Критерий регулярности булевского неавтономного автомата с разделенным входом

В.А. Носов

В работе получен критерий регулярности неавтономного автомата с двоичными алфавитами, не сводящийся к проверке регулярности частичных функций перехода. Проверка регулярности неавтономного автомата сведена к проверке регулярности единственного семейства булевых функций и проверке свойства, названного правильностью, другого семейства булевых функций, причем оба семейства естественно ассоциированы с функцией перехода автомата.

1 Введение

Пусть $A = (I, S, \delta)$ – произвольный конечный автомат без выхода, где I – множество входов, S – множество состояний, $\delta : I \times S \to S$ – функция переходов. Автомат A называется регулярным (перестановочным) если для любого $a \in I$ функция $\delta(i, s)|_{i=a}$ является биекцией множества S. Будем предполагать, что автомат A задан в булевской форме, т.е. $I = E_k$, $S = E_n$ – множества двоичных наборов длин k и n соответственно, δ задано семейством из n булевских функций от $k + n$ переменных $x_1, \dots, x_k$, $y_1, \dots, y_n$, где $(x_1, \dots, x_k) \in E_k$, $(y_1, \dots, y_n) \in E_n$, $\delta = (f_1, \dots f_n)$, $f_i = f_i(x_1, \dots, x_k, y_1, \dots, y_n)$, $i \in \overline{1, n}$.

Будем предполагать также, что входы автомата A разделены, т.е. для всех $i \in \overline{1, n}$ выполнено условие

$$f_i = f_i(x_i, y_1, , \dots, y_n) \tag{1}$$

(при этом $k = n$).

Другими словами, при разделенном входе каждая функция f_i зависит точно от одного бита входа. Регулярность автономных булевских автоматов рассматривалась в работах [1], [2], [3], в которых был получен ряд критериев регулярности. Ясно, что вопрос о регулярности неавтономного автомата сводится к проверке регулярности $|I|$ автономных автоматов, причем для булевской формы автомата $|I| = 2^k$, а для случая разделенного входа $|I| = 2^n$.

Наша цель – получить прямой критерий регулярности неавтономного булевского автомата с разделенным входом.

2 Переход к каноническим координатам

Пусть функция переходов автомата задана функциями $(f_1, ..., f_n)$, где $f_i = f_i(x_i, y_1, \ldots, y_n)$, $i \in \overline{1,n}$. Разложим каждую функцию f_i по переменной x_i в виде $f_i = g_i \cdot x_i + h_i$, где $g_i = g_i(y_1, \ldots, y_n)$, $h_i = h_i(y_1, \ldots, y_n)$, $i \in \overline{1,n}$.

Для регулярности автомата необходимо, чтобы функция $(h_1, \ldots, h_n)$ обладала свойством регулярности, поэтому, предполагая это условие выполненным, произведем замену переменных

$$h_i(y_1, \ldots, y_n) = z_i, \qquad i = \overline{1,n}$$

Тогда функция переходов автомата представляется в виде

$$F_i(z_1, \ldots, z_n) \cdot x_i + z_i, \qquad i = \overline{1,n} \tag{2}$$

где

$$F_i = g_i\left(h_1^{-1}(z_1, \ldots, z_n), \ldots, h_n^{-1}(z_1, \ldots, z_n)\right).$$

Про формулы (2) будем говорить, что функция переходов задана в канонических координатах.

Для произвольного семейства булевских функций $F_1, \ldots, F_n$ от переменных $z_1, \ldots, z_n$ определим $\forall\exists$-свойство (свойство правильности) условиями:

$$\begin{array}{l}\text{Для любых } (z'_1, \ldots, z'_n) \neq (z''_1, \ldots, z''_n) \text{ существует} \\ \alpha \in \overline{1,n}, \text{ такое, что } z'_\alpha \neq z''_\alpha,\ F_\alpha(z'_1, \ldots, z'_n) = F_\alpha(z''_1, \ldots, z''_n)\end{array} \tag{3}$$

Лемма 1 *Для регулярности семейства функций (2) при всех $(x_1, \ldots, x_n)$ необходимо и достаточно, чтобы для семейства функций $(F_1, \ldots, F_n)$ выполнялось свойство правильности (3).*

Доказательство. Пусть семейство $(F_1, \ldots, F_n)$ удовлетворяет условию правильности (3). Пусть $a = (a_1, \ldots, a_n)$, $z' = (z'_1, \ldots, z'_n)$, $z'' = (z''_1, \ldots, z''_n)$ – произвольные двоичные наборы, причем $z' \neq z''$. По условию существует $\alpha \in \overline{1,n}$, такое, что выполнено $z'_\alpha \neq z''_\alpha$, $F_\alpha(z') = F_\alpha(z'')$.

