В. М. Захаров, Ш. Р. Нурутдинов, С. В. Шалагин, Синтез автономных вероятностных автоматов на основе полей Галуа,
Исслед. по информ., 2000, выпуск 2, 107–116

СИНТЕЗ АВТОНОМНЫХ ВЕРОЯТНОСТНЫХ АВТОМАТОВ НА ОСНОВЕ ПОЛЕЙ ГАЛУА

В.М. Захаров, Ш.Р. Нурутдинов, С.В. Шалагин

Предлагается алгоритмический подход к синтезу вероятностных автоматов, выполняющих роль генератора последовательностей случайных кодов, основанный на представлении автомата однородной вычислительной структурой в конечном поле Галуа.

Алгоритм синтеза дан для семейства автономных вероятностных автоматов, позволяющих получить простые и сложные цепи Маркова и различные немарковские случайные последовательности.

Одним из известных подходов к синтезу специализированных цифровых устройств в однородных структурах является использование аппарата полей Галуа. На основе вычислений в конечных полях эффективно реализуется потоковая система обработки n-мерных двоичных векторов. Реализация такой обработки показана, в частности, в [1] для построения систолических структур, в [2, 3] – для синтеза комбинационных схем и автоматов с памятью.

В данной работе решается задача синтеза автономных вероятностных автоматов на основе полей Галуа. Решение задачи сведено к синтезу управляемого генератора случайных кодов.

Определения автономных вероятностных автоматов

Автономный вероятностный автомат (АВА) является частным случаем вероятностного автомата (ВА) общего вида, задаваемого системой:

$$A = (X, Y, S, \mu(s', y/s, x)),$$

где X и Y - конечные входной и выходной алфавиты, S - конечное множество состояний, через $\mu(s', y/s, x)$ обозначается условная вероятность того, что ВА, находясь в состоянии $s \in S$ и получив на вход букву $x \in X$, перейдёт в новое состояние $s' \in S$ и выдаст букву $y \in Y$. Рассматривая ВА без входа, то есть случай, когда X содержит только одну букву, будем иметь систему:

$$ABA = (Y, S, \mu(s', y/s)), \qquad (1)$$

которая определяет семейство автономных вероятностных автоматов, различающихся ограничениями на Y, S и способами задания $\mu(s', y/s)$.

Автомат (1) выполняет роль генератора дискретных случайных последовательностей с дискретным временем (СП). Ограничения, накладываемые на (1) позволяют получить семейство классов СП (простые и сложные цепи Маркова [4] и различные немарковские СП [5, 6]).

Введём в рассмотрение следующие типы автономных вероятностных автоматов, следуя [5, 6, 7].

Определение 1. Автономным вероятностным автоматом типа $A(1)$ будем называть систему

$$A(1) = (S, P_S, \pi_0), \tag{2}$$

где $S = \{s_1, s_2, ..., s_n\}$ - конечное множество состояний, P_S - стохастическая матрица размера $n \times n$, $\pi_0 = \{\pi_{ij}\}$, $i, j = \overline{1,n}$ - n-мерный стохастический вектор, задающий начальное распределение вероятностей состояний. Задание АВА в виде системы (2) эквивалентно заданию простой однородной цепи Маркова (ЦМ).

Определение 2. Автономным вероятностным автоматом типа $A(2)$ будем называть систему

$$A(2) = (Q, S, \lambda(q,s)), \tag{3}$$

где S - тот же объект, что и в (2), Q - дискретная случайная величина, принимающая конечное число значений $q_1, q_2, ..., q_l$ на входе $A(2)$ с вероятностями $p_1, p_2, ..., p_l$,

$$\sum_{i=1}^{l} p_i = 1, \quad 0 \le p_i \le 1,$$

$\lambda(q,s)$ - функция переходов, ставящая в соответствие паре (q,s) однозначно новое состояние $s' \in S$.

Последовательность состояний автомата (3) является простой однородной ЦМ, определяемой стохастической матрицей P, которая вычисляется по формуле

$$P = \sum_{k=1}^{l} p_k M(q_k), \tag{4}$$

где $M(q_k)$ - простая матрица (по терминологии [7]), соответствующая входной букве q_k. Элементы матрицы $M(q_k)$, обозначим их через $\pi_{ij}(q_k)$, $i, j = \overline{1,n}$, определяются из соотношения

$$\pi_{ij}(q_k) = \begin{cases} 1, & \lambda(q_k, s_i) = s_j \\ 0, & \lambda(q_k, s_i) \neq s_j \end{cases}, i, j = \overline{1,n}. \tag{5}$$

Далее определим автономные вероятностные автоматы с выходом. Заметим, что выходная последовательность АВА с выходом представляет

собой функцию простой ЦМ, то есть в общем случае СП на выходе не является ЦМ [4].

