УДК 004.052

С.Ю. Мельников

О задаче определения функции выходов автомата со случайным входом по статистике встречаемости слова в выходной последовательности

Рассматривается задача определения функции выходов конечного сильносвязного автомата Мура со случайным входом по относительной частоте встречаемости фиксированного слова в его выходной последовательности. Показано, что эта задача сводится к задаче дискретной минимизации модуля линейной формы.

Ключевые слова: конечный автомат, определение функции выходов, дискретная минимизация, регистр сдвига.

Рассматривается перерабатывающий последовательность независимых одинаково распределенных по полиномиальной схеме случайных величин конечный сильносвязный автомат Мура. Полиномиальная схема считается известной и заданной стохастическим вектором значений вероятностей символов входного алфавита, входная последовательность, начальное распределение и последовательность состояний считаются неизвестными. Наблюдения производятся над выходной последовательностью автомата.

С такими предположениями связан ряд прикладных и теоретических задач, рассматриваемых в литературе. Перечислим некоторые из них. Задача выбора минимального набора мультиграмм в выходной последовательности, вероятности которых характеризуют автомат, приводит к задаче анализа алгебраических свойств семейства вероятностных распределений таких мультиграмм как функций от вероятностного распределения на входе [1, 2]. Поиск новых методов вычислений приводит к задаче анализа класса функций, описывающих вероятности мультиграмм в выходной последовательности, как функций действительных переменных [3, 4]. Ряд работ [5, 6] посвящен задаче тестирования дискретных устройств путем подачи на них случайных последовательностей (тестов) и анализа статистик на выходах. В [7] для известной функции переходов автомата рассматривалась задача определения функции выходов по набору вероятностей биграмм в выходной последовательности. В данном случае при тех же условиях рассматривается задача определения функции выходов по значению вероятности одного фиксированного слова в выходной последовательности.

В первой части статьи рассматривается перерабатывающий последовательность независимых одинаково распределенных случайных величин сильносвязный автомат Мура. Вероятностной функцией для его функции выходов относительно слова γ назван предел относительной частоты встречаемости слова γ в растущих начальных отрезках выходной последовательности. Областью определения вероятностной функции является множество всевозможных распределений на входном алфавите. На множестве функций выходов введено отношение статистической эквивалентности по признаку тождественного равенства их вероятностных функций. Рассматриваются задачи определения класса эквивалентности неизвестной функции выходов по значению вероятностной функции и по статистике выборочного среднего. Показано, что задача определения класса эквивалентности неизвестной функции выходов по статистике выборочного среднего сводится к задаче дискретной минимизации модуля линейной формы.

Во второй части статьи рассматривается частный случай исследуемой задачи, соответствующий двоичному проходному регистру сдвига с неизвестной булевой функцией выходов, на вход которого поступает последовательность бернуллиевских случайных величин. Возникающая в этом случае вероятностная схема описана в [8, 9]. В п. 1 изучается информация о функции выходов, получаемая по значковой статистике выходной последовательности. На множестве булевых функций вводится отношение эквивалентности по признаку тождества их вероятностных функций. Получены точные и асимптотические выражения для числа и мощностей классов эквивалентности. Показано, что задача определения класса эквивалентности функции выходов сводится к целочисленной задаче

мимнимизации модуля линейной формы при линейных ограничениях. Для всех значений параметра бернуллиевского распределения, за исключением конечного множества «особенных распределений», при достаточной длине выходной последовательности эта задача имеет единственное решение. Исследуется строение множества «особенных распределений».

1. *Задача определения функции выходов автомата Мура, перерабатывающего последовательность независимых случайных величин*

Определение вероятностной функции

Пусть $A=(X,Y,Q,h,f)$ – конечный детерминированный сильносвязный автомат Мура, где $X=\{x_1,x_2,...,x_m\}$ – входной алфавит; $Y=\{y_1,y_2,...,y_k\}$ – выходной алфавит; $Q=\{q_1,q_2,...,q_r\}$ – множество состояний; $h:Q\times X\to Q$ – функция переходов; $f:Q\to Y$ – функция выходов. Пусть на множестве Q задано некоторое начальное вероятностное распределение $\mathbf{q^{(0)}}=\left(q_1^{(0)},q_2^{(0)},...,q_r^{(0)}\right)$, и на вход автомата A поступает последовательность независимых случайных величин $x^{(i)}$, $i=1,2,...$ с распределением $P\left(x^{(i)}=x_j\right)=p_j$, $p_j>0, j=1,2,...,m-1, p_m=1-\sum\limits_{j=1}^{m-1}p_j>0$.

Автомату A, перерабатывающему последовательность $x^{(i)}$, $i=1,2,...$, соответствует автономный вероятностный автомат, определяемый квадратными матрицами $\mathbf{M}(y)=\left(m_{ij}(y),y\in Y\right)$ порядка r, где

$$m_{ij}(y)=\sum_{\substack{x\in X\\ h(q_i,x)=q_j\\ f(q_i)=y}}p_x\ .$$

Пусть $\gamma=y^{(1)}y^{(2)}...y^{(l)}$, $y^{(i)}\in Y$, $i=1,2,...,l$. Положим $\mathbf{M}=\sum\limits_{y\in Y}\mathbf{M}(y)$, $\mathbf{M}(\lambda)=\mathbf{E}$, $\mathbf{M}(\gamma)=\mathbf{M}\left(y^{(1)}\right)\mathbf{M}\left(y^{(2)}\right)...\mathbf{M}\left(y^{(l)}\right)$, где λ – пустое слово, $\mathbf{E}$ – единичная матрица порядка r. Через $\boldsymbol{\eta}(\gamma)$ обозначим сумму столбцов матрицы $\mathbf{M}(\gamma)$, $\boldsymbol{\eta}(\gamma)=\mathbf{M}(\gamma)(\mathbf{11...1})^T$, где $(\mathbf{11...1})^T$ – вектор-столбец порядка r, составленный из единиц.

Как нетрудно видеть, последовательность состояний автомата образует эргодическую цепь Маркова с вектором начального распределения $\mathbf{q^{(0)}}$ и матрицей переходных вероятностей $\mathbf{M}$. Следовательно, существует единственный стохастический вектор $\bar{\boldsymbol{\pi}}=(\pi_1,\pi_2,...,\pi_r)$, такой, что $\bar{\boldsymbol{\pi}}\mathbf{M}=\bar{\boldsymbol{\pi}}$. Вектор $\bar{\boldsymbol{\pi}}$ не зависит от $\mathbf{q^{(0)}}$. Закон больших чисел для цепей Маркова [10. С. 61] позволяет интерпретировать величины π_i и $\bar{\boldsymbol{\pi}}\boldsymbol{\eta}(\gamma)$ как пределы относительных частот встречаемости состояния q_i и слова γ в растущих начальных отрезках последовательности состояний и выходной последовательности автомата A соответственно.

Проведенные построения относятся к вектору $\bar{\mathbf{p}}=(p_1,p_2,...,p_{m-1})$, принадлеащему связной открытой области

$$D=\left\{\bar{\mathbf{p}}=(p_1,p_2,...,p_{m-1}),\ \sum_{j=1}^{m-1}p_j<1, p_j>0, j=1,2,...,m-1\right\}$$

евклидова пространства R^{m-1}. В частности, для $m=2$ (случай автомата с двоичным входным алфавитом и бернуллиевской входной последовательности с распределением $P\{1\}=p_1$, $P\{0\}=p_0$, $p_0+p_1=1, p_0>0, p_1>0$) векторы $\bar{\boldsymbol{\pi}}$ и $\boldsymbol{\eta}(\gamma)$ являются функциями одной действительной переменной p_1. Функция $P_\gamma\left(\bar{\mathbf{p}}\right)=\bar{\boldsymbol{\pi}}\boldsymbol{\eta}(\gamma)$ называется ([1]) *вероятностной функцией автомата A для слова γ*.

Лемма 1. Вероятностная функция автомата A для слова γ представима в виде отношения двух полиномов от $\bar{\mathbf{p}}=(p_1,p_2,...,p_{m-1})$ с целыми коэффициентами:

$$P_\gamma\left(\bar{\mathbf{p}}\right)=\frac{R_\gamma\left(\bar{\mathbf{p}}\right)}{S\left(\bar{\mathbf{p}}\right)},$$

причем знаменатель $S\left(\bar{\mathbf{p}}\right)$ не зависит от γ, степени числителя и знаменателя ограничены числами $r+l$ и r соответственно: $0\le\deg S\left(\bar{\mathbf{p}}\right)\le r$, $0\le\deg R_\gamma\left(\bar{\mathbf{p}}\right)\le r+l$, где l – длина слова γ.