Тогда имеем $z'_\alpha + a_\alpha \cdot F_\alpha(z') \neq z''_\alpha + a_\alpha \cdot F_\alpha(z'')$ и, следовательно, семейство (2) регулярно при $(x_1, \dots, x_n)(a_1, \dots, a_n)$.

Пусть теперь семейство $(F_1, \dots, F_n)$ не удовлетворяет условию правильности (3). Значит, существуют наборы z' и z'', $z' \neq z''$, такие, что для всех $\alpha \in \overline{1,n}$, для которых $z'_\alpha \neq z''_\alpha$ выполнено $F_\alpha(z') \neq F_\alpha(z'')$. Определим семейство $a = (a_1, \dots, a_n)$ где $a_\alpha = z'_\alpha + z''_\alpha$, $a \in \overline{1,n}$. Для выбранных a_α имеем для всех $\alpha \in \overline{1,n}$

$$z'_\alpha + a_\alpha F_\alpha(z') = z''_\alpha + a_\alpha F_\alpha(z'').$$

Это означает, что семейство функций (2) не регулярно при $(x_1, \dots, x_n) = (a_1, \dots, a_n)$.

3 Критерий правильности семейства булевых функций

В предыдущем разделе приведен критерий проверки правильности семейств булевых функций, основанный на проверке табличных свойств функций. Рассмотрим задачу отыскания соответствующего критерия, основанного на проверке аналитических свойств функций, что может привести к построению более эффективных алгоритмов. В настоящем разделе дается такой критерий и показывается, что рассматриваемая задача является NP-трудной.

Для семейства булевых функций $f = (f_i)$, $i = \overline{1,n}$ определим семейство $\check{f} = (\check{f}_i)$, $i = \overline{1,n}$, где для любого $i \in [1,n]$ имеем

$$\check{f}_i = x_i + f_i$$

Пусть I – некоторое множество индексов, где $I \subset [1,n]$ и $\varepsilon_I = (\varepsilon_\alpha)$, $\alpha \in I$, $\varepsilon_\alpha \in < 0, 1 >$ – семейство констант с индексами из множества I. Определим семейство функций аналогично предыдущему

$$\check{f}^0_{CI} = (\check{f}^0_i), \qquad i \in CI$$

где CI – дополнение множества I в $[1,n]$, полагая для любого $\lambda \in CI$

$$\check{f}^0_\lambda(x) = \check{f}_\lambda(x)|_{x_\alpha = \varepsilon_\alpha}, \qquad \alpha \in I \tag{1}$$

Другими словами, $\check{f}^0$ - это функции семейства $\check{f}$ с индексами из множества CI, в которых переменные с индексами из I замещены константами семейства ε_I.

Справедлива

Лемма 2 *Семейство булевых функций f правильно тогда и только тогда, когда для любого множества $I \subset [1,n]$ и любого семейства констант ε_I семейство $\check{f}^0_{CI}$ будет регулярным, т.е. будет осуществлять взаимно однозначное отображение соответствующих наборов (x_i), $i \in CI$.*

Доказательство аналогично доказательству леммы 1.

Для дальнейшего нам понадобится один из критериев регулярности семейства булевых функций – критерий Хаффмена [6]: семейство булевых функций $f = (f_i)$, $i = \overline{1,n}$ регулярно тогда и только тогда, когда все произведения $f_{i_1}, \ldots, f_{i_s}$, $1 \leq s \leq n-1$ не содержат в приведенной полиномиальной записи члена $x_1 \ldots x_n$, а произведение $f_1 \ldots f_n$ содержит такой член.

Введем некоторые определения. Пусть $f(x_1, \ldots, x_n)$ – булева функция от n переменных и $I \subseteq [1,n]$. Множество переменных $x_I = (x_i)$, $i \in I$, где для определенности возьмем $I = [1,s]$, $1 \leq s \leq n$, будем называть существенным для функции f, если

$$\sum_{\alpha_1,\ldots,\alpha_s} f(\alpha_1, \ldots, \alpha_s, x_{s+1}, \ldots, x_n) \not\equiv 0 \quad \text{(сумма по модулю 2)} \tag{2}$$

При $s = 1$ мы имеем определение существенности одного переменного. При $s = n$ утверждение о существенности множества переменных (x_i), $i \in [1,n]$ равносильно нечетности веса f.

