие как класс случайных последовательностей с конечным числом состояний и класс функций однородных конечных цепей Маркова. Высказанные идеи ниже развиваются более детально.

Вводные замечания

Понятие вероятностного автомата было введено независимо и практически одновременно несколькими авторами. Хронологически первыми были Дж. У. Карлайл ([3], 1963) и М. О. Рабин ([5], 1963). Используя собственные определения и обозначения, мы приводим ниже некоторые необходимые в дальнейшем факты теории вероятностных автоматов. Доказательства предложений этого раздела можно найти в [2] или [1].

Вероятностный автомат (общего вида) это объект

$$\langle X, Y, S, p(s', y/s, x)\rangle,$$

где $X=\{x_1, x_2, \ldots, x_m\}$ — конечное множество входных символов (букв), $S=\{s_1, s_2, \ldots, s_k\}$ — конечное (или счетное) множество состояний, $Y=\{y_1, y_2, \ldots, y_n\}$ — конечное множество выходных символов. В содержательном рассмотрении условное вероятностное распределение $p(s', y/s, x)$ определяет вероятность того, что вероятностный автомат перейдет в следующее состояние s' и реагирует выходным символом y при условии, что он получил на вход символ x, находясь в текущем состоянии s. Ясно, что для распределения $p(s', y/s, x)$ должны выполняться условия:

$$0 \leqslant p(s', y/s, x) \leqslant 1, \qquad \sum_{s' \in S, y \in Y} p(s', y/s, x) = 1, \qquad (s, x) \in (S \times X).$$

Введем в рассмотрение $k \times k$-матрицы $A(y/x)$, где
$$a_{s,s'} = p(s', y/s, x), \qquad A(y/x) = (a_{s,s'}).$$

Элементы матриц $A(y/x)$ неотрицательны и не более единицы. Очевидно, что

$$\sum_{y \in Y} A(y/x) = A(x)$$

— стохастические матрицы.

Если обозначить через μ_0 стохастический вектор, представляющий распределение вероятностей начальных состояний вероятностного автомата, тогда распределение вероятностей его состояний при условии, что автомат имел на входе символ x и уже отреагировал выхоным символом y, описывается вектором

$$\mu(y/x) = \mu_0 A(y/x).$$

Допустим, что $v = x_1 x_2 \ldots x_t$ и $w = y_1 y_2 \ldots y_t$ — некоторые слова одинаковой длины в алфавитах соответственно X и Y. Введем обозначение

$$A(w/v) = A(y_1/x_1) A(y_2/x_2) \ldots A(y_t/x_t).$$

Тогда для слов vx и wy соответствующий вектор $\mu(wy/vx)$ вычисляется в соответствии с формулой:

$$\mu(wy/vx) = \mu(w/v) A(y/x).$$

Рассмотрим словарную функцию двух аргументов

$$\tau(w/v) = \mu(e) A(w/v) \varepsilon,$$

где через ε обозначен вектор-столбец, все координаты которого равны единице. Функция $\tau(w/v)$ называется *входно-выходным отношением* вероятностного автомата $(A, \mu(e))$ или *многотактным каналом*, представленным вероятностным автоматом A с начальным вектором состояний $\mu(e)$. Величина $\tau(w/v)$ есть вероятность того, что вероятностный автомат A отвечает реакцией w на входное слово v, при условии, что $\mu(e)$ — это его начальный вектор состояний. Заметим, что $\tau(e/e) = 1$.

Мы будем обозначать этот многотактный канал как

$$I = \langle X, Y, \tau(w/v) \rangle.$$

Положим $\boldsymbol{\tau}(w/v) = A(w/v)\varepsilon$. Вектор-столбец $\boldsymbol{\tau}(w/v)$ называется *поствектором состояний вероятностного автомата* A; s-координата

$\tau_s(w/v)$ поствектора $\tau(w/v)$ означает вероятность реакции вероятностного автомата словом w, при условии, что на входе было слово v, а вероятностный автомат стартовал из фиксированного начального состояния s. Для любой пары слов $|w_1|=|v_1|$, $|w_2|=|v_2|$, мы будем иметь

$$\tau(w_1 w_2/v_1 v_2) = A(w_1/v_1)\tau(w_2/v_2).$$

Если словарная функция $\tau(w/v)$ двух аргументов определена вероятностным автоматом A, начальным вектором состояний $\boldsymbol{\mu}(e)$ и поствектором $\boldsymbol{\varepsilon}$:

$$\tau(w/v) = \boldsymbol{\mu}(e)A(w/v)\boldsymbol{\varepsilon},$$

то будем говорить, что многотактный канал $\tau(w/v)$ *представлен* в вероятностном автомате A.

Сформулируем несколько основных теорем относительно вероятностного автомата общего вида, на которых базируются дальнейшие рассмотрения. Вероятностный автомат Γ,

$$\Gamma = \langle X, Z, p_\Gamma(z/x)\rangle,$$

обладающий одноэлементным множеством состояний называется *управляемым источником* (генератором) случайных кодов. С точки зрения теории случайных последовательностей управляемый источник следует рассматривать как стационарную последовательность случайных кодов со взаимно независимыми значениями. Иначе говоря, для произвольной пары слов $(x_1 \dots x_t,\ z_1 \dots z_t)$ справедливо тождество

$$\mu(z_1 \dots z_t/x_1 \dots x_t) = \mu(z_1/x_1) \cdots \mu(z_t/x_t).$$

Если рассматриваемый вероятностный автомат является автономным вероятностным автоматом, т. е. алфавит X содержит единственный символ, то для каждого слова $z_1 \dots z_t$ случайной последовательности как выходной последовательности для Γ выполняется условие:

$$\mu(z_1 \dots z_t) = \mu(z_1) \cdots \mu(z_t).$$

Определение 1. Пусть заданы управляемый источник Γ и вероятностный автомат B,

$$B = \langle Z, Y, S, p_B(s', y/s, z)\rangle.$$

Тогда вероятностный автомат $A = \langle X, Y, S, p_A(s', y/s, x)\rangle$, где

$$p_A(s', y/s, x) = \sum_{z \in Z} p_\Gamma(z/x) p_B(s', y/s, z)$$

называется *последовательной композицией (соединением) источника Γ и вероятностного автомата B*.