Доказательство. Элементы матрицы $\mathbf{M}$ являются линейными функциями от $\bar{\mathbf{p}}$, причем коэффициенты этих функций есть целые числа. Применяя правило Крамера для решения системы линейных уравнений $\bar{\boldsymbol{\pi}}\mathbf{M}=\bar{\boldsymbol{\pi}}$, получаем, что каждый из π_j представим в виде отношения двух полиномов с целыми коэффициентами, степени которых не превосходят r. Знаменатели этих отношений не зависят от j.

Элементы матрицы $\mathbf{M}(\gamma)$ являются полиномами от $\bar{\mathbf{p}}$ степеней не выше l. Следовательно, координаты вектора $\boldsymbol{\eta}(\gamma)=\mathbf{M}(\gamma)(\mathbf{11...1})^T$ обладают тем же свойством. Поскольку $P_\gamma\left(\bar{\mathbf{p}}\right)=\bar{\boldsymbol{\pi}}\boldsymbol{\eta}(\gamma)$, лемма доказана.

В [3] имеется описание вероятностных функций для знака сильносвязных автоматов с двоичными входным и выходным алфавитами.

Теорема 1 [3]. Функция $G(p)$ является вероятностной функцией для знака сильносвязного автомата тогда и только тогда, когда она удовлетворяет условиям:

1) $G(p)$ определена на интервале $(0,1)$ и принимает значения из отрезка $[0,1]$;

2) функция $G(p)$ представима в виде $Q(p)/S(p)$, где $Q(p)$ и $S(p)$ – полиномы с целыми коэффициентами, $S(p)>0$ при $p\in(0,1)$;

3) если $G(p)$ принимает значение 0 или 1 внутри интервала, то она является тождественной константой.

Задача определения неизвестной функции выходов

Пусть $\mathrm{A}=\{A=(X,Y,Q,h,f), f\in F_{r,k}\}$ – класс описанных выше конечных сильносвязных автоматов Мура, функции выходов которых принадлежат множеству $F_{r,k}$ всех функций из Q в Y. Рассмотрим возможность определения неизвестной функции выходов f автомата $A\in\mathrm{A}$ по значению его вероятностной функции $P_\gamma\left(\bar{\mathbf{p}}\right)$ для заданного $\bar{\mathbf{p}}\in D$. С целью подчеркнуть зависимость вероятностной функции от f будем обозначать ее $P_{\gamma,f}\left(\bar{\mathbf{p}}\right)$.

Функции f_1 и f_2 из $F_{r,k}$ назовем *статистически эквивалентными относительно слова* $\gamma\in Y^*$ (и примем для такого случая обозначение $f_1\approx f_2$), если $P_{\gamma,f_1}\left(\bar{\mathbf{p}}\right)=P_{\gamma,f_2}\left(\bar{\mathbf{p}}\right)$ для всех $\bar{\mathbf{p}}\in D$. Нетрудно видеть, что так введенное отношение в самом деле является отношением эквивалентности, разбивающим $F_{r,k}$ на непересекающиеся классы. Соответствующее фактор-множество обозначим $F_{r,k}\big/_{\approx}$. Очевидно, по значению вероятностной функции $P_{\gamma,f}\left(\bar{\mathbf{p}}\right)$ в точке $\bar{\mathbf{p}}\in D$ статистически эквивалентные функции выходов неразличимы, и определение функции выходов возможно лишь с точностью до класса эквивалентности. Оказывается, что класс эквивалентности можно определить «почти всегда».

Лемма 2 [11]. Пусть $S(x_1,x_2,...,x_n)$ – ненулевой полином от переменных $x_1,x_2,...,x_n$. Мера Лебега в n-мерном евклидовом пространстве множества $\left\{(x_1,x_2,...,x_n)\middle|S(x_1,x_2,...,x_n)=0\right\}$ равна нулю.

Утверждение 1. Для всех $\bar{\mathbf{p}}\in D$, за исключением некоторого множества $\Omega\subset D$, имеющего нулевую меру Лебега (в R^{m-1}), значению $P_{\gamma,f}\left(\bar{\mathbf{p}}\right)$ соответствует единственный класс эквивалентности функции f.

Доказательство. Рассмотрим семейство U функций от $\bar{\mathbf{p}}=(p_1,p_2,...,p_{m-1})$:

$$U=\left\{P_{\gamma,f}(\bar{\mathbf{p}})-P_{\gamma,g}(\bar{\mathbf{p}}),\ f,g-\text{не эквивалентные функции из } F_{r,k}\right\}.$$

Семейство U конечно, перенумеруем его произвольным образом. С помощью леммы 1 легко показать, что i-я функция из U имеет вид $u_i(\bar{\mathbf{p}})=\dfrac{R_i(\bar{\mathbf{p}})}{S(\bar{\mathbf{p}})}$, где $R_i(\bar{\mathbf{p}})$ и $S(\bar{\mathbf{p}})$ – многочлены от $\bar{p}$. По построению среди $u_i(\bar{\mathbf{p}})$ нет тождественного нуля.

Положим $\Omega=\bigcup\limits_i\left\{\bar{\mathbf{p}}\in D\,\middle|\,u_i(\bar{\mathbf{p}})=0\right\}$. По лемме 2 мера Лебега (в R^{m-1}) каждого из множеств $\left\{\bar{\mathbf{p}}\in D\,\middle|\,u_i(\bar{\mathbf{p}})=0\right\}$ равна нулю, поэтому мера множества Ω также равна нулю.

Зафиксируем $\bar{\mathbf{p}}\in D\setminus\Omega$. Тогда $u_i(\bar{\mathbf{p}})\neq 0$ ни для какой функции рассматриваемого семейства. Это означает, что все элементы множества $\left\{P_{\gamma,f}(\bar{\mathbf{p}}),\ f-\text{не эквивалентные функции из } F_{r,k}\right\}$ различны. Поэтому значению $P_{\gamma,f}(\bar{\mathbf{p}})$ соответствует единственный класс эквивалентности функции f, указать который можно, например, перебрав все классы эквивалентности.

Последовательность $\{\sigma_j,\ j=0,1,...\}$ состояний автомата A в рассматриваемой схеме является простой однородной цепью Маркова с вектором начального распределения $\mathbf{q}^{(\mathbf{0})}$ и матрицей переходных вероятностей $\mathbf{M}$. Из цепи $\{\sigma_j,\ j=0,1,...\}$ образуем новую марковскую цепь $\left\{\sigma_j^{(l)},\ j=0,1,...\right\}$, состояния которой представляют собой всевозможные последовательности длины l состояний цепи $\{\sigma_j,\ j=0,1,...\}$. Более точно множество состояний $Q^{(l)}$ новой цепи определим следующим образом:

$$Q^{(l)}=\left\{\left(q^{(1)},q^{(2)},...,q^{(l)}\right)\,\middle|\,m_{q^{(1)}q^{(2)}}m_{q^{(2)}q^{(3)}}...m_{q^{(l-1)}q^{(l)}}>0\right\}.$$

Обозначим $\left|Q^{(l)}\right|=r^{(l)}$ (очевидно, $r^{(l)}\le r^l$), и зафиксируем на $Q^{(l)}$ лексикографический порядок. В [12] показано, что из эргодичности цепи $\{\sigma_j,\ j=0,1,...\}$ следует эргодичность цепи $\left\{\sigma_j^{(l)},\ j=0,1,...\right\}$ и существование для последней предельного распределения $\bar{\boldsymbol{\pi}}^{(l)}=\left(\pi^{(l)}_{\bar{\mathbf{q}}},\bar{\mathbf{q}}\in Q^{(l)}\right)$. Если $\bar{\mathbf{q}}=\left(q^{(1)},q^{(2)},...,q^{(l)}\right)\in Q^{(l)}$, то

$$\boldsymbol{\pi}^{(l)}_{\bar{\mathbf{q}}}=\pi_{q^{(1)}}m_{q^{(1)}q^{(2)}}...m_{q^{(l-1)}q^{(l)}}.$$

С целью подчеркнуть зависимость вектора предельного распределения от $\bar{\mathbf{p}}=(p_1,p_2,...,p_{m-1})$ будем его обозначать $\bar{\boldsymbol{\pi}}^{(l)}(\bar{\mathbf{p}})$.