Легко проверить, что множество переменных $x_I = (x_i)$, $i \in I$ существенно для функции $f(x_1, \ldots, x_n)$ тогда и только тогда, когда в канонической полиномиальной записи разложения функции f по переменным x_i, $i \in I$ коэффициент у произведения $\prod\limits_{i \in I} x_i$ не будет тождественно равен нулю. Это следует из хорошо известного тождества

$$\begin{aligned} f(x_1, ..., x_n) &= \bigvee_{\alpha_1,\ldots,\alpha_s} f(\alpha_1, ..., \alpha_s, x_{s+1}, ..., x_n) x_1^{\alpha_1} ... x_s^{\alpha_s} = \\ &= \sum_{\alpha_1,\ldots,\alpha_s} f(\alpha_1, ..., \alpha_s, x_{s+1}, ..., x_n)(x_1 + \alpha_1 + 1)...(x_s + \alpha_s + 1) \end{aligned} \tag{3}$$

Для дальнейшего нам понадобятся две технические леммы, легко доказываемые непосредственно на основе определения.

Лемма 3 *Если множество переменных $x_S = (x_i)$, $i \in S$, $S \subseteq [1,n]$ существенно для функции $f(x_1, \ldots, x_n)$, то множество переменных $x_P = (x_i)$, $i \in P$, $P \subseteq [1,n]$ также будет существенным при $P \subset S$.*

Лемма 4 *Пусть функция $f^0(x_1, \ldots, x_n)$ получена из функции $f(y_1, \ldots, y_m)$ путем замещения некоторых переменных константами.*

Пусть множество переменных $x_I = (x_i)$, $i \in I$, $I \subseteq [1,n]$ существенно для функции $f^0(x_1,\ldots,x_n)$. Тогда оно существенно и для функции $f(y_1,\ldots,y_m)$.

Справедлива следующая

Теорема 1 *Семейство булевых функций $f = (f_i)$, $i \in [1,n]$ будет правильным тогда и только тогда, когда для любого подмножества I, $I \subseteq [1,n]$ произведение функций $\prod\limits_{i\in I} f_i$ не зависит существенно от множества переменных $x_I = (x_i)$, $i \in I$.*

Доказательство. Необходимость. Пусть условие – для любого подмножества I, $I \subseteq [1,n]$ произведение функций $\prod\limits_{i\in I} f_i$ не зависит существенно от множества переменных $x_I = (x_i)$, $i \in I$ – не выполняется. Значит существует $I \subseteq [1,n]$, для которого $\prod\limits_{i\in I} f_i$ зависит существенно от $x_I = (x_i)$, $i \in I$. Из всех таких множеств выберем минимальное по включению множество. Пусть для определенности $I = \{i_1,\ldots,i_s\}$. Покажем, что найдется набор констант, заместив которыми переменные x_i, $i \in CI$, в функциях семейства $\check{f}_i = x_i + f_i$, $i \in I$, получим нерегулярное семейство $\check{f}^0 = (\check{f}_i^0)$, $i \in I$.

Рассмотрим произведение

$$\prod_{i\in I} \check{f}_i = \prod_{i\in I}(x_i + f_i) = \prod_{i\in I} x_i + \sum_{(L_1,L_2)} \prod_{i\in L_1} x_i \cdot \prod_{j\in L_2} f_j + \prod_{i\in I} f_i \qquad (4)$$

где сумма в (4) распространяется по всем разбиениям множества I на сумму непустых множеств L_1, L_2, т.е. таким L_1, L_2, что $I = L_1 \cup L_2$, $L_1 \cap L_2 = \emptyset$.

По условию, произведение $\prod\limits_{i\in I} f_i$ существенно зависит от множества переменных $x_I = (x_i)$, $i \in I$. Значит, существует набор констант ε_{CI} для переменных с индексами из CI, такой, что функция

$$\prod_{i\in I} f_i|_{x_\alpha=\varepsilon_\alpha}, \qquad \alpha \in CI \qquad (5)$$

содержит член $\prod\limits_{i\in I} x_i$ в приведенной канонической записи.