Определение 3. Автономным вероятностным автоматом типа $A(3)$ будем называть систему

$$A_1(3) = (A(1), Y, y = \delta(s)), \tag{6}$$

где $A(1)$- автомат (2), $Y = \{y_1, y_2, ..., y_m\}$ - конечный выходной алфавит, $y = \delta(s)$ - функция выхода, однозначно ставящая в соответствие состоянию $s \in S$ букву $y \in Y$.

Автоматом типа $A(3)$ будем называть также и систему

$$A_2(3) = (A(2), Y, y = \delta(s)),$$

где Y и $\delta(s)$ те же, что и в (6).

Определение 4. Автономным вероятностным автоматом типа $A(4)$ будем называть систему

$$A(4) = (A(1), Y, \mu), \tag{7}$$

где $A(1)$, Y - те же объекты, что и в (6), μ - функция выхода, задаваемая стохастической матрицей P_y размера $n \times m$, имеющей вид

$$P_y = \|p_{ij}\|_{n \times m} = \begin{pmatrix} P(y_1/s_1) & P(y_2/s_1) & \dots & P(y_m/s_1) \\ P(y_1/s_2) & P(y_2/s_2) & \dots & P(y_m/s_2) \\ \dots & \dots & \dots & \dots \\ P(y_1/s_n) & P(y_2/s_n) & \dots & P(y_m/s_n) \end{pmatrix}, \tag{8}$$

где элемент p_{ij}, $i = \overline{1,n}$, $j = \overline{1,m}$, определяет вероятность появления буквы y_j при условии, что $A(4)$ находится в состоянии s_i.

Определение 5. Автономным вероятностным автоматом типа $A(5)$ будем называть систему

$$A(5) = (A_{n\partial}, Y, \mu), \tag{9}$$

где Y, μ, те же объекты, что и в (7), через $A_{n\partial}$ обозначен конечный детерминированный автомат (КДА), реализующий подстановку, то есть заданный множеством состояний S и функцией перехода $\lambda(s)$.

Определение 6. Автономным вероятностным автоматом типа $A(5)$ будем называть систему

$$A(6) = (U, S, \lambda(u,s), Y, \mu) = (A_n, Y, \mu), \tag{10}$$

где Y, μ то же самые, что и в (7), A_n - конечный детерминированный полуавтомат, заданный множеством состояний S, входным алфавитом U=Y

(совпадающим с выходным алфавитом Y) и функцией перехода $\lambda(u,s)$.

Определение 7. Автономным вероятностным автоматом типа $A(7)$ будем называть систему

$$A(7) = (A_M, BA_{бп}), \tag{11}$$

Здесь:

A_M - КДА типа Мура, задаваемый системой

$$A_M = (U, S, X, \lambda(u,s), \delta(s)),$$

где $U = \{u_1, u_2, ..., u_m\}$ - входной алфавит,

$X = \{x_1, x_2, ..., x_h\}$ - выходной алфавит,

$S = \{s_1, s_2, ..., s_n\}$ - множество состояний,

$\lambda(u,s)$ - функция перехода и $\delta(s)$ - функция выхода.

$BA_{бп}$ - вероятностный автомат без памяти. Он задаётся системой:

$$BA_{бп} = (Z, Y, \mu(y/x)),$$

где $Z = \{z_1, z_2, ..., z_h\} = X$ - входной алфавит, совпадающий с X, $Y = U$ - выходной алфавит, совпадающий с U. Функция $\mu(y/z)$, $z \in Z$, определяет условную вероятность появления буквы y на выходе $BA_{бп}$, если на его вход подана буква z. Функцию $\mu(y/z)$ будем задавать стохастической матрицей P_Z размера $h \times m$ вида:

$$P_Z = \|p_{ij}\|_{h \times m} = \begin{pmatrix} P(y_1/z_1) & P(y_2/z_1) & \dots & P(y_m/z_1) \\ P(y_1/z_2) & P(y_2/z_2) & \dots & P(y_m/z_2) \\ \dots & \dots & \dots & \dots \\ P(y_1/z_h) & P(y_2/z_h) & \dots & P(y_m/z_h) \end{pmatrix}, \tag{12}$$

где элемент p_{ij}, $i = \overline{1,h}$, $j = \overline{1,m}$, - определяет вероятность появления буквы y_j при условии, что на вход $BA_{бп}$ подана буква z_i.