Определим функцию $\Psi^f_\gamma:Q^{(l)}\to\{0,1\}$, положив

$$\Psi^f_\gamma\left(q^{(1)},q^{(2)},...,q^{(l)}\right)=\begin{cases}1,\ \text{если } f\left(q^{(i)}\right)=y^{(i)},\ i=1,2,...,l,\\ 0\ \text{в противном случае.}\end{cases}$$

Вектор-столбец $\left(\Psi^f_\gamma(\bar{\mathbf{q}}),\bar{\mathbf{q}}\in Q^{(l)}\right)^T$ обозначим $\boldsymbol{\Psi}^f_\gamma$. Во введенных обозначениях вероятностная функция автомата представляется в виде скалярного произведения векторов размера $r^{(l)}$:

$$P_{\gamma,f}(\bar{\mathbf{p}})=\bar{\boldsymbol{\pi}}^{(l)}(\bar{\mathbf{p}})\boldsymbol{\Psi}^f_\gamma.$$

Рассмотрим линейное пространство $\left\langle \left\{ \pi^{(l)}_{\left(q^{(1)},q^{(2)},...,q^{(l)}\right)}\left(\bar{\mathbf{p}}\right), \left(q^{(1)},q^{(2)},...,q^{(l)}\right)\in Q^{(l)} \right\} \right\rangle_R$ над полем действительных чисел, порожденное элементами вектора предельного распределения. Это пространство состоит из действительных функций от $\bar{\mathbf{p}}=(p_1,p_2,...,p_{m-1})$ вида $\sum\limits_{\bar{\mathbf{q}}\in Q^{(l)}} c_{\bar{\mathbf{q}}}\pi^{(l)}_{\bar{\mathbf{q}}}\left(\bar{\mathbf{p}}\right)$; $c_{\bar{\mathbf{q}}}$ – произвольные действительные числа; $\bar{\mathbf{q}}\in Q^{(l)}$. Пусть t – размерность этого пространства. Очевидно, $t\le r^{(l)}$. Выберем в нем базис $\bar{\mathbf{d}}\left(\bar{\mathbf{p}}\right)=\left(d_1\left(\bar{\mathbf{p}}\right),d_2\left(\bar{\mathbf{p}}\right),...,d_t\left(\bar{\mathbf{p}}\right)\right)$. Через $\mathbf{C}$ обозначим действительную матрицу размера $t\times r^{(l)}$, для которой

$$\bar{\boldsymbol{\pi}}^{(l)}\left(\bar{\mathbf{p}}\right)=\bar{\mathbf{d}}\left(\bar{\mathbf{p}}\right)\mathbf{C}.$$

Выбирая в качестве базиса $\tilde{\mathbf{d}}$, где $\bar{\mathbf{d}}=\tilde{\mathbf{d}}\mathbf{H}$, $\mathbf{H}$ – действительная квадратная матрица порядка $r^{(l)}$, $\det\mathbf{H}\ne 0$, имеем

$$\bar{\boldsymbol{\pi}}^{(l)}\left(\bar{\mathbf{p}}\right)=\tilde{\mathbf{d}}\mathbf{H}\mathbf{C}.$$

Выбором подходящего базиса приведем матрицу $\mathbf{C}$ к ступенчатому виду (эрмитовой нормальной форме [13]), и с помощью перенумерации множества состояний получим матрицу следующего вида:

$$\mathbf{HC}=\begin{pmatrix} b_1^1 & b_2^1 & \cdots & b_{s_1}^1 & * & * & \cdots & * & \vdots & * & * & \cdots & * \\ 0 & 0 & \cdots & 0 & b_1^2 & b_2^2 & \cdots & b_{s_2}^2 & \vdots & * & * & \cdots & * \\ & & \cdots & & & & \cdots & & \ddots & & & \cdots & \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & \vdots & b_1^t & b_2^t & \cdots & b_{s_t}^t \end{pmatrix}=\mathbf{B}.$$

Такое переупорядочивание множества $Q^{(l)}$ приводит к разбиению его на t блоков:

$$Q^{(l)}=\bigcup_{i=1}^{t} Q_i,\ i=1,2,...,t,\ Q_i\cap Q_j=0, i\ne j.$$

Состояние $\bar{\mathbf{q}}\in Q^{(l)}$ принадлежит i-му блоку разбиения Q_i, $i=1,2,...,t$, тогда и только тогда, когда функция $\pi^{(l)}_{\bar{\mathbf{q}}}\left(\bar{\mathbf{p}}\right)$ линейно выражается через первые i базисных функций, т.е. через первые i координат вектора $\tilde{\mathbf{d}}\left(\bar{\mathbf{p}}\right)$,

$$\pi^{(l)}_{\bar{\mathbf{q}}}\left(\bar{\mathbf{p}}\right)=\sum_{j\le i} a_j\tilde{d}_j\left(\bar{\mathbf{p}}\right), a_i\ne 0 \qquad (1)$$

и не представляется линейной комбинацией первых $i-1$ базисных функций.

Отметим, что размерность t пространства $\left\langle \left\{ \pi^{(l)}_{\bar{\mathbf{q}}}\left(\bar{\mathbf{p}}\right), \bar{\mathbf{q}}\in Q^{(l)} \right\} \right\rangle_R$ является константой, зависящей только от функции переходов автомата. Выбор базиса и связанные с ним ступенчатый вид матрицы $\mathbf{B}$ и представление (1) не определены однозначно.

Предполагаем, что для рассматриваемого класса автоматов ступенчатая матрица $\mathbf{B}$ выбрана произвольным образом и зафиксирована.

Утверждение 2. Функции f и g из $F_{r,k}$ статистически эквивалентны относительно слова γ тогда и только тогда, когда

$$\mathbf{B}\boldsymbol{\Psi}^f_\gamma=\mathbf{B}\boldsymbol{\Psi}^g_\gamma. \qquad (2)$$

Доказательство. Тождество $P_{\gamma,f}\left(\bar{\mathbf{p}}\right)=P_{\gamma,g}\left(\bar{\mathbf{p}}\right)$ имеет место тогда и только тогда, когда $\bar{\boldsymbol{\pi}}^{(l)}\left(\bar{\mathbf{p}}\right)\boldsymbol{\Psi}^f_\gamma=\bar{\boldsymbol{\pi}}^{(l)}\left(\bar{\mathbf{p}}\right)\boldsymbol{\Psi}^g_\gamma$. Последнее равенство переписывается в виде $\tilde{\mathbf{d}}\mathbf{B}\boldsymbol{\Psi}^f_\gamma=\tilde{\mathbf{d}}\mathbf{B}\boldsymbol{\Psi}^g_\gamma$, что в силу линейной независимости базисных функций равносильно (2).

Доказанное утверждение позволяет отождествить класс эквивалентности функции f с вектором $\mathbf{B}\boldsymbol{\Psi}_\gamma^f$ и получить следующие результаты.

Утверждение 3. Число различных классов статистической эквивалентности относительно слова γ равно

$$\left|F_k \big/ \approx\right| = \left|\left\{\mathbf{B}\boldsymbol{\Psi}_\gamma^f \,\middle|\, f \in F_{r,k}\right\}\right|.$$

Мощность $\left|[f_0]_\approx\right|$ класса эквивалентности, содержащего функцию f_0, равна числу решений уравнения

$$\mathbf{B}\left(\boldsymbol{\Psi}_\gamma^{f_0} - \boldsymbol{\Psi}_\gamma^f\right) = 0,$$

где неизвестной является функция $f \in F_{r,k}$.

Согласно утверждению 1, для $\bar{\mathbf{p}} \in D \setminus \Omega$ значению $P_{\gamma,f}\left(\bar{\mathbf{p}}\right)$ соответствует единственный класс эквивалентности функции f. Теперь можно уточнить этот результат.

Утверждение 4. Для $\bar{\mathbf{p}} \in D \setminus \Omega$ уравнение

$$\tilde{\mathbf{d}}\boldsymbol{\mu} = P_{\gamma,f}\left(\bar{\mathbf{p}}\right) \tag{3}$$

при ограничениях на неизвестные $\boldsymbol{\mu} = (\mu_1, \mu_2, \ldots \mu_t) \in \left\{\mathbf{B}\boldsymbol{\Psi}_\gamma^f, f \in F_{r,k}\right\}$ имеет единственное решение $\boldsymbol{\mu}_0 = \mathbf{B}\boldsymbol{\Psi}_\gamma^f$, соответствующее классу эквивалентности функции f.

В случае когда $\bar{\mathbf{p}} \in \Omega$, уравнение (3) имеет несколько решений, среди которых содержится вектор, соответствующий классу эквивалентности истинной функции выходов.

Границы для числа классов эквивалентности

Структурность матрицы $\mathbf{B}$ позволяет получить границы для числа классов эквивалентности. Прежде всего заметим, что имеет место включение

$$\left\{\mathbf{B}\boldsymbol{\Psi}_\gamma^f, f \in F_k\right\} \subseteq V^{r^{(l)}}, \text{ где } V = \{0,1\},$$

которое для $l = 1$ превращается в равенство множеств. Отсюда вытекает неравенство $\left|F_{r,k} \big/ \approx\right| \le \left|\left\{\mathbf{B}\bar{\boldsymbol{\varepsilon}} \,\middle|\, \bar{\boldsymbol{\varepsilon}} \in V^{r^{(l)}}\right\}\right|$ с равенством при $l = 1$.