Теорема 1. *Пусть $A = \langle X, Y, S, p(s', y/s, x)\rangle$ — вероятностный автомат с k состояниями. Существуют управляемый источник случайных кодов $\Gamma = \langle X, Z, p_\Gamma(z/x)\rangle$ и детерминированный автомат $D = \langle Z, Y, S, \delta(s, z), \lambda(s, z)\rangle$ с k состояниями такие, что вероятностный автомат A изоморфен последовательному соединению источника Γ и детерминированного автомата D.*

Определение 2. Многотактный канал I называется *автоматным* многотактным каналом, если существует вероятностный автомат, который его представляет как входно-выходное отношение для некоторого начального вектора состояний $\boldsymbol{\mu}_0$.

Следующая теорема описывает необходимые и достаточные условия автоматности многотактного канала [1].

Теорема 2. *Для того, чтобы многотактный канал*

$$I = \langle X, Y, \tau(w/v)\rangle$$

был автоматным, необходимо и достаточно, чтобы выполнялись следующие условия:

$$1) |v| \neq |w| \longrightarrow \tau(w/v) = 0, \quad 2) \sum_{y \in Y} \tau(wy/vx) = \tau(w/v).$$

Положим

$$\tau_{v', w'}(w/v) = \frac{\tau(w'w/v'v)}{\tau(w'/v')},$$

если $\tau(w', v') \neq 0$.

Замечание 1. Если многотактный канал I является автоматным и вероятность $\tau(w'/v')$ не равна нулю для пары слов (v', w'), тогда многотактный канал

$$I(w'/v') = \langle X, Y, \tau_{v', w'}(w/v)\rangle$$

тоже автоматный.

Определение 3. Многотактный канал $I(w'/v')$, определенный для пары слов (v', w'), $\tau(w'/v') \neq 0$ называется (v', w')*-состоянием многотактного канала* I.

Для формулировки критерия того, что автоматный многотактный канал I имеет конечное число различных состояний, нам необходимы следующие два определения. Мы будем рассматривать каналы $I(w'/v')$ как последовательности вида

$$I = (1, \ldots, \tau_{w', v'}(w/v), \ldots),$$

полагая, что множество пар слов одинаковой длины $X^* \times Y^*$ вполне упорядочено определенным образом, скажем, лексикографически, и $\tau_{w', v'}(w/v)$ «занимает место» с «номером» (v, w) и пусть линейное пространство E_τ есть линейная оболочка множества состояний канала I. Эта «линеаризация» случайных последовательностей дает возможность рассматривать их линейные преобразования.

Пусть матрица $D(w'/v') = \|d_{(v_1, w_1), (v_2, w_2)}(w'/v')\|$ определена условиями

$$d_{(v_1, w_1), (v_2, w_2)}(w'/v') = \begin{cases} 1, & \text{если } v_1 = v'v_2,\ w_1 = w'w_2, \\ 0 & \text{в противном случае.} \end{cases}$$

Преобразование

$$D(w'/v') \colon E_\tau \longrightarrow E_\tau$$

мы будем называть (v', w')*-вращением линейного пространства* E_τ.

Определение 4. Множество многотактных каналов Γ, $\Gamma \subset E_\tau$, называется *выпуклым относительно полугруппы* (v, w)*-вращений*, если любые (v, w)-вращения каналов из Γ являются выпуклыми линейными комбинациями каналов из того же множества Γ.

Определение 5. Множество $\Gamma(\Omega)$ из E_τ называется *опорным множеством для* Ω, $\Omega \subset E_\tau$, если его выпуклое линейное замыкание содержит Ω.

Теорема 3. *Для того, чтобы автоматный многотактный канал I был конечно-автоматным, необходимо и достаточно, чтобы для множества состояний этого канала существовало конечное опорное множество $\Gamma(I)$, выпуклое относительно полугруппы (v, w)-вращений. Число состояний вероятностного автомата $A(I)$, представляющего канал I, может быть выбрано равным мощности множества $\Gamma(I)$.*

Определение 6. *Полудетерминированным* называется вероятностный автомат $A = \langle X, Y, S, p(s', y/s, x)\rangle$, если существует такая функция $s' = \varphi(s, x, y)$, что условное вероятностное распределение $p(s', y/s, x)$ может быть отлично от нуля лишь для таких пар слов (s, x) и (s', y), для которых выполняется равенство $s' = \varphi(s, x, y)$.

Теорема 4. *Для того, чтобы автоматный многотактный канал имел конечное число различных состояний, необходимо и достаточно, чтобы существовал полудетерминированный конечный вероятностный автомат $A(I)$, представляющий этот канал фиксированным начальным состоянием. Число состояний автомата $A(I)$ может быть равно числу различных состояний канала I.*

Можно описать класс многотактных каналов с еще более слабыми ограничениями.

Замечание 2. Вероятностный автомат называется псевдо-вероятностным, если из его определения удалить условие неотрицательности элементов переходных матриц $A(y/x)$, вектора состояний $\boldsymbol{\mu}$ и решающего поствектора $\boldsymbol{m}$.

Определение 7. Пусть $\Sigma_1 = \{(v_1, w_1), \ldots, (v_k, w_k)\}$, $\Sigma_2 = \{(v_1', w_1'), \ldots, (v_k', w_k')\}$ — две произвольных последовательности пар слов одинаковой длины. Матрица

$$R_{\Sigma_1, \Sigma_2} = \begin{pmatrix} \tau(w_1 w_1'/v_1 v_1') & \ldots & \tau(w_1 w_k'/v_1 v_k') \\ \ldots & \ldots & \ldots \\ \tau(w_k w_1'/v_k v_1') & \ldots & \tau(w_k w_k'/v_k v_k') \end{pmatrix}$$

называется *составной последовательностной матрицей* с входным множеством Σ_1 и выходным множеством Σ_2.