Структурное представление АВА

Рассмотрим структурные модели определённых выше АВА. Будем использовать известный подход структурного синтеза ВА, основанный на представлении ВА в виде последовательностной композиции управляемого генератора дискретной случайной величины (УГСВ) и КДА [5].

Генератор называется управляемым, если требуется, чтобы смена закона распределения производилась со скоростью, сравнимой с быстродействием самого устройства. Задача синтеза управляемого генератора случайных кодов (УГСК) есть задача синтеза некоторого детерминированно-

го преобразователя исходного случайного процесса или случайного кода в требуемый случайный код [5]. Данный преобразователь можно построить, используя представление $BA_{бп}$ однородной вычислительной структурой с управляющими входами. Значения управляющих входов определяют конкретные преобразования исходного случайного кода в определённые случайные коды.

На рис. 1 изображена структурная модель автоматов типа $A(1)$ и $A(2)$, где блок ГСВ выполняет функцию генератора случайной величины Q, а КДА реализует функцию перехода $\lambda(q,s)=s'$.

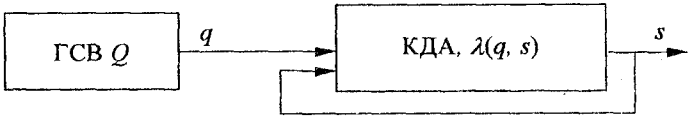

Рис. 1.

АВА типа $A(2)$ представляется данной структурой по определению. АВА типа $A(1)$ сводится к этой композиции на основе представления исходной матрицы P_S в виде соотношения (4):

$$P_S=\sum_{k=1}^{l} p_k M(q_k),$$

где $l \le n(n-1)$. По матрице $M(q_k)$ функцию $\lambda(q,s)$ задают следующим образом. Если в $M(q_k)$ элемент $\pi_{ij}(q_k)=1$, то паре (q_k,s_i) ставится в соответствие однозначно состояние s_j, $i,j=\overline{1,n}$ (см. (5)).

Структурная модель автомата типа $A(3)$ изображена на рис. 2, где блок 2 является КДА типа Мура, функции перехода и выходы задаются, соответственно, функциями $\lambda(q,s)=s'$ и $\delta(s)=y$.

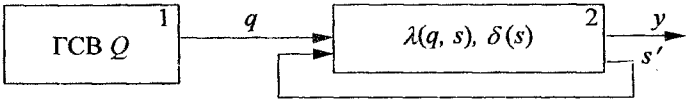

Рис. 2.

Автомат типа $A(4)$ представлен структурной моделью на рис. 3, состоящей из двух частей. Часть I (блоки 1, 2) реализует стохастическую матрицу P_S, а часть II (блок 3) выполняет функцию $\mu(y/s)$. Так как $\mu(y/s)$ задана стохастической матрицей, то блок 3 может быть представлен последовательной композицией по аналогии с частью I на основе разложения матрицы (8) в виде суммы

$$P_y = \sum_{k=1}^{l} p'_k M(q'_k),\ \ l \le n(n-1),\ \ 0 \le p'_k \le 1,\ \ \sum_{k=1}^{l} p'_k = 1,$$

где $M(q'_k)$ - простые матрицы размера $n \times m$.

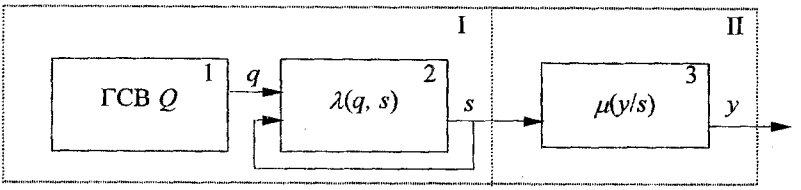

Рис. 3.

Соответствующий вариант структуры автомата $A(4)$ представлен на рис. 4, где часть II содержит блоки 3 и 4.