Пусть $\mathbf{B}_i$ – подматрица размера $i \times s_i$ матрицы $\mathbf{B}$ с множеством строк $\{1,2,\ldots,i\}$ и столбцов, соответствующих множеству Q_i, $i = 1,2,\ldots,t$. Нижнюю (i-ю) строку матрицы $\mathbf{B}_i$ обозначим $\bar{\mathbf{b}}_i$. Очевидно, все ее элементы отличны от нуля.

Обозначим: $m_i = \left|\left\{\mathbf{B}_i\bar{\boldsymbol{\varepsilon}}^{(i)}, \bar{\boldsymbol{\varepsilon}}^{(i)} \in V^{s_i}\right\}\right|$ – число образов точек s_i-мерного единичного куба при линейном отображении $\mathbf{B}_i : V^{s_i} \to V^i$, $i = 1,2,\ldots,t$; $k_i = \left|\left\{\bar{\mathbf{b}}_i\bar{\boldsymbol{\varepsilon}}^{(i)}, \bar{\boldsymbol{\varepsilon}}^{(i)} \in V^{s_i}\right\}\right|$ – число различных сумм, составленных из элементов нижней строки матрицы B_i, $i = 1,2,\ldots,t$.

Очевидны соотношения:

$$s_i \le k_i \le m_i \le 2^{s_i},\ i = 1,2,\ldots,t.$$

Утверждение 5. Для числа классов статистической эквивалентности относительно слова γ справедливы неравенства:

$$\left|F_{r,k} \big/ \approx\right| \le m_1 m_2 \ldots m_t, \tag{4}$$

$$\text{при } l = 1 \quad \left|F_{r,k} \big/ \approx\right| \ge k_1 k_2 \ldots k_t. \tag{5}$$

Доказательство. Для произвольного вектора $\bar{\boldsymbol{\varepsilon}} \in V^{r^{(l)}}$ имеем:

$$\mathbf{B}\bar{\boldsymbol{\varepsilon}} = \begin{pmatrix} \mathbf{B}^{(1)}\bar{\boldsymbol{\varepsilon}}^{(1)} \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} \mathbf{B}^{(2)}\bar{\boldsymbol{\varepsilon}}^{(2)} \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \ldots + \mathbf{B}^{(t)}\bar{\boldsymbol{\varepsilon}}^{(t)} = \boldsymbol{\beta}_1 + \boldsymbol{\beta}_2 + \ldots + \boldsymbol{\beta}_t,$$

где $\bar{\boldsymbol{\varepsilon}}^{(i)}$ – подвектор вектора $\bar{\boldsymbol{\varepsilon}}$, соответствующий множеству Q_i. Так как вектор $\boldsymbol{\beta}_i$ может принимать лишь m_i значений, то $\mathbf{B}\bar{\boldsymbol{\varepsilon}} = \sum \boldsymbol{\beta}_i$ может принимать не более $m_1 m_2 \ldots m_t$ различных значений. Неравенство (4) доказано.

Неравенство (5) равносильно неравенству

$$\left| \left\{ \mathbf{B}\bar{\boldsymbol{\varepsilon}} \middle| \bar{\boldsymbol{\varepsilon}} \in V^r \right\} \right| \geq k_1 k_2 \ldots k_t. \qquad (6)$$

Для доказательства последнего применим индукцию по t.

1^0. $t = 1$. Матрица $\mathbf{B}$ является матрицей-строкой размера $1 \times s_1$, и (6) очевидно.

2^0. Пусть $\mathbf{B}$ имеет вид

$$\mathbf{B} = \begin{pmatrix} \mathbf{B}^{(t-1)} & & D \\ 0 & \cdots \; 0 & b_1^{(t)} b_2^{(t)} \ldots b_{s_t}^{(t)} \end{pmatrix}.$$

Обозначим через Q' множество $\left(r^{(l)} - s_t\right)$-мерных двоичных вектор-столбцов $\bar{\mathbf{q}}'$, для которых значения $\mathbf{B}^{(t-1)}\bar{\mathbf{q}}'$ различны, а через Q'' – множество s_t-мерных двоичных вектор-столбцов $\bar{\mathbf{q}}''$, для которых различны значения $(b_1^{(t)} b_2^{(t)} \ldots b_{s_t}^{(t)})\bar{\mathbf{q}}''$. По предположению индукции, $|Q''| \geq k_t$. Положим $Q''' = Q' \times Q''$. Для $\bar{\mathbf{q}}''' = \left(\bar{\mathbf{q}}', \bar{\mathbf{q}}''\right) \in Q'''$ имеем

$$\mathbf{B}\bar{\mathbf{q}}''' = \mathbf{B}\begin{pmatrix} \bar{\mathbf{q}}' \\ \bar{\mathbf{q}}'' \end{pmatrix} = \begin{pmatrix} \mathbf{B}^{(t-1)}\bar{\mathbf{q}}' + \mathbf{D}\bar{\mathbf{q}}'' \\ (b_1^t b_2^t \ldots b_{s_t}^t)\bar{\mathbf{q}}'' \end{pmatrix}.$$

Для фиксированного $\bar{\mathbf{q}}'_0 \in Q'$ и произвольного $\bar{\mathbf{q}}''$, пробегающего множество Q'', t-я координата вектора $\mathbf{B}\bar{\mathbf{q}}'''$ принимает ровно k_t значений. Зафиксируем одно из этих значений, соответствующее какому-то вектору $\bar{\mathbf{q}}''_0 \in Q''$, и заставим $\bar{\mathbf{q}}'$ пробегать все множество Q'. Очевидно, число различных значений вектора $\mathbf{B}^{(t-1)}\bar{\mathbf{q}}' + \mathbf{D}\bar{\mathbf{q}}''$ равно $|Q'| \geq k_1 k_2 \ldots k_{t-1}$. Таким образом, для каждого из k_t значений t-й координаты вектора $\mathbf{B}\bar{\mathbf{q}}'''$ нами указано по меньшей мере $k_1 k_2 \ldots k_{t-1}$ различных значений первых $t-1$ координат этого вектора. Неравенство (6), а вместе с ним и утверждение доказаны.

Определение класса эквивалентности неизвестной функции выходов по статистике выборочного среднего

Пусть в рассматриваемой схеме входная последовательность $x^{(1)}, x^{(2)}, \ldots, x^{(N)}$ перерабатывается автоматом A в выходную последовательность $y^{(1)}, y^{(2)}, \ldots, y^{(N)}$. Через $g^{(k)}$ обозначим функцию, которая вычисляется по выходной последовательности длины $k \geq 1$ и слову γ следующим образом:

$$g^{(k)} = \begin{cases} 1, \text{ если последние } l \text{ символов выходной} \\ \text{последовательности длины } k \text{ составляют слово } \gamma, \\ 0 \text{ в противном случае.} \end{cases}.$$

Положим

$$Y_N = \frac{1}{N - l + 1} \sum_{k=l}^{N} g^{(k)}.$$

Оценим объем материала N, достаточный для определения класса статистической эквивалентности функции выходов f по статистике Y_N с заданным уровнем надежности δ, $0<\delta<1$. Воспользуемся нормальной аппроксимацей.

Для последовательности $g^{(1)},g^{(2)},...,g^{(N)}$ при $N\to\infty$ справедлива ЦПТ [10], согласно которой случайная величина

$$\frac{\sum\limits_{k=l}^{N} g^{(k)} - (N-l+1)P_f\left(\overline{p}\right)}{\sqrt{d_f\,(N-l+1)}}$$

сходится по распределению к стандартному нормальному закону. Величина предельной дисперсии d_f вычисляется [12] следующим образом:

$$d_f = \sum_{i,j=1}^{r} \eta_i(\gamma) c_{ij} \eta_j(\gamma) + \sum_{j=1}^{r} \pi_j \eta_j(\gamma)\left(1-\eta_j(\gamma)\right), \tag{7}$$

где $\eta_i(\gamma)$ – компоненты вектора $\boldsymbol{\eta}(\gamma)$, равные условной вероятности появления на выходе автомата последовательности γ, если он находился в состоянии q_i; c_{ij} – элементы матрицы $\mathbf{C}$ предельных ковариаций цепи $\{\sigma_j, j=0,1,...\}$.

Элементы матрицы предельных ковариаций вычисляются по формуле

$$c_{ij} = \pi_i z_{ij} + \pi_j z_{ji} - \pi_i \delta_{ij} - \pi_i \pi_j, \tag{8}$$

где δ_{ij} – символ Кронекера; z_{ij} – элементы фундаментальной матрицы

$$\mathbf{Z} = \left(\mathbf{E} - \left(\mathbf{M} - \boldsymbol{\eta}\overline{\boldsymbol{\pi}}\right)\right)^{-1}$$

эргодической цепи $\{\sigma_j, j=0,1,...\}$.