Подставим данный набор констант ε_{CI} в остальные члены соотношения (4).

Покажем, что $\prod\limits_{i\in L_1} x_i \cdot \prod\limits_{j\in L_2} f_j^0$, где f_j^0 – функция, получившаяся из f_j при подстановке констант, не содержит члена $\prod\limits_{i\in I} x_i$ в канонической записи при любых непустых L_1, L_2. Предположим противное.

Пусть произведение $\prod\limits_{i\in L_1} x_i \cdot \prod\limits_{j\in L_2} f_j$ дает член $\prod\limits_{i\in I} x_i$ в приведенной канонической записи при некоторых L_1, L_2. Это значит, что $\prod\limits_{j\in L_2} f_j^0$ имеет нечетное число членов, которые имеют вхождение члена $\prod\limits_{i\in L_2} x_i$, в противном случае при умножении на $\prod\limits_{i\in L_1} x_i$ все члены $\prod\limits_{i\in I} x_i$ уничтожатся. Тогда функция $\prod\limits_{j\in L_2} f_j^0$ может быть записана в виде

$$\prod_{j\in L_2} f_j^0 = \prod_{i\in L_2} x_i(Q_1((x_\lambda), \lambda \notin L_2) + Q_2((x_\lambda), \lambda \in [1, n])) \qquad (6)$$

где полином $Q_1((x_\lambda), \lambda \notin L_2)$ не зависит от переменных с индексами из L_2 и имеет нечетное число членов, полином Q_2 имеет степень меньшую, чем $|L_2|$ по переменным x_i, $i \in L_2$.

Из (6) следует, что при $x_\lambda = 1$, $\lambda \notin L_2$ коэффициент при $\prod\limits_{i\in L_2} x_i$ обращается в единицу и, значит, множество переменных $x_{L_2} = (x_i)$, $i \in L_2$ будет существенным для функции $\prod\limits_{j\in L_2} f_j^0$, а значит по лемме 3 оно будет существенным и для функции $\prod\limits_{j\in L_2} f_j$. Поскольку $L_2 \subset I$ – собственное подмножество, то это противоречит предположению о минимальности множества I. Значит, в соотношении (4) после замещения переменных x_α, $\alpha \in CI$ указанными константами ε_{CI}, получим только два вхождения члена $\prod\limits_{i\in I} x_i$, которые уничтожаются, и функция $\prod\limits_{i\in I} \check{f}_i^0$ не будет содержать члена $\prod\limits_{i\in I} x_i$. Следовательно, семейство $f_I^0 = (f_i^0)$, $i \in I$ не удовлетворяет критерию Хаффмена для регулярности и согласно сделанному выше замечанию (лемма 2) семейство f не является правильным. Необходимость доказана.

Достаточность. Пусть для любого подмножества $I \subseteq [1, n]$ произведение функций $\prod\limits_{i\in I} f_i$ не зависит существенно от множества переменных $x_I = (x_i)$, $i \in I$. Покажем, что отсюда следует правильность семейства $f = (f_i)$, $i \in [1, n]$. Для этого достаточно показать, в силу сделанного выше замечания, что семейство $\check{f}_{CI}^0 = (\check{f}_i^0)$, $i \in CI$, $\check{f}_i^0 = (x_i + f_i^0)$, $i \in CI$ удовлетворяет критерию регулярности Хаффмена при любом $I \subseteq [1, n]$ и любом семействе констант ε_I.

Пусть сначала $I = \emptyset$. Рассмотрим произведение $\prod\limits_{i=1}^{n} \check{f}_i = \prod\limits_{i=1}^{n}(x_i + f_i)$ и покажем, что оно содержит член $\prod\limits_{i=1}^{n} x_i$.

Имеем

$$\prod_{i=1}^{n}(x_i+f_i)=\prod_{i=1}^{n}x_i+\sum_{(L_1,L_2)}\prod_{i\in L_1}x_i\cdot\prod_{j\in L_2}f_j+\prod_{i=1}^{n}f_i, \tag{7}$$

где сумма в (7) распространяется по всем непустым разбиениям (L_1, L_2) множества $[1, n]$.

Произведение $\prod\limits_{i=1}^{n} f_i$ не содержит члена $\prod\limits_{i=1}^{n} x_i$ по условию. Покажем, что при любых непустых L_1, L_2 произведение $\prod\limits_{i\in L_1} x_i \cdot \prod\limits_{j\in L_2} f_j$ не дает члена $\prod\limits_{i=1}^{n} x_i$.