Определение 8. Многотактный канал I называется *слабо конечно-автоматным*, если существует конечный псевдо-вероятностный автомат $A(I)$, который представляет канал I как свое входно-выходное отношение.

Следующая теорема доказана Дж. Карлайлом.

Теорема 5. *Для того, чтобы многотакный канал I был слабо конечно-автоматным, необходимо и достаточно, чтобы каждая составная последовательностная матрица для произвольных входного и выходного множеств пар слов имела конечный максимальный ранг. Этот ранг равен числу состояний минимального псевдовероятностного автомата, представляющего этот канал I.*

Импликация случайных кодов и случайные последовательности

Концепция вероятностной импликации является удобным средством для решения задач синтеза вероятностных преобразователей и играет существенную роль также при синтезе детерминированных автоматов, преобразующих случайные последовательности. Предварительно мы рассмотрим это понятие на примере преобразователя без памяти.

Обозначим через J и T соответственно множества индексов координат двух стохастических векторов $\boldsymbol{p}$ и $\boldsymbol{q}$. Будем говорить, что вероятностное распределение (стохастический вектор) p *имплицирует* вероятностное распределение (стохастический вектор) q, если возможно разбить множество J на систему непересекающихся подмножеств индексов $\langle J_s, s \in T \rangle$, $J_i \bigcap J_j = \varnothing$, $i \neq j$, таким образом, что

$$\sum_{i \in I_s} p_i = q_s, \quad s \in T.$$

Будем обозначать это как $p \longrightarrow q$.

Замечание 3. Для того, чтобы стохастический вектор p имплицировал стохастический вектор q, необходимо и достаточно, чтобы существовал детерминированный преобразователь (функция φ) множества J в множество T такой, что φ: $J \longrightarrow T$ и

$$\sum_{s = \varphi(i)} p_i = q_s, \quad s \in T.$$

Рассмотрим ситуацию более детально. Случайный код определяет некоторое соответствие между значениями кода и их вероятностями:

$$\xi = \begin{bmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ p_1 & p_2 & \dots & p_n \end{bmatrix}.$$

Преобразование одного случайного кода ξ в другой случайный код η сопровождается параллельным (сопутствующим) преобразованием вероятностного распределения ξ в вероятностное распределение η:

$$\eta = \varphi(\xi)$$
$$q(\eta) = \varphi^*(p(\xi)).$$

Поэтому импликация $(p \longrightarrow q)$ сопровождается двумя типами функций. Первая функция $\varphi^*(p)$ (это линейный оператор) реализует преобразование вероятностных распределений (стохастических векторов). Удобно представлять этот оператор φ^* в виде матрицы H_φ (это стохастическая матрица, все элементы которой равны нулям и единицам, т. е. простая матрица) и писать

$$q(\eta) = p(\xi) H_\varphi.$$

Вторая функция имеет вид $\varphi(\xi)$ и реализует отображение множеств значений случайных кодов η и ξ с вероятностными распределениями p и q.

Рассмотрим простой пример. Пусть $\eta = \varphi(\xi)$ — некоторая двоичная функция n двоичных переменных

$$y = \varphi(x_1, x_2, \dots, x_n)$$

и выражение

$$\varphi(x_1, x_2, \dots, x_n) = \bigvee_{\sigma_1, \sigma_2, \dots, \sigma_n} x_1^{\sigma_1} x_2^{\sigma_2} \cdots x_n^{\sigma_n} \varphi(\sigma_1, \sigma_2, \dots, \sigma_n),$$

где выражение x^σ обозначает

$$x^\sigma = \begin{cases} x, & \text{если } \sigma = 1, \\ \bar{x}, & \text{если } \sigma = 0, \end{cases}$$

есть дизъюнктивная нормальная форма этой функции. Тогда полилинейная функция φ^* (для каждой координаты вектора q) при взаимно независимых случайных переменных на входе $x_1, x_2, \ldots, x_n$, принимающих значения с вероятностями $P(x_i=1)=p_i$, $P(x_i=0)=1-p_i$ имеет вид

$$P(\varphi(x_1, x_2, \ldots, x_n)=1)=\varphi^*(p_1, p_2, \ldots, p_n)= \\ = \sum_{\sigma_1, \sigma_2, \ldots, \sigma_n} p_1^{\sigma_1} p_2^{\sigma_2} \cdots p_n^{\sigma_n} \varphi(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Здесь выражение p^σ означает

$$p^\sigma = \begin{cases} p, & \text{если } \sigma=1, \\ 1-p, & \text{если } \sigma=0. \end{cases}$$

Например, для $\varphi(x, y)=x \vee y$ получим $\varphi^*(p, q)=pq+p(1-q)+(1-p)q= =p+q-pq$.

Следующая известная теорема раскрывает другой аспект понятия импликации.

Теорема 6. *Произвольная стохастическая $n \times n$ матрица A может быть представлена в виде выпуклой линейной комбинации не более (n^2-n+1) простых матриц*

$$A=\alpha_1 C_1+\alpha_2 C_2+\ldots+\alpha_s C_s.$$

Демонстрационное значение теоремы состоит в том, что здесь стохастический вектор $\alpha=(\alpha_1, \alpha_2, \ldots, \alpha_s)$ имплицирует каждый стохастический вектор-строку матрицы A. С другой стороны, видно, что это разложение A представляет собой декомпозицию автономного вероятностного автомата — частный случай теоремы 1, где система простых матриц $\{C_i, i=1, \ldots, s\}$ представляет собой детерминированный автомат, имеющий то же число состояний, что и исходный вероятностный автомат A.