Задача определения класса статистической эквивалентности функции выходов по статистике Y_N для $\overline{p}\in D\setminus\Omega$ является задачей различения $\left|F_{r,k}\middle/\approx\right| = v$ гипотез о принадлежности с.в. Y_N к тому или иному распределению из v нормальных совокупностей:

$$\left\{\mathrm{N}\left(P_{g_1}, \frac{d_g}{\sqrt{N-l+1}}\right) \middle| g\in F_{r,k}, g\approx g_1\right\},$$

$$\left\{\mathrm{N}\left(P_{g_2}, \frac{d_g}{\sqrt{N-l+1}}\right) \middle| g\in F_{r,k}, g\approx g_2\right\},$$

$$\left\{N\left(P_{g_v}, \frac{d_g}{\sqrt{N-l+1}}\right) \middle| g\in F_{r,k}, g\approx g_v\right\}.$$

Здесь множество $\{g_1,g_2,...,g_v\}$ образовано попарно неэквивалентными функциями, по одному представителю от каждого класса эквивалентности.

Построим критерий различения перечисленных гипотез с помощью метода доверительных интервалов. Для этого нам потребуется равномерная по всем функциям $f\in F_{r,k}$ верхняя граница для предельных дисперсий $d_{\max}\ge d_f$. Получим ее.

Из (7) следует оценка

$$d_f = \sum_{i,j=1}^{r} \eta_i(\gamma) c_{ij} \eta_j(\gamma) + \sum_{j=1}^{r} \pi_j \eta_j(\gamma)\left(1-\eta_j(\gamma)\right) \le \sum_{i,j=1}^{r} \eta_i(\gamma) c_{ij} \eta_j(\gamma) + 1/4 \le r\lambda_{\max}(\mathbf{C}),$$

где $\lambda_{\max}(\mathbf{C})$ – наибольшее собственное число матрицы $\mathbf{C}$. (Матрица $\mathbf{C}$ симметрична и положительно определена).

Получим границу для предельной дисперсии в терминах собственных чисел матрицы $\mathbf{M}$, которые обозначим $\lambda_1 = 1, \lambda_2, ..., \lambda_r$. Нетрудно убедиться, что собственные числа матрицы $\mathbf{E} - \left(\mathbf{M} - \boldsymbol{\eta}\bar{\boldsymbol{\pi}}\right)$ имеют вид $\left(1, 1-\lambda_2, ..., 1-\lambda_r\right)$, а собственные числа матрицы $\mathbf{Z}$ есть $\left(1, \frac{1}{1-\lambda_2}, ..., \frac{1}{1-\lambda_r}\right)$.

В силу положительной определенности матрицы $\mathbf{C}$ справедливо неравенство $\lambda_{\max}(\mathbf{C}) \le tr(\mathbf{C})$, где $tr(\mathbf{C})$ – след матрицы $\mathbf{C}$.

С учетом (8) имеем

$$tr(\mathbf{C}) \le 2tr(\mathbf{Z}) - 1 = 1 + 2\sum_{t=2}^{r} \frac{1}{1-\lambda_t}.$$

Необходимая оценка получена:

$$d_{\max} = r\left(1 + 2\sum_{t=2}^{r} \frac{1}{1-\lambda_t}\right) + \frac{1}{4}.$$

Для заданного p обозначим $\varepsilon_0 = \min_{f,g} \left|P_f(\bar{\mathbf{p}}) - P_g(\bar{\mathbf{p}})\right| = \min_{\substack{\boldsymbol{\mu}_1, \boldsymbol{\mu}_2 \in F_{r,k} / \approx \\ \boldsymbol{\mu}_1 \ne \boldsymbol{\mu}_2}} \left|\bar{\mathbf{d}}(\bar{\mathbf{p}})(\boldsymbol{\mu}_1 - \boldsymbol{\mu}_2)\right|$, где первый минимум берется по всем парам неэквивалентных функций f и g. По построению отношения эквивалентности имеем $\varepsilon_0 > 0$.

Зададимся уровнем надежности δ, $0 < \delta < 1$. Учитывая, что

$$P\left\{\left|Y_N - P_f(\bar{p})\right| < \frac{\varepsilon_0}{2}\right\} \approx 2\Phi\left(\frac{\varepsilon_0}{\sqrt{d_f(N-l+1)}}\right),$$

где Φ – функция распределения стандартного нормального закона, найдем N_0 как наименьшее целое, удовлетворяющее неравенству

$$\frac{\delta}{2} > \Phi\left(\frac{\varepsilon_0}{\sqrt{d_{\max}(N-l+1)}}\right). \qquad (9)$$

Применение метода доверительных интервалов приводит к следующему утверждению.

Утверждение 6. Пусть для $N \ge N_0, \bar{\mathbf{p}} \notin \Omega$ вектор $\boldsymbol{\mu}_0 \in \left\{\mathbf{B}\bar{\boldsymbol{\varepsilon}}, \bar{\boldsymbol{\varepsilon}} \in V^{r^{(l)}}\right\}$ является решением задачи минимизации

$$\begin{cases} \left|Y_N - \bar{\mathbf{d}}(\bar{\mathbf{p}})\boldsymbol{\mu}\right| \to \min \\ \text{при ограничении } \boldsymbol{\mu} \in \left\{\mathbf{B}\bar{\boldsymbol{\varepsilon}}, \bar{\boldsymbol{\varepsilon}} \in V^{r^{(l)}}\right\}. \end{cases}$$

Тогда с вероятностью, не меньшей δ, можно утверждать, что класс статистической эквивалентности истинной функции выходов f есть $\boldsymbol{\mu}_0$.

Сформулируем аналогичный результат для случая $\bar{\mathbf{p}} \in \Omega$. Пусть

$$\varepsilon_0 = \min_{P_f \ne P_g} \left|P_f(\bar{\mathbf{p}}) - P_g(\bar{\mathbf{p}})\right| = \min_{\substack{\boldsymbol{\mu}_1, \boldsymbol{\mu}_2 \in F_{r,k} / \approx \\ \bar{\mathbf{d}}(\mathbf{p})\boldsymbol{\mu}_1 \ne \bar{\mathbf{d}}(\mathbf{p})\boldsymbol{\mu}_2}} \left|\bar{\mathbf{d}}(\bar{\mathbf{p}})(\boldsymbol{\mu}_1 - \boldsymbol{\mu}_2)\right|.$$

Утверждение 7. Пусть N_0 определено соотношением (9). Для $N \ge N_0$ с вероятностью, не меньшей δ, соответствующий классу статистической эквивалентности истинной функции выходов f вектор $\boldsymbol{\mu}_0$ содержится среди решений неравенства

$$\left|Y_N - \bar{\mathbf{d}}(\bar{\mathbf{p}})\boldsymbol{\mu}\right| < \frac{\varepsilon}{2},$$

рассматриваемого при ограничении $\boldsymbol{\mu} \in \left\{\mathbf{B}\bar{\boldsymbol{\varepsilon}}, \bar{\boldsymbol{\varepsilon}} \in V^{r^{(l)}}\right\}$.

2. Задача определения булевой функции выходов проходного регистра сдвига с бернуллиевским входом.

Рассматривается задача определения неизвестной булевой функции выходов проходного регистра сдвига с бернуллиевским входом по значковой статистике выходной последовательности. Будем придерживаться общей схемы, изложенной ранее.

Пусть F_n – множество всех булевых функций от n аргументов, $n=1,2,...$. Для булевой функции $f(x_1,x_2,...,x_n)\in F_n$ через $A_f=\left(X=\{0,1\},V^n,Y=\{0,1\},h,f\right)$ обозначим автомат Мура, являющийся двоичным регистром сдвига с накопителем размера $n\geq 1$, множеством состояний V^n, функцией переходов h, определяемой по правилу $h\left((\alpha_1,...,\alpha_n),x\right)=(\alpha_2,...,\alpha_n,x)$, где $x,\alpha_i\in\{0,1\}$, $i=1,2,...,n$, функцией выходов $f(x_1,x_2,...,x_n)$.

Предположим, что на вход A_f поступает бернуллиевская последовательность независимых двоичных случайных величин $x^{(i)}$, $i=1,2,...$ с распределением $P\left\{x^{(i)}=1\right\}=p$, $P\left\{x^{(i)}=0\right\}=1-p$, $0<p<1$. Для удобства предположим, что на множестве начальных заполнений регистра задано вероятностное распределение $P(\varepsilon_1,\varepsilon_2,...,\varepsilon_n)=p^{\sum\varepsilon_i}(1-p)^{n-\sum\varepsilon_i}$. Очевидно, такое предположение не является ограничительным.

Вероятностная функция автомата A_f для знака «1» выходной последовательности является [8] полиномом $\Phi_f(p)=\sum_{j=0}^{n}s_j p^j(1-p)^{n-j}$, где $s_k=\left\|f(x_1,...,x_n)\Big/\|(x_1,...,x_n)\|=k\right\|, k=0,1,...,n$, – веса функции f на подуровнях булевого куба.