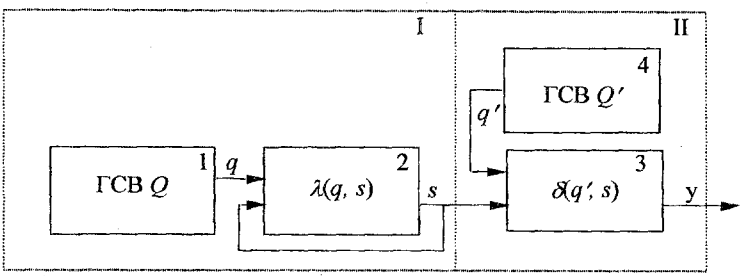

Рис. 4.

Блок 4 генерирует дискретную случайную величину

$$Q': \begin{array}{|c|c|c|c|} \hline q'_1 & q'_2 & \cdots & q' \\ \hline p'_1 & p'_2 & \cdots & p'_l \\ \hline \end{array}.$$

Значения q'_k, $k = \overline{1,l}$, поступают на вход блока 3 с вероятностями p'_k, определяемыми из разложения матрицы P_y. Блок 3 реализует функцию выхода $\delta(s) = y$, которая задаётся по матрице $M(q'_k)$ размера $n \times m$ рассмотренным выше способом.

На рис. 5 изображена структурная модель автомата типа $A(5)$, которая представляет собой частный случай структуры на рис. 4: часть I реализуется автоматом подстановки $A_{n\partial}$.

Структурная модель автомата типа $A(6)$ дана на рис. 6. В этой структуре введена обратная связь, на основе которой полуавтомат A_n реализует функцию перехода $\lambda(u,s)$.

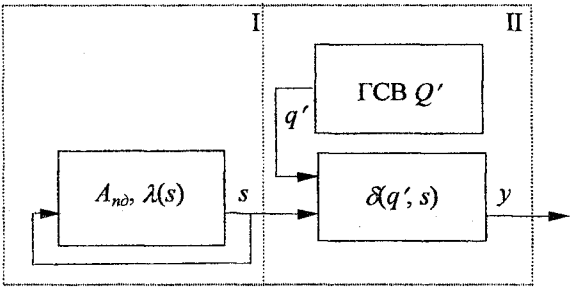

Рис. 5.

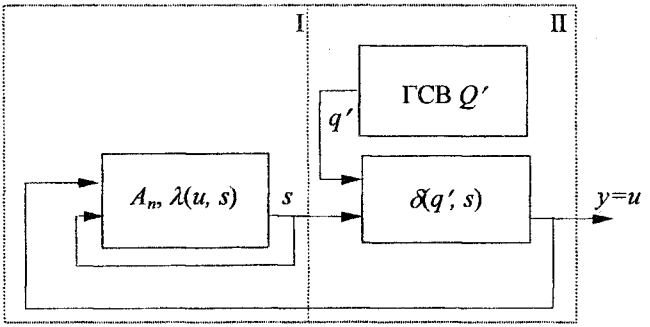

Рис. 6.

Структурная модель автомата типа $A(7)$ является развитием структуры автомата типа $A(6)$. Она изображена на рис. 7. На этой схеме часть I реализует автомат Мура, а часть II - вероятностный автомат $BA_{бп}$, структурные части которого Q' и $\delta(q',z)$ определяются по разложению матрицы (12) в виде, аналогичном разложению матрицы P_y, где простые матрицы $M(q'_k)$ имеют размер $h \times m$.

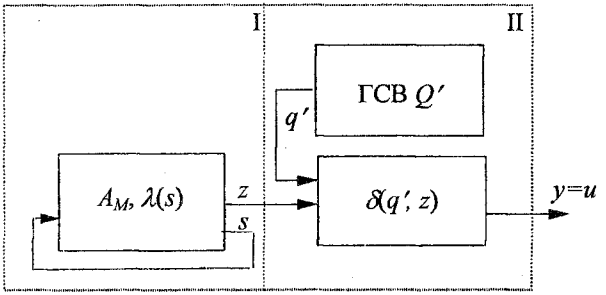

Рис. 7.

Синтез управляемых генераторов случайных кодов

Представление структуры АВА в виде рассмотренных композиций сводит задачу синтеза структуры АВА к синтезу УГСК и КДА. Задача синтеза КДА в поле Галуа решена в [3, 8]. В этом разделе приведём решение в поле Галуа для управляемого генератора случайных кодов.