Этот факт демонстрирует тесные связи, имеющиеся между концепциями вероятностной импликации, преобразованиями случайных последовательностей и декомпозицией таких преобразователей.

При рассмотрении последовательностей случайных кодов, иначе говоря, в случае преобразователей с памятью, целесообразно ввести понятие *последовательностной импликации.*

Пусть дана последовательность случайных кодов

$$\tilde{\xi}\colon \xi_1, \xi_2, \ldots, \xi_n, \ldots,$$

где коды ξ_i принимают значения в одном и том же алфавите Y. Введем вероятности

$$P(\xi_1=y_1, \xi_2=y_2, \ldots, \xi_n=y_n)=\mu(y_1 y_2 \ldots y_n)=\mu(w),$$

где $w=y_1 y_2 \ldots y_n$.

Определение 9. Объект

$$J=\langle \mu(w), w \in Y^* \rangle$$

называется *последовательностью случайных кодов*, если $\mu(w)$ есть словарная функция

$$\mu\colon Y^* \longrightarrow [0, 1],$$

удовлетворяющая условиям:

$$1)\mu(e)=1, \qquad 2)\sum_{y \in Y} \mu(wy)=\mu(w).$$

Легко видеть, что эти условия эквивалентны условиям совместности А. Н. Колмогорова и определяют случайную последовательность в обычном смысле. Напомним, что обычно случайная последовательность задается в виде системы вероятностей множеств выборочных траекторий последовательности, образующих всевозможные конечные «цилиндры» вида $\xi_{i_1}=y_{i_1}, \xi_{i_2}=y_{i_2}, \ldots, \xi_{i_s}=y_{i_s}$, удовлетворяющие условиям совместности. В нашем случае задания случайной последовательности рассматриваются только «сплошные» цилиндры вида $\xi_1=y_1, \xi_2=y_2, \ldots, \xi_N=y_N$, где $y_1y_2\ldots y_N=w$ — слово в алфавите Y^*. Такая характеризация случайных последовательностей позволяет их рассматривать как многотактные каналы с однобуквенным входным алфавитом. Ситуация здесь аналогична представлению ограниченно-детерминированных функций в виде конечного детерминированного последовательностного преобразователя. Отличие состоит в том, для случайных последовательностей преобразователь является вероятностным.

Пусть даны две последовательности случайных кодов $\tilde{\xi}$: $\xi_1, \xi_2, \ldots$ $\ldots, \xi_n, \ldots$, и $\tilde{\eta}$: $\eta_1, \eta_2, \ldots, \eta_n, \ldots$ с системами вероятностей соответственно $\langle \mu_1(v), v\in X^*\rangle$ и $\langle \mu_2(w), w\in Y^*\rangle$. Будем говорить, что последовательность случайных кодов $\tilde{\xi}$ *последовательностно имплицирует* последовательность случайных кодов $\tilde{\eta}$, если для любого положительного целого n, $n>0$, конечная начальная подпоследовательность $\tilde{\xi}_n=\xi_1, \xi_2, \ldots, \xi_n$ имплицирует начальную конечную подпоследовательность $\tilde{\eta}_n=\eta_1, \eta_2, \ldots, \eta_n$, $\tilde{\xi}_n \longrightarrow \tilde{\eta}_n$, $n=1,2,\ldots$, так, что:

1) для любого целого положительного n и произвольных слов v, $v\in X^*$, и w, $w\in Y^*$, $|v|=|w|$ существует словарная функция φ_n такая, что

$$\mu_2(w)=\sum_{w=\varphi_n(v)}\mu_1(v),$$

2) для любых целого положительного n, слова v и символа x из X

$$\varphi_{n+1}(vx)=\varphi_n(v)\varphi'(x).$$

Второе условие в определении последовательностной импликации эквивалентно требованию, что система словарных отображений φ_n определяет некоторое словарное отображение над всей полугруппой X^*, которое является автоматным, т. е. для каждой пары слов v_1, v_2 из X^* справедливо соотношение

$$\varphi(v_1v_2)=\varphi(v_1)\varphi'(v_2).$$

Таким образом, можно сформулировать следующую теорему.

Теорема 7. *Последовательность случайных кодов $\tilde{\xi}$ последовательностно имплицирует последовательность случайных кодов $\tilde{\eta}$ тогда и только тогда, когда существует детерминированный автомат, который преобразует последовательность $\tilde{\xi}$ как входную последовательность автомата в выходную последовательность $\tilde{\eta}$.*

Другая форма этой теоремы описывает условия представимости последовательности пар случайных кодов в вероятностном автомате в том случае, когда представляющий автомат является детерминированным. Пусть $J_1=\langle \mu(v), v\in X^*\rangle$ и $J_2=\langle \mu(w), w\in Y^*\rangle$ — последовательность случайных кодов.

Теорема 8. *Для существования детерминированного автомата Мили, преобразующего случайную последовательность J_1 в случайную последовательность J_2, необходимо и достаточно, чтобы для каждого* *слова w выполнялось соотношение*

$$\mu(w) = \sum_{w=\varphi(v)} \mu(v),$$

где отображение φ: $X^* \longrightarrow Y^*$ является автоматным.

Следствие 1. *Детерминированный автомат, преобразующий последовательность J_1 в последовательность J_2 может быть конечным тогда и только тогда, когда автоматное отображение φ имеет конечное число состояний.*

Замечание 4. Для любого конечного (или счетного) семейства конечных вероятностных распределений (стохастических векторов) $\Sigma = \{\boldsymbol{q}_1, \boldsymbol{q}_2, \ldots, \boldsymbol{q}_s\}$ можно построить конечное распределение вероятностей (стохастический вектор) $\boldsymbol{q}$, которое имплицирует каждое из распределений (векторов) семейства Σ.

В выборе этого имплицирующего распределения имеется большой произвол, который может быть использован для оптимизации решения. Аналогично, справедливо и следующее замечание.