В обозначениях первого параграфа в исследуемом случае имеем: $l=1,\gamma=1,Q=V^n$, $|Q|=r=2^n$. Для $\mathbf{q}=(\varepsilon_1,\varepsilon_2,...,\varepsilon_n)$ если $\sum\varepsilon_j=i$, то $\pi_{\mathbf{q}}=p^i(1-p)^{n-i}$, $i=0,1,...,n$.

Очевидно, размерность пространства, порожденного функциями $\pi_{\mathbf{q}}$, равна $n+1$. Воспользовавшись линейной независимостью системы функций $\left\{p^{i-1}(1-p)^{n-i+1},i=1,2,...,n+1\right\}$ на отрезке [0, 1], положим

$$d_i(p)=p^{i-1}(1-p)^{n-i+1},i=1,2,...,n+1.$$

Разбиение множества Q состояний на классы Q_i соответствует разбиению V^n на классы векторов фиксированного веса. Упорядочим векторы V^n по возрастанию весов, а в группах векторов постоянного веса примем лексикографический порядок. Введенная в первом параграфе матрица $\mathbf{B}$ в данном случае имеет размер $(n+1)\times 2^n$. Она обладает «ступенчатой» структурой:

$$\mathbf{B}=\begin{pmatrix}1 & & & & & & & \\ & 1 & 1 & 1 & & \cdots & & \\ & & \cdots & & 1 & 1 & 1 & \\ & & & & & & & 1\end{pmatrix}.$$

В i-й строке матрицы $\mathbf{B}$ имеется ровно $\binom{n}{i-1}$ единиц (указаны только ненулевые элементы).

Булевы функции f и g от n аргументов назовем *статистически эквивалентными* (и примем для такого случая обозначение $f\approx g$), если вероятностные функции автоматов A_f и A_g совпадают как функции от p на отрезке $[0,1]$.

Утверждение 8. Статистическая эквивалентность булевых функций f и g равносильна равенству их весов на подуровнях одинакового веса:

$$\left\| f(x_1,...,x_n) \Big/ \|(x_1,...,x_n)\| = i \right\| = \left\| g(x_1,...,x_n) \Big/ \|(x_1,...,x_n)\| = i \right\|, \; i = 0,1,...,n \; .$$

Доказательство. Определенный выше вектор $\mathbf{\Psi}_{\gamma}^{f}$ в данном случае является вектором табличного задания функции f. Воспользовавшись полученным видом матрицы $\mathbf{B}$, нетрудно видеть, что доказываемые равенства являются покоординатной записью критерия утверждения 2.

Полученный результат позволяет отождествить фактор-множество $F_n \Big/ \approx$ с множеством $(n+1)$ – мерных векторов с целочисленными координатами

$$\left\{ (s_0, s_1, ..., s_n), s_i \in \left\{ 0,1,..., \binom{n}{i} \right\} \right\} .$$

Утверждение 9. Для $p \in [0,1] \setminus \Omega_n$, где Ω_n – конечное множество точек отрезка $[0,1]$, по значению $\Phi_f(p)$ можно указать класс эквивалентности функции f. Справедлива оценка

$$|\Omega_n| \le \frac{n}{2} \left(\left| F_n \Big/ \approx \right| \right) .$$

Доказательство. Рассмотрим семейство M_n не равных тождественно нулю полиномов от p вида $\sum_{j=0}^{n} c_j p^j (1-p)^{n-j}$, где c_j – целые числа, удовлетворяющие неравенствам

$$-\binom{n}{j} \le c_j \le \binom{n}{j}, \; j = 0,...,n.$$

Определим множество Ω_n как объединение множеств корней полиномов рассматриваемого семейства, которые принадлежат отрезку $[0,1]$. Степень каждого полинома не превосходит n. Поскольку в этом семействе содержатся все попарные разности вероятностных полиномов функций из F_n, приходим к оценке

$$|\Omega_n| \le n \left(\left| F_n \Big/ \approx \right| \right) .$$

Отбрасывая по одному из каждой пары различающихся только знаком полиномов, приходим к доказываемой формуле. Доказательство утверждения завершается теми же рассуждениями, что и при доказательстве утверждения 1.

Доказанный результат допускает наглядную геометрическую интерпретацию (рис. 1). В квадрате $[0,1] \times [0,1]$ изобразим графики вероятностных функций $\Phi_f(p)$ для всех неэквивалентных булевых функций из F_n. Тогда множество «особенных распределений» Ω_n есть множество абсцисс точек пересечения указанных графиков.

Следующее утверждение, по сути, является переформулировкой утверждения 4 для случая регистра сдвига.

Утверждение 10. Для $p \in [0,1] \setminus \Omega_n$ уравнение

$$\Phi_f(p) = \sum_{j=0}^{n} \mu_j p^j (1-p)^{n-j}$$

при ограничениях на неизвестные $0 \le \mu_j \le \binom{n}{j}, \; j = 0,...,n$ имеет единственное целочисленное решение $\left(\mu_0^{(0)}, \mu_1^{(0)}, ..., \mu_n^{(0)} \right)$, соответствующее классу эквивалентности функции f.

В случае когда $p \in \Omega_n$, данное уравнение имеет несколько решений, среди которых содержится вектор весов на подуровнях истинной функции выходов.

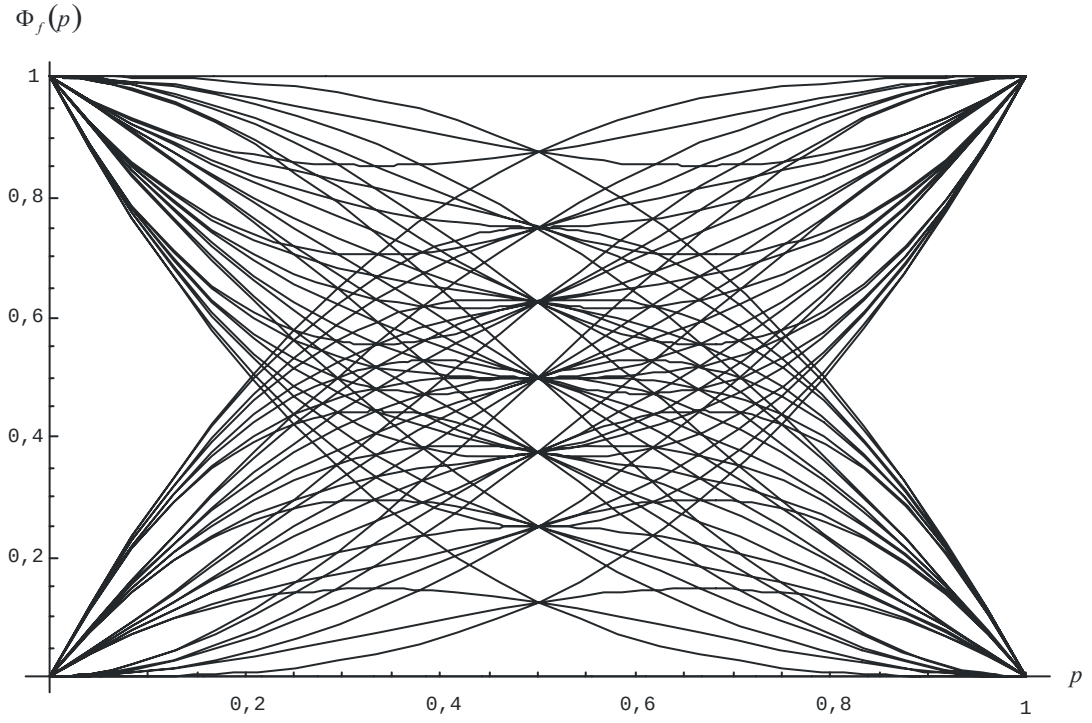

Рис. 1. Вероятностные функции $\Phi_f(p)$ для всех неэквивалентных булевых функций из F_3

Структура отношения статистической эквивалентности

Полученные в утверждении 5 верхняя и нижняя границы для числа классов эквивалентности в рассматриваемом случае оказываются равными, что в совокупности с результатом утверждения 8 позволяет получить следующее

Утверждение 11. Число классов эквивалентности равно

$$\left|F_n \big/ \approx\right| = \prod_{k=0}^{n} \left(\binom{n}{k} + 1 \right). \tag{10}$$

Число функций, эквивалентных f_0, равно

$$\left[\!\left[f_0 \right]\!\right] = \prod_{k=0}^{n} \binom{n}{k}_{s_k^{(0)}},$$

где $s_k^{(0)} = \left\| f_0(x_1,\ldots,x_n) \big/ \|(x_1,\ldots,x_n)\| = k \right\|, k = 0,1,\ldots,n$.