Одноканальный УГСК. Пусть x n-мерная дискретная случайная величина (ДСВ), ряд распределения которой задан таблицей вида

$$x:\begin{array}{|c|c|c|c|}\hline x_1 & x_2 & \dots & x_l \\ \hline p_1 & p_2 & \cdots & p_l \\ \hline \end{array}, \qquad (13)$$

где $\sum_{i=1}^{l} p_i = 1$. Пусть $p_i = s_i / q_i$, где s_i, q_i - положительные целые. Представим таблицу (13) в виде отображения поля Галуа на себя. Для этого закодируем значения переменной x элементами данного поля. Построим поле $G = GF(2^n)$. Пусть $r = н.о.к.(q_1, q_2, ..., q_l)$, найдём $\min(n): n \geq \log_2 r$. Таблицу (13) реализуем в виде отображения подмножеств поля G на его элементы. Для этого произвольным образом закодируем значения переменной x элементами поля G. Отображение имеет вид

$$G_1 \to x_1; G_2 \to x_2; ...; G_l \to x_l, \qquad (14)$$

где $G_i \in G$, $G_i \cap G_j = \varnothing$, $i \neq j$.

Мощность подмножеств G_i определим из условия $|G_i| = rs_i / q_i$, $i = \overline{1,l}$. Ввиду универсальности синтезируемой однородной структуры, распределение элементов поля G по подмножествам $G_1, G_2, ..., G_l$ делается произвольным образом. В результате имеем отображение (14), которое задано множеством G и имеет значения внутри данного множества.

Реализуем (14) в виде многочлена от одной переменной над G:

$$g(x) = \sum_{i=0}^{l-1} a_i x^i, \qquad a_i, x \in G. \qquad (15)$$

Вычисление значения многочлена $g(x)$ в точках $x = x_i$ реализуем однородной последовательной вычислительной структурой - каналом. Он состоит из $2n$ одинаковых блоков [3, 8].

В результате построена однородная структура, реализующая ДСВ, заданную таблицей (13). При этом для различных таблиц типа (13) получим различные наборы коэффициентов $a_i, i = \overline{0, l-1}$, многочлена (15). Данные наборы подаются на управляющие входы канала. Для реальных случайных величин, состоящих из более чем 20 двоичных разрядов, многочлен (15) содержит более 2^{20} слагаемых. В следующем разделе рассматривается

возможность уменьшения показателя (степени) поля Галуа, в котором производятся преобразования.

Многоканальный УГСК. Многоканальный УГСК генерирует случайную величину, которая является композицией независимых случайных величин.

Пусть n=2m. Тогда n-мерная ДСВ x представима в виде $x = x_1 + x_2 2^m$, где x_1, x_2 - m-мерные независимые ДСВ. Определим ряд распределения вероятностей ДСВ x_1 и x_2, если известен ряд распределения (13) ДСВ x. Для ряда распределения ДСВ x аналогом является матрица распределения двух ДСВ (x_1, x_2) - прямоугольная матрица, в которой записаны все вероятности $p_{ij} = p_{(i-1)s+j}$, где $p_k, k = \overline{1,2^m}$ взяты из таблицы (13), $i, j = \overline{1,s}$, $s = 2^m$. Запишем матрицу распределения двух ДСВ (x_1, x_2) при известной таблице распределения ДСВ x (13) в виде

$$T = \left| t_{ij} \right|_{s \times s}. \tag{16}$$

Зная матрицу распределения двух ДСВ (x_1, x_2), можно найти законы распределения ДСВ x_1 и x_2 по отдельности

$$P\{x_1 = x_{1,i}\} = \sum_{j=1}^{s} t_{ij}, \quad P\{x_2 = x_{2,j}\} = \sum_{i=1}^{s} t_{ij}. \tag{17}$$

Переменные x_1 и x_2 являются независимыми ДСВ с матрицей распределения (16), если выполняется

$$t_{ij} = P\{x_1 = x_{1,i}\} P\{x_2 = x_{2,j}\}, \quad i, j = \overline{1,s}, \quad s = 2^m. \tag{18}$$

На основе вышеизложенного материала предлагается следующий алгоритм синтеза многоканального УГСК для ДСВ x, представленной в виде композиции двух ДСВ x_1 и x_2.