Замечание 5. Для любого конечного семейства последовательностей случайных кодов $J_i = \langle \mu_i(w), w \in Y^* \rangle$ с конечным алфавитом Y можно построить стационарную, с независимыми значениями, последовательность случайных кодов $S = \langle \mu(v), v \in X^* \rangle$, которая последовательно имплицирует каждую последовательность J_i.

Будем рассматривать далее последовательность случайных кодов $J = \langle \mu(w), w \in Y^* \rangle$ как выходную последовательность автономного вероятностного автомата. Другими словами, мы рассматриваем эту последовательность как многотактный канал, представленный в некотором вероятностном автомате с входным алфавитом из единственной буквы. Сравнение теоремы 2 с определением 9 показывает правомерность такого рассмотрения. Из последнего замечания и теоремы 1 вытекает следующее утверждение.

Теорема 9. *Каждая последовательность случайных кодов $J = \langle \mu(w), w \in Y^* \rangle$ автоматна.*

Этот результат можно получить также из сравнения теоремы 2 и определения 9 последовательности случайных кодов.

Продемонстрируем процедуру построения представляющего (генерирующего) вероятностного автомата по заданной выходной последовательности случайных кодов. Мы будем опираться при этом на представление вероятностного автомата в виде последовательной композиции управляемого источника случайных кодов и некоторого детерминированного автомата Мили. В случае автономного вероятностного автомата управляемый источник на входе детерминированного автомата определяет стационарную последовательность случайных кодов со взаимно независимыми значениями. Пусть последовательность случайных кодов

$$\langle \mu(w), w \in Y^* \rangle$$

имеет имплицирующую стационарную последовательность

$$\langle \mu(v), v \in X^* \rangle,$$

где для каждого слова $v = x_1 x_2 \ldots x_k$

$$\mu(x_1 x_2 \ldots x_k) = \mu(x_1)\mu(x_2)\ldots\mu(x_k)$$

и детерминированный автомат D,

$$D = \langle X, Y, S, \delta(s, x), \lambda(s, x) \rangle$$

есть имплицирующий автомат. Представим пару функций (δ, λ) в виде $n \times n$ матрицы $C(y/x)$, где

$$c_{s_1, s_2}(y/x) = \begin{cases} 1, & \text{если } s_2 = \delta(s_1, x),\ y = \lambda(s_1, x), \\ 0 & \text{в противном случае.} \end{cases}$$

Тогда автономный вероятностный автомат A, который представляет последовательность J как свою выходную, имеет матрицу переходов

$$A(y) = \sum_{x \in X} \mu(x) C(y/x).$$

Какова «схема действия» линейного оператора H_φ в случае последовательностной импликации $\widetilde{\xi} \longrightarrow \widetilde{\eta}$? Это преобразование реализует некоторый детерминированный автомат, имеющий функцию перехода $s' = \delta(s, x)$ и функцию выхода $y = \lambda(s, x)$. Поскольку переменная x принимает случайные значения в соответствии с вероятностным распределением $p(\xi_n)$ на n-м шаге процесса, мы получаем, что первая функция определяет стохастическую матрицу A, которая реализует случайную перестановку состояний автомата. Функция выхода определяет простую матрицу H_s, которая зависит от текущего состояния автомата и реализует линейный оператор, преобразующий входное распределение вероятностей в выходное:

$$q(\eta_n) = p(\xi_n) H_s.$$

Таким образом, этот процесс последовательностной импликации одной последовательности случайных кодов из другой определяется двумя линейными операторами: стохастическая матрица A описывает процесс изменения состояний (меток матриц H_s), а система простых матриц H_s определяет операторы типа φ^*, реализующие импликации случайных кодов на текущем шаге процесса. Очевидно, что в общем случае автомат-преобразователь имеет неограниченное множество состояний, так что матрица A счетного порядка, соответственно, является счетной и мощность множества $\{H_s\}$.

Возвращаясь к теореме 9, мы видим, что произвольный автономный вероятностный автомат порождает некоторую систему матриц

$$\Xi = \{A, H_s, s \in S\},$$

где A — стохастическая $|S| \times |S|$-матрица, H_s, $s \in S$, — $|Y| \times |X|$ простые матрицы.

Более того, верна следующая теорема.

Теорема 10. *Для произвольной системы матриц*

$$\Xi = \{A, H_s, s \in S\},$$

удовлетворяющих условиям 1) *и* 2), *можно построить вероятностный автомат, который порождает эту систему* Ξ.

Сравнение этих результатов с теоремой 6 показывает, что вместо системы $\Xi = \{A, H_s, s \in S\}$ можно рассматривать систему

$$\Delta = \{\alpha, \quad C_x, x \in X, \quad H_s, s \in S\},$$

так что можно сформулировать такое следствие.

Следствие 2. *Произвольная последовательность случайных кодов (произвольный автономный вероятностный автомат) взаимно однозначно определяется системой типа* Δ, *где* Y — *алфавит последовательности (выходной алфавит вероятностного автомата),* X — *некоторое конечное, а* S — *конечное или счетное множество,* $\alpha = (\alpha_{x_1}, \alpha_{x_2}, \ldots, \alpha_{x_k})$ — *стохастический вектор,* C_{x_i}, $x_i \in X$ *и* H_s, $s \in S$, — *соответственно системы* $|S| \times |S|$ *и* $|Y| \times |X|$ *простых матриц.*