Конкретные значения чисел классов статистической эквивалентности для функций от малого количества переменных сведены в таблицу.

n	2	3	4	5
$\left\|F_n \big/ \approx\right\|$	12	144	11664	8622400
$\dfrac{\left\|F_n \big/ \approx\right\|}{2^{2^n}}$	0,75	0,56	0,18	0,002

Утверждение 12. При $n \to \infty$ справедливо соотношение

$$\left|F_n \big/ \approx\right| = \exp\left(\frac{n^2}{2} - n\ln n + O(n) \right).$$

Доказательство. Воспользовавшись формулой суммирования Эйлера–Маклорена для суммы $\sum_{i=0}^{n} i\ln i$, нетрудно получить, что $\sum_{i=0}^{n} i\ln i = \frac{n^2}{2}\ln n - \frac{n^2}{4} + n\ln n + O(\ln n)$. Записывая (10) в виде произведения факториалов и используя формулу Стирлинга, приходим к доказываемому соотношению.

Свойства множества Ω_n

Опишем некоторые свойства множества Ω_n «особенных распределений».

Теорема 2. При $n \geq 1$ справедливы следующие соотношения:

1) $\Omega_n \subset \Omega_{n+1}$.

2) $\left\{0,1,\frac{1}{2}\right\} \subset \Omega_n$.

3) $p \in \Omega_n$ тогда и только тогда, когда $(1-p) \in \Omega_n$.

4) Точка $p \in \Omega_n$ является рациональной тогда и только тогда, когда $p = \frac{s}{s+t}$ либо $p = \frac{t}{s+t}$, где s и t – целые числа, удовлетворяющие условиям

$$0 \leq s \leq \left(\left[\frac{n}{\left[\frac{n+1}{2}\right]}\right]\right), \quad 0 \leq t \leq \left(\left[\frac{n}{\left[\frac{n}{2}\right]}\right]\right).$$

5) В интервалах $\left(\frac{1}{2}-\varepsilon_n, \frac{1}{2}\right)$ и $\left(\frac{1}{2}, \frac{1}{2}+\varepsilon_n\right)$, где $\varepsilon_n = \frac{1}{2}4^{-n}$, нет точек множества Ω_n.

Доказательство. Умножая произвольный многочлен из M_n на p, получаем многочлен из M_{n+1}, откуда следует включение множеств корней и первый пункт теоремы.

Для доказательства второго пункта достаточно рассмотреть двоичные функции 0, x_1, и $\overline{x_1}$, принадлежащие F_1, после чего воспользоваться п. 1.

Третий пункт вытекает из инвариантности множества F_n относительно операции инвертирования всех переменных.

Докажем четвертый пункт теоремы. Пусть $z_0 \geq 0$, $0 \leq p_0 < 1$, $p_0 = \frac{z_0}{1+z_0}$. Точка z_0 является корнем полинома $\sum_{j=0}^{n} c_j z^j$ тогда и только тогда, когда p_0 является корнем полинома $\sum_{j=0}^{n} c_j p^j (1-p)^{n-j}$. Нетрудно показать, что множество неотрицательных рациональных корней полиномов $\sum_{j=0}^{n} c_j z^j$, где c_j – целые числа, не все равные нулю одновременно, такие, что

$$-\binom{n}{j} \leq c_j \leq \binom{n}{j}, \; j = 0,1,...,n,$$

имеет вид $\left\{\frac{s}{t}, \text{ или } \frac{t}{s} \,\middle|\, t,s - \text{целые}, \; 0 \leq s \leq \left(\left[\frac{n}{\left[\frac{n+1}{2}\right]}\right]\right), \; 0 \leq t \leq \left(\left[\frac{n}{\left[\frac{n}{2}\right]}\right]\right)\right\}$.

Учитывая, что $p_0 = \frac{z_0}{1+z_0}$, получаем, что все рациональные корни многочленов из M_n на отрезке $[0,1]$, т.е. все рациональные точки Ω_n образуют множество $\{\frac{s}{s+t}$ либо $\frac{t}{s+t}$, где s и t – целые числа, удовлетворяющие условиям $0 \leq s \leq \left(\left[\frac{n}{\left[\frac{n+1}{2}\right]}\right]\right)$, $0 \leq t \leq \left(\left[\frac{n}{\left[\frac{n}{2}\right]}\right]\right)\}$.

Для доказательства п. 5 оценим наименьший по абсолютной величине корень многочлена $G\left(\frac{1}{2}-\delta\right), G(\delta)\in \mathrm{M}_n$.

Пусть $p=\frac{1}{2}-\delta$. Имеем:

$$\sum_{j=0}^{n} c_j p^j (1-p)^{n-j} = \sum_{j=0}^{n} c_j \left(\frac{1}{2}-\delta\right)^j \left(\frac{1}{2}+\delta\right)^{n-j} = 2^{-n}\sum_{j=0}^{n} c_j (1-2\delta)^j (1+2\delta)^{n-j} =$$

$$= 2^{-n}\sum_{j=0}^{n} c_{n-j}\sum_{k=0}^{j}\binom{j}{k}(2\delta)^k \sum_{s=0}^{n-j}(-1)^s\binom{n-j}{s}(2\delta)^s = 2^{-n}\sum_{l=0}^{n}(2\delta)^l \sum_{j=0}^{n} c_{n-j}\sum_{s=l-j}^{n-j}(-1)^s\binom{n-j}{s}\binom{j}{l-s} = 2^{-n}\sum_{l=0}^{n}(2\delta)^l t_l,$$

где $t_l = \sum_{j=0}^{n} c_{n-j}\sum_{s=l-j}^{n-j}(-1)^s\binom{n-j}{s}\binom{j}{l-s}$.

Воспользовавшись неравенством

$$-\binom{n}{j}\le c_j \le \binom{n}{j},$$

нетрудно показать, что

$$|t_l|\le 2^n\binom{n}{l}\le 2^n\binom{n}{\left[\frac{n}{2}\right]} = T.$$

Рассмотрим полином $T(x)=\sum_{i=0}^{n} t_i x^i$ на интервале $x\in(0,1)$. Пусть сперва $t_0\neq 0$. Без ограничения общности можно считать $t_0>0$. Тогда

$$|T(x)|\ge t_0 - \left|\sum_{i=1}^{n} t_i x^i\right| \ge t_0 - \left|\sum_{i=1}^{n} T x^i\right| = t_0 - xT\frac{1-x^n}{1-x}\ge t_0 - \frac{xT}{1-x}.$$

Следовательно, при $x<\tau_0=\frac{t_0}{T+t_0}$ имеет место $T(x)>0$.

Пусть теперь $t_0=t_1=...=t_{k-1}=0$, $t_k\neq 0, k\le n$. Вновь можно считать $t_k>0$. Тогда

$$|T(x)|\ge x^k\left(t_k - \left|\sum_{i=k+1}^{n} t_i x^{i-k}\right|\right)\ge x^k\left(t_k - \left|\sum_{i=k+1}^{n} T x^{i-k}\right|\right) = t_k - xT\frac{1-x^{n-k}}{1-x}\ge t_k - \frac{xT}{1-x}.$$

Следовательно, при $x<\tau_k=\frac{t_k}{T+t_k}$ имеет место $T(x)>0$.

Итак, многочлен $T(x)=\sum_{i=0}^{n} t_i x^i$ не имеет корней в интервале $x\in(0,\min\tau_k)$. Воспользовавшись тем, что коэффициенты t_i – целые числа, получаем, что наименьший по абсолютной величине корень δ_0 многочлена $G\left(\frac{1}{2}-\delta\right), G(\delta)\in \mathrm{M}_n$ удовлетворяет неравенству

$$\delta_0\ge\frac{1}{2}4^{-n}.$$

Теорема доказана.

Определение класса статистической эквивалентности неизвестной функции выходов по значковой статистике

Пусть в рассматриваемой схеме входная последовательность $\left(x^{(1)},x^{(2)},...,x^{(N)}\right)$ перерабатывается автоматом A_f в выходную последовательность $\left(y^{(1)},y^{(2)},...,y^{(N)}\right)$, где $y^{(i)}=f\left(x^{(i)},...,x^{(i+n-1)}\right)$. Обозначим $Y_N=\frac{1}{N}\sum_{k=l}^{N} y^{(k)}$. Оценим объем материала N, достаточный для

определения класса эквивалентности функции выходов f по статистике Y_N с заданным уровнем надежности $\delta, 0<\delta<1$. Будем использовать критерий, построенный в первом параграфе. В данном случае можно получить более простую верхнюю границу для предельных дисперсий d_f, чем в общем случае. Воспользовавшись тем, что для n-зависимых двоичных с.в. $y^{(i)}$, $i=1,2,...$, справедлива оценка $D\left(\sum_{i=1}^{n} y^{(i)}\right)\le\frac{n+1}{2}N$, получаем, что $d_f\le\frac{n+1}{2}$, $f\in F_n$.