Шаг 1. Представление n-мерной ДСВ x в виде $x = x_1 + x_2 2^m$.

Шаг 2. Построение матрицы вида (16) по заданной таблице (13).

Шаг 3. На основе (17) построение таблиц распределений ДСВ x_1 и x_2.

Шаг 4. Проверка независимости ДСВ x_1 и x_2 по условию (18).

Шаг 5. В случае прохождения шага 4, таблицы распределений для ДСВ x_1 и x_2 реализуются двумя однородными вычислительными структурами, которые описаны в разделе 3.1.

В результате получен 2-х канальный УГСК для величины x. На входы каналов подаются равномерно распределённые ДСВ, а с выходов снимаются значения ДСВ x_1 и x_2, которые в совокупности составляют значение ДСВ x. Данные идеи могут быть использованы и при синтезе f-канального УГСК, $f \geq 2$. Пусть $n = fm$. Представим x в следующем виде:

$x = x_i 2^{im}$, где $i = \overline{1, f}$. Получим систему из f ДСВ. Пусть они независимы. По заданному ряду распределения (13) построим f-мерную матрицу распределений

$$T_{i_1 \times i_2 \times .. \times i_f} \qquad i_1 i_2 ... i_f = \overline{1, s},\ s = 2^m. \tag{19}$$

Вероятности матрицы (19) связаны с вероятностями в таблице (13) следующим образом:

$$T_{i_1 i_2 .. i_f} = T_k, \text{ где } k = (i_1 - 1)s^{f-1} + (i_2 - 1)s^{f-2} + ... + (i_{f-1} - 1)s + i_f.$$

Вероятности в таблицах распределения ДСВ $x_1, x_2, ..., x_f$ вычисляются согласно

$$\begin{cases} P\{x_1 = x_{1,i_1}\} = \sum\limits_{i_2 ... i_f = 1}^{s} T_{i_1 i_2 ... i_f}, \\ P\{x_2 = x_{2,i_2}\} = \sum\limits_{i_1, i_3 ... i_f = 1}^{s} T_{i_1 i_2 ... i_f}, \\ \qquad ... \\ P\{x_f = x_{f,i_f}\} = \sum\limits_{i_1, i_2, ..., i_{f-1} = 1}^{s} T_{i_1 i_2 ... i_f}, \end{cases}.$$

Здесь $s = 2^m$. Условие независимости ДСВ $x_1, x_2, ..., x_f$ примет вид:

$$P_{i_1 i_2 .. i_f} = P\{x_1 = x_{1,i_1}\} P\{x_2 = x_{2,i_2}\} ... P\{x_f = x_{f,i_f}\}.$$

Описанный в данном разделе алгоритм может быть модифицирован для синтеза f-канального УГСК.

Работа поддержана грантом РФФИ № 99-01-00163 "Энтропийно-сложностные свойства дискретных вычислительных моделей"

Литература

1. Никонов В.В. и др. Систолическая обработка информации: элементная база и алгоритмы // Зарубежная радиоэлектроника. - 1987. - №7. – С. 34-52.

2. Нурутдинов Ш.Р. Реализация комбинационной схемы при помощи многочлена от нескольких переменных над конечным полем // Тезисы докл. VII Всесоюзн. конф. по теоретической кибернетике. Часть 2. – Горький, 1988. – С. 61-62.

3. Нурутдинов Ш.Р. Обеспечение отказоустойчивости сетевой модели автомата // Исследования по прикладной математике. Вып. 16. - Казань: Изд-во КГУ, 1989. - С 138-144.

4. Романовский В.И. Дискретные цепи Маркова. – М.: Гостехиздат, 1949.

5. Бухараев Р.Г., Захаров В.М. Управляемые генераторы случайных кодов. - Казань: Изд-во КГУ, 1978.

6. Альпин Ю.А., Захаров В.М. Теоретико-автоматный метод описания и моделирования случайных процессов // Вероятностные методы и кибернетика. Вып. 19. – Казань: Изд-во КГУ, 1983. – С. 10-16.

7. Поспелов Д.А. Вероятностные автоматы. – М.: Энергия, 1970.

8. Нурутдинов Ш.Р., Столов Е.Л. Перестраиваемые схемы в системах встроенного тестирования // Автоматика и телемеханика. - 1995. - №3. - С. 179-183.