Линейное пространство E_μ последовательностей случайных кодов

Мы видели, что вероятностные распределения произвольной последовательности случайных кодов порождаются благодаря последовательностной активности некоторых линейных операторов. Ввиду этого возникает возможность дать интегральное описание множеству вероятностей всех начальных подпоследовательностей заданной последовательности случайных кодов. Пусть $J = \langle \mu(w),\ w \in Y^* \rangle$ — заданная последовательность и $\mu(w') \neq 0$ для любого слова w'. Тогда отношение

$$\mu_{w'}(w) = \mu(w'w)/\mu(w')$$

также является последовательностью случайных кодов. Назовем ее w'-состоянием последовательности J и обозначим как

$$J(w') = \langle \mu_{w'}(w),\ w \in Y^* \rangle.$$

Будем рассматривать случайную последовательность $J(w')$ как последовательность действительных чисел

$$J(w') = (1, \ldots, \mu_{w'}(w), \ldots),$$

полагая вновь,что множество слов Y^* упорядочено лексикографически и вероятность $\mu_{w'}(w)$ занимает место с «номером» w и пусть линейное пространство E_μ является линейной оболочкой L_μ. Пусть, далее, матрица $D(w') = \|d_{w_1, w_2}\|$ определена условиями

$$d_{w_1, w_2} = \begin{cases} 1, & \text{если } w_1 = w'w_2, \\ 0 & \text{в противном случае.} \end{cases}$$

Линейное преобразование

$$D(w') \colon E_\mu \longrightarrow E_\mu$$

будем называть *w'-вращением линейного пространства* E_μ.

Свойства пространства E_μ существенны для спецификации последовательности J. Необходимо принять во внимание две главные характеристики E_μ — его размерность и возможную структуру его базисов. В аналитической форме преобразование $D(w')$ можно представить следующим образом:

$$JD(w') = \mu(w')J(w').$$

Определение 10. Множество последовательностей случайных кодов $\Gamma, \Gamma \subset E_\mu$, назовем *выпуклым относительно полугруппы w'-вращений*, если каждое w'-вращение последовательностей из Γ есть выпуклая линейная комбинация последовательностей того же множества Γ.

Другими словами, множество последовательностей Γ выпукло относительно полугруппы w'-вращений тогда и только тогда, когда для любой последовательности J_α из Γ и произвольного слова w' мы имеем

$$J_\alpha D_{w'} = \sum_{J_\beta \in \Gamma} a_{\alpha\beta}(w') J_\beta,$$

где все числа $a_{\alpha\beta}(w')$ неотрицательны. Обозначим как H_Γ матрицу (в общем случае, счетного порядка), строки которой перечисляют все последовательности множества Γ:

$$J_\Gamma = \begin{pmatrix} \cdots \\ J \\ \cdots \end{pmatrix}$$

Тогда, если ввести матрицы с неотрицательными элементами $A(w) = \|a_{\alpha\beta}(w)\|$, то из определения вытекает, что

$$H_\Gamma D(w) = A(w) H_\Gamma.$$

Система матриц $\langle A(y), y \in Y^* \rangle$ при определенных условиях (см. ниже) определяет вероятностный автомат, который генерирует последовательность случайных кодов J как выходную последовательность, а матрица H_Γ определяет «проекцию»

$$J_{w'} = \alpha(w') H_\Gamma$$

пространства E_μ на пространство E_A,

$$E_A = \mathrm{Lin}\{\alpha(w) = \alpha_0 A(w), w \in Y^*\},$$

в котором функционирует вероятностный автомат A.

Определение 11. *Опорное множество* $\Gamma(\Omega)$ *для множества* $\Omega, \Omega \subset E_\mu$, — это такое любое подмножество E_μ, выпуклое линейное замыкание которого содержит в себе множество Ω.

Заметим, что система

$$\langle Y, Y, Y^*, \{D(y), y \in Y\}\rangle$$

задает детерминированный автомат со счетным числом состояний, который определен независимо от конкретной последовательности J, исключая алфавит Y. Пусть конструируется базис в E_μ из элементов множества L_μ. Имеется четыре возможности: размерность $\dim(E_\mu)$ счетная, размерность $\dim(E_\mu)$ конечная, пространство E_μ содержит некоторое конечное опорное множество относительно системы преобразований $D(y)$, $y \in Y$. Последний, четвертый, случай учитывает еще одну дополнительную возможность — когда опорное множество полудетерминированно, иначе говоря, когда для любого преобразования $D(y)$, $y \in Y$, элементы опорного множества переходят в элементы опорного же множества. В соответствии с этими вариантами мы получаем определенные классы последовательностей случайных кодов.

Характеристика некоторых классов случайных последовательностей

Случай, когда $\dim(E_\mu)$ счетна, не требует большей детализации, он рассматривается в теореме 9. Далее всюду предполагается, что размерность $\dim(E_\mu)$ конечна. Для формулировки соответствующих теорем мы будем рассматривать последовательности случайных кодов как многотактные каналы с единственной буквой входного алфавита и используем теоремы 3 и 5. Так что, пусть $\Sigma_1 = \{w_1), \ldots, (w_k)\}$, $\Sigma_2 = \{(w'_1), \ldots, (w'_k)\}$ — две произвольные последовательности слов из множества Y^* и матрица

$$R_{\Sigma_1, \Sigma_2} = \begin{pmatrix} \mu(w_1 w'_1) & \ldots & \mu(w_1 w'_k) \\ \ldots & \ldots & \ldots \\ \mu(w_k w'_1) & \ldots & \mu(w_k w'_k) \end{pmatrix}$$

— составная последовательностная матрица со входным множеством Σ_1 и выходным множеством Σ_2.

Теорема 11. *Для того, чтобы случайная последовательность* $\mu(w)$ *была слабо конечно-автоматна, необходимо и достаточно, чтобы для каждой пары* Σ_1 *и* Σ_2 *матрица* R_{Σ_1, Σ_2} *имела* *конечный ранг. Этот ранг равен числу состояний минимального псевдо-вероятностного автомата, представляющего эту последовательность* $\mu(w)$.

Другой путь описания условий слабой конечно-автоматности случайной последовательности доставляет линейное пространство E_μ. Очевидно, что имеет место следующее утверждение.