Для заданного $p\notin\Omega_n$ обозначим $\varepsilon_0=\min\left|P_f(p)-P_g(p)\right|=\min\limits_{\boldsymbol{\mu}\neq\boldsymbol{\mu}'}\left|\mathbf{d}(p)(\boldsymbol{\mu}-\boldsymbol{\mu}')\right|$, где первый минимум берется по всем парам неэквивалентных булевых функций f и g.

По построению отношения эквивалентности имеем $\varepsilon_0>0$. Зададимся уровнем надежности δ, $0<\delta<1$. Учитывая, что при больших N (мы вновь пользуемся нормальной аппроксимацией)

$$P\left\{\left|Y_N-P_f(p)\right|>\frac{\varepsilon_0}{2}\right\}\approx 2\Phi\left(\frac{\varepsilon_0}{\sqrt{d_f N}}\right),$$

где Φ – функция распределения стандартного нормального закона, найдем N_0 как наименьшее целое N, удовлетворяющее неравенству

$$\frac{\delta}{2}>\Phi\left(\frac{\varepsilon_0}{\sqrt{N(n+1)/2}}\right). \tag{11}$$

Приходим к следующему утверждению.

Утверждение 13. Пусть N_0 определено соотношением (11). Для $N\ge N_0$, $p\notin\Omega_n$, через $\left(\mu_0^{(0)},\mu_1^{(0)},...,\mu_n^{(0)}\right)$ обозначим решение целочисленной задачи минимизации

$$\begin{cases}\left|Y_N-\sum\limits_{j=0}^{n}\mu_j p^j(1-p)^{n-j}\right|\to\min\\ \text{при ограничении } 0\le\mu_j\le\binom{n}{j},\ \mu_j-\text{целые}.\end{cases}$$

Тогда с вероятностью, не меньшей δ, можно утверждать, что класс статистической эквивалентности истинной функции выходов f соответствует вектору $\left(\mu_0^{(0)},\mu_1^{(0)},...,\mu_n^{(0)}\right)$.

Если параметр p лежит в пределах, указанных в п. 5 теоремы 2, последний результат можно уточнить. Для таких p неравенство (11) можно переписать в виде

$$\min\left\{\left|\sum_{i=1}^{n}\mu_i p^i(1-p)^{n-i}-\sum_{i=1}^{n}\mu_i' p^i(1-p)^{n-i}\right|\right\}\ge|1-2p|^n\left(1-\frac{|1-2p|T}{1-|1-2p|}\right)\ge|1-2p|^n\left(1-\frac{|1-2p|4^n}{1-|1-2p|}\right),$$

где минимум в левой части берется по всем различным целочисленным векторам $\left(\mu_0,\mu_1,...,\mu_n\right)$ и $\left(\mu_0',\mu_1',...,\mu_n'\right)$ с условием $0\le\mu_j,\mu_j'\le\binom{n}{j}$.

Следовательно, в данном случае N_0 можно определить как наименьшее целое, удовлетворяющее неравенству

$$\frac{\delta}{2}>\Phi\left(\frac{|1-2p|^n\left(1-\frac{|1-2p|4^n}{1-|1-2p|}\right)}{\sqrt{N_0(n+1)/2}}\right). \tag{12}$$

Утверждение 14. Пусть $\left|\frac{1}{2}-p\right|<\frac{1}{2}4^{-n}$, N_0 определяется соотношением (12). Для $N\ge N_0$, через $\left(\mu_0^{(0)},\mu_1^{(0)},...,\mu_n^{(0)}\right)$ обозначим решение целочисленной задачи минимизации

$$\begin{cases} \left|Y_N-\sum\limits_{i=0}^{n}\mu_j p^j(1-p)^{n-j}\right|\to\min \\ \text{при ограничении } 0\le\mu_j\le\binom{n}{j},\ \mu_j-\text{целые}. \end{cases}$$

Тогда с вероятностью, не меньшей δ, можно утверждать, что класс статистической эквивалентности истинной функции выходов f соответствует вектору $\left(\mu_0^{(0)},\mu_1^{(0)},...,\mu_n^{(0)}\right)$.

Сформулируем результат, аналогичный утверждению 13 для случая $p\in\Omega_n$. Пусть $\varepsilon_0=\min\left|P_f(p)-P_g(p)\right|=\min_{\mathbf{d}(p)\boldsymbol{\mu}\ne\mathbf{d}(p)\boldsymbol{\mu}'}\left|\mathbf{d}(p)(\boldsymbol{\mu}-\boldsymbol{\mu}')\right|$, где первый минимум берется по всем парам неэквивалентных булевых функций f и g.

Утверждение 15. Пусть N_0 определено соотношением (11). Для $N\ge N_0$, $p\notin\Omega_n$, с вероятностью, не меньшей δ, соответствующий классу статистической эквивалентности истинной функции выходов f вектор $\left(\mu_0^{(0)},\mu_1^{(0)},...,\mu_n^{(0)}\right)$ содержится среди целочисленных решений неравенства

$$\left|Y_N-\sum_{j=0}^{n}\mu_j p^j(1-p)^{n-j}\right|<\frac{\varepsilon}{2},$$

рассматриваемого при ограничении $0\le\mu_j\le\binom{n}{j}$, μ_j-целые.

Таким образом, в случае, когда в качестве автомата выступает двоичный регистр сдвига и рассматриваются значковые характеристики выходной последовательности, задача сводится к задаче целочисленной минимизации модуля линейной формы при линейных ограничениях, размерность которой равна размеру регистра плюс единица, т.е. логарифмически зависит от числа состояний.

Литература

1. Барашко А.С. О ранге и статистическом отображении сильносвязного автомата // Кибернетика. – 1987. – № 4. – С. 56–60.

2. Kingman J.F.C. Some algebraic results and problems in the theory of stochastic processes with a discrete parameter // Stochastic Anal. (ed. by D.G. Kedell and E.F. Harding). – 1973. – P. 315–330.

3. Кудрявцев В.Б. Введение в теорию автоматов / В.Б. Кудрявцев, С.В. Алешин, А.С. Подколзин. – М.: Наука, 1985. – 320 с.

4. Рябинин А.В. Стохастические функции конечных автоматов // Алгебра, логика и теория чисел: 7 темат. конф. мех.-мат. фак. МГУ. (фев.–март 1985). – М., 1986. – С. 77–80.

5. Голембиовский Д.Ю. Диагностика цифровых устройств. Микропрограммное и вероятностное тестирование: конспект лекций / Д.Ю. Голембиовский. – Саратов: СПИ, 1993. – 28 с.

6. Hadjicostis Christoforos N. Probabilistic detection of FSM single state-transition faults based on state occupancy measurements // IEEE Trans. Autom. Contr. – 2005. – Vol. 50, № 12. – P. 2078–2083.

7. Мельников С.Ю. Об использовании спектров графов автоматов в задаче определения функции выходов по вероятностям биграмм в выходной последовательности // Вестник Моск. гос. ун-та леса. – 2007. – № 2(51). – С.153–158.

8. Севастьянов Б.А. Условное распределение выхода автоматов без памяти при заданных характеристиках входа // Дискретн. матем. – 1994. – Т. 6, вып. 1. – С. 34–39.

9. Хохлов В.И. Точные формулы для вторых моментов условных преобладаний по Севастьянову // Обозрение прикладной и промышленной математики. – 2003. – Т. 10, вып. 3. – С. 579–582.

10. Сарымсаков Т.А. Основы теории процессов Маркова. – М.: Гос. изд. техн.-теор. лит., 1954. – 208 с.

11. Колмогоров А.Н. Элементы теории функций и функционального анализа / А.Н. Колмогоров, С.В. Фомин. – М.: Наука, 1989. – 624 с.

12. Кемени Дж. Конечные цепи Маркова / Дж. Кемени, Дж. Снелл. – М.: Наука, 1970. – 272 с.

13. Маркус М. Обзор по теории матриц и матричных неравенств / М. Маркус, Х. Минк. – М.: Наука, 1972. – 232 с.

Мельников Сергей Юрьевич
Канд. физ.-мат. наук, зам. ген. директора ООО «Лингвистические и информационные технологии», г. Москва
Тел.: 8 (495) 792-39-25
Эл. почта: info@linfotech.ru

Melnikov S.Yu.

On the finite automaton output function with the random input by the frequency of a word in the output sequence

The article deals with the problem of finding the output function of finite automaton with the random input by the relevant frequency of a certain word in its output sequence. The problem reduces to the discrete minimization of the linear form module. When binary shift register is regarded as finite automaton and character characteristic of the output sequence, the problem reduces to the integer-valued minimization of the linear form module under the linear constraints. The dimension of the problem is equal to the span of the register plus one, i.e. is on logarithmic dependence on the quantity of states.

Keywords: finite automaton; finding the output function; discrete minimization; shift register.