Теорема 12. *Для того, чтобы последовательность случайных кодов* $J = \langle \mu(w), w \in Y^* \rangle$ *была слабо конечно-автоматна, необходимо и достаточно, чтобы выполнялось условие*

$$\dim E_\mu < \infty.$$

Для того, чтобы получить критерий конечно-автоматности случайной последовательности $\mu(w)$, используем вновь методологию, развитую для многотактных каналов, и свойство выпуклости и опорности множества $\Gamma(\mu(w))$ случайной последовательности $\mu(w)$. Тогда мы получаем следующую теорему.

Теорема 13. *Для того, чтобы последовательность случайных кодов* $\mu(w)$ *была конечно-автоматной, необходимо и достаточно, чтобы в пространстве* E_μ *для множества всех состояний последовательности* $\mu(w)$ *существовало конечное опорное множество, выпуклое относительно полугруппы всех* w*-вращений. Число состояний вероятностного автомата* A, *представляющего эту последовательность, может быть выбрано равным мощности множества* $\Gamma(\mu(w))$.

Сравнивая теоремы 1, 7 и следствие 1, мы можем сформулировать и другой критерий для описания конечно-автоматности последовательности случайных кодов.

Теорема 14. *Для того, чтобы последовательность случайных кодов* $J = \langle \mu(w), w \in Y^* \rangle$ *была конечно-автоматной, необходимо и достаточно, чтобы существовал автономный вероятностный автомат с конечным числом состояний, генерирующий последовательность* $\mu(w)$ *как свою выходную последовательность.*

Сравнение теорем 1 и 14 приводит к следующей важной теореме.

Теорема 15. *Для того, чтобы последовательность случайных кодов* $J = \langle \mu(w), w \in Y^* \rangle$ *была функцией конечной однородной цепи Маркова, необходимо и достаточно, чтобы она была выходной последовательностью конечного детерминированного автомата со стационарной, с независимыми значениями, входной случайной последовательностью.*

Следствие 3. *Класс функций однородных конечных цепей Маркова замкнут относительно конечно-автоматных преобразований детерминированными автоматами.*

Другую форму этой теоремы дает следующая теорема.

Теорема 16. *Для того, чтобы последовательность случайных кодов* $\mu(w)$ *была конечно-автоматной, необходимо и достаточно, чтобы существовала стационарная последовательность случайных кодов с независимыми значениями, последовательностно ее имплицирующая и отображение свободных полугрупп, определенных алфавитами этой последовательности, было бы конечно-автоматным.*

Конечно-автоматная случайная последовательность может иметь, однако, неограниченное число различных состояний. Элементарный пример доставляет последовательность случайный кодов, генерируемая вероятностным автоматом с двумя состояниями и двумя символами выходного алфавита, который имеет одну из матриц переходов вида:

$$A(y_1) = \begin{pmatrix} 1/2 & 1/4 \\ 0 & 1/2 \end{pmatrix}$$

и начальный вектор состояний $\mu = (1, 0)$. Характеристику класса случайных последовательностей с конечным числом различных состояний дает следующая теорема.

Теорема 17. *Для того, чтобы последовательность случайных кодов $J = \langle \mu(w), w \in Y^* \rangle$ имела конечное число различных состояний, необходимо и достаточно, чтобы существовал такой конечный детерминированный автомат $A = \langle Y, S, \delta(s, y) \rangle$, что вероятности любого начального куска q этой последовательности $\mu(q)$ вычислялись бы в форме*

$$\mu(y_1 \ldots y_k) = \mu_{s_0}(y_1) \ldots x_{s_{k-1}}(y_k),$$

где последовательность индексов $s_0, \ldots, s_{k-1}$ определяется как последовательность состояний некоторого детерминированного автомата A для входного слова q.

Таким образом, в множестве рассмотренных классов случайных последовательностей возникает следующая иерархия, определяемая автоматным способом их генерирования. Обозначим как $\Xi(Y)$ класс всех случайных последовательностей, определенных над алфавитом Y. Из теоремы 9 следует, что каждая последовательность случайных кодов может быть получена в виде выходной последовательности подходящего автономного вероятностного автомата. В том случае, если существует конечный автономный вероятностный автомат, порождающий выходную случайную последовательность, мы говорим, что она принадлежит классу $\Xi_{pf}(Y)$ всех конечно-автоматных случайных последовательностей. Эти случайные последовательности могут быть порождаемы конечным вероятностным автоматом, однако, иметь бесконечное число состояний. Из теорем 13–16 вытекает, что класс $\Xi_{pf}(Y)$ совпадает с классом функций конечных однородных марковских цепей. Существует еще одна возможность описания функций однородных цепей Маркова. Допустим, что случайная последовательность J получена как выход конечного детерминированного автомата общего вида со стационарной, с взаимно независимыми значениями, случайной последовательностью на входе. Это будет функция конечной однородной цепи Маркова из класса $\Xi_{dfg}(Y)$. Таким образом, имеем

$$\Xi_{pf} = \Xi_{dfg}.$$

Дальше, пусть для случайной последовательности J существует конечный автономный полудетерминированный автомат, порождающий ее с фиксированным начальным состоянием. Тогда последовательность J принадлежит классу случайных последовательностей $\Xi_d f(Y)$ с конечным числом состояний. В том случае, если для случайной последовательности J существует конечный псевдо-вероятностный автомат, порождающий ее как свою выходную последовательность, мы относим ее в класс $\Xi_{ppf}(Y)$. Наконец, класс конечных однородных цепей Маркова $\Xi_{dfn}(S)$ мы получаем, когда рассматривается детерминированный конечный автомат без выхода (рассматривается случайная последовательность состояний автомата). Таким образом, рассмотренные классы удовлетворяют следующей цепочке включений:

$$\Xi \supset \Xi_{ppf} \supset \Xi_{pf} = \Xi_{dfg} \supset \Xi_{sdf}.$$

Последовательности пар случайных кодов

Одним из направлений дальнейшего развития автоматной теории последовательностей случайных кодов, наряду с задачей синтеза последовательности с заданными свойствами, является задача декомпозиции случайной последовательности на более простые, в том или ином смысле, компоненты. Эта постановка необычна с точки зрения теории вероятностей, но автоматный подход позволяет рассматривать подобные задачи, методология решения которых предопределяется структурной теорией вероятностных автоматов. Мы наметим один подход к решению на примере наиболее простой задачи в этом ряду — декомпозиции случайной последовательности в пару параллельных последовательностей случайных кодов. Рассмотрим такую ситуацию, когда на входе вероятностного автомата задана случайная последовательность. Объект

$$J = \langle \mu(v, w), |v| = |w|, v \in X^*, w \in Y^* \rangle$$

называется *последовательностью пар случайных кодов*, если словарная функция $\mu(v, w)$

$$\mu\colon (X \times Y)^* \longrightarrow [0, 1],$$

удовлетворяет условиям:

$$1)\mu(e, e) = 1, \qquad 2) \sum_{x \in X, y \in Y} \mu(vx, wy) = \mu(v, w).$$

Последовательность J_x, определенную словарной функцией

$$\mu(v) = \sum_{|w| = |v|} \mu(v, w),$$

будем называть *левой последовательностью* случайной последовательности J.

Многотактный канал $\tau(J)$, заданный условиями

$$\tau(w/v) = \begin{cases} 0, & \text{если } |v| \neq |w|, \\ \mu(v, w)/\mu(v), & \text{если } |v| = |w|, \mu(v) \neq 0, \\ \text{произвольное распределение,} & \text{если } \mu(v) = 0, \end{cases}$$

называется многотактным каналом, *ассоциированным* с J.

Определение 12. Последовательность пар случайных кодов J *представлена* в вероятностном автомате A (с начальным вектором состояний $\boldsymbol{\mu}(e)$), если ассоциированный многотактный канал $\tau(J)$ совпадает с многотактным автоматным каналом $\tau_A(w/v)$, представленным в этом автомате A.

Сравнивая условия теорем 1 и 2, мы получаем

Замечание 6. Произвольная последовательность пар случайных кодов определяет автоматный многотактный канал (и представима в вероятностном автомате).

Аналогично случаю автоматного многотактного канала, вводится понятие состояния случайной последовательности. Пусть $|v| = |w|$, $\mu(w/v) \neq 0$. Мы говорим, что

$$\frac{\mu(q'q/p'p)}{\mu(q'/p')} = \mu_{p',q'}(p, q)$$

есть (v', w')-*состояние последовательности* J.

Наибольший интерес представляет класс последовательностей пар случайных кодов с конечным числом состояний. Нижеследующая теорема описывает такие последовательности в терминах корреляции составляющих ее случайных кодов.

Теорема 18. *Для того, чтобы последовательность пар случайных кодов J имела конечное число состояний, необходимо и достаточно, чтобы конечное число состояний имела ее левая последовательность J_x и существовали*

1) *конечная система условных распределений вероятности* $\tau_a(y/x)$, $a \in T = \{1, \ldots, N\}$,

2) *словарная функция* $a(v, w)$, *принимающая конечное число целочисленных значений,* a: $(X \times Y)^* \longrightarrow T$, *удовлетворяющая условиям:*

$$a(v_1, w_1) = a(v_2, w_2) \longrightarrow a(v_1 x, w_1 y) = a(v_2 x, w_2 y),$$

такая, что для любой пары слов одинаковой длины (v, w), $\mu(v) \neq 0$, *условная вероятность для пары слов* (vx, wy) *определяется формулой:*

$$\mu(wy/vx) = \mu(w/v)\tau_{a(v,w)}(y/x).$$

Эту теорему можно сформулировать также в терминах полудетерминированного автомата.

Следствие 4. *Для того, чтобы последовательность пар случайных кодов* J *имела конечное число состояний, необходимо и достаточно, чтобы левая последовательность* J_x *имела конечное число состояний и существовал такой конечный полудетерминированный автомат*

$$D = \langle X, Y, S, \delta(d, y/a, x)\rangle,$$

что условная вероятность $\mu(w/v)$ *для каждой пары слов одинаковой длины* (v, w) *вычислялась в форме*

$$\mu(y_1, \ldots, y_k/x_1, \ldots, x_k) = \tau_{a_0}(y_1/x_1) \cdots \tau_{a_{k-1}}(y_k/x_k),$$

где последовательность индексов $a_0, \ldots, a_{k-1}$ — *это последовательность состояний автомата* D, *соответствующая входно-выходной последовательности* $(x_1, \ldots, x_k, y_1, \ldots, y_k)$.

Необходимые и достаточные условия конечно-автоматности и слабой конечно-автоматности последовательности пар случайных кодов могут быть сформулированы аналогично условиям теорем 3 и 5.

Просуммируем — какого типа последовательность пар случайных кодов $\mu(v, w)$ получается при определенных предположениях относительно природы правой последовательности $\mu(v)$ и последовательности $\mu(w/v)$ для каждого фиксированного слова w. Легко видеть, что эту информацию дает следующая сводная таблица:

$\mu(p)\backslash\mu(q/p)$	*ppf*	*pf*	*sdf*
ppf	*ppf*	*ppf*	*ppf*
pf	*ppf*	*pf*	*pf*
sdf	*ppf*	*pf*	*sdf*

СПИСОК ЛИТЕРАТУРЫ

1. Бухараев Р. Г. Основы теории вероятностных автоматов. — М.: Наука, 1985.
2. Bukharaev R. G. Theorie der stochastischen Automaten. — Stuttgart: B. G. Teubner, 1995.
3. Carlyle J. W. Reduced forms for stochastic sequential machines // J. Math. Analysis and Appl. — 1963. — V. 7, № 2. — P. 167–175.
4. Davis A. S. Markov chains as random input automata // Amer. Math. Monthly. — 1961. — V. 68, № 3. — P. 264–267.
5. Rabin M. O. Probabilistic automata // Inf. and Control. — 1963. — V. 6, № 3.

Поступило в редакцию 16 V 2000