Предположим противное и пусть существуют такие непустые L_1, L_2. Это значит, что $\prod\limits_{j\in L_2} f_j$ содержит нечетное число членов, содержащих вхождение произведения $\prod\limits_{j\in L_2} x_j$. Запишем $\prod\limits_{j\in L_2} f_j$ в виде

$$\Phi_{L_2}=\prod_{j\in L_2}f_j=\prod_{j\in L_2}x_i\cdot(Q_1((x_\lambda),\lambda\notin L_2))+Q_2((x_\lambda),\lambda\in[1,n]), \tag{8}$$

где многочлен $Q_1((x_\lambda), \lambda \notin L_2)$ имеет нечетное число членов, а многочлен Q_2 имеет степень по переменным x_λ, $\lambda \in L_2$ меньшую, чем $|L_2|$. Полагая в (8) $x_\lambda = 1$, $\lambda \in L_1$, получим $Q_1((x_\lambda)\lambda \notin L_2) = 1$ и, значит, $\Phi^0_{L_2}$ при данной фиксации переменных x_λ, $\lambda \in L_1$, существенно зависит от множества переменных $x_{L_2} = (x_i)$, $i \in L_2$. Значит, по лемме 3 и функция Φ_{L_2} также существенно зависит от $x_{L_2} = (x_i)$, $i \in L_2$, что противоречит условию. Значит, в (7) первый член $\prod\limits_{i=1}^{n} x_i$ не может уничтожиться и произведение $\prod\limits_{i=1}^{n} \check{f}_i$ содержит член $\prod\limits_{i=1}^{n} x_i$.

Пусть теперь $M \subset [1, n]$ – собственное подмножество.

Рассмотрим произведение $\Phi_M = \prod\limits_{i\in M} \check{f}_i \prod\limits_{i\in M} (x_i + f_i)$ и покажем, что оно не содержит члена $\prod\limits_{i=1}^{n} x_i$ при любом $M \subset [1, n]$.

Имеем

$$\prod_{i\in M}(x_i+f_i)=\prod_{i\in M}x_i+\sum_{(L_1,L_2)}\prod_{i\in L_1}x_i\cdot\prod_{j\in L_2}f_j+\prod_{j\in M}f_j, \tag{9}$$

где сумма в (9) распространяется по всем непустым разбиениям (L_1, L_2) множества M.

Произведение $\prod_{i\in M} f_i$ не содержит члена $\prod_{i=1}^{n} x_i$, поскольку это означало бы, что множество переменных (x_i), $i \in [1,n]$ существенно для $\Phi_M = \prod_{i\in M} f_i$, а значит и его подмножество $x_M = (x_i)$, $i \in M$ по лемме 3 также существенно для Φ_M, что противоречит условию.

Далее, для любых непустых L_1, L_2 произведение $\prod_{i\in L_1} x_i \cdot \prod_{j\in L_2} f_j$ не может давать члена $\prod_{i=1}^{n} x_i$. Если, напротив, это имеет место для фиксированных L_1, L_2, то $\prod_{j\in L_2} f_j$ содержит нечетное число членов, имеющих вхождение $\prod_{i\in CL_1} x_i$, где CL_1 – дополнение множества L_1 в $[1,n]$. Аналогично проделанному выше, представляем

$$\Phi_{L_2} = \prod_{j\in L_2} f_j = \prod_{i\in CL_1} x_i \cdot (Q_1((x_\lambda), \lambda \in L_1)) + Q_2((x_\lambda), \lambda \in [1,n]), \qquad (10)$$

где Q_1 имеет нечетное число членов, Q_2 имеет степень по переменным x_λ, $\lambda \in CL_1$ меньшую, чем $|CL_1|$.

Полагая в (10) $x_\lambda = 1$, $\lambda \in L_1$, получаем $Q_1 = 1$ и, значит, $\Phi^0_{L_2}$ существенно зависит от (x_i), $i \in CL_1$. Следовательно, и Φ_{L_2} существенно зависит от (x_i), $i \in CL_1$. Поскольку $L_2 \subset CL_1$, то Φ_{L_2} существенно зависит и от $x_{L_2} = (x_i)$, $i \in L_2$, что противоречит условию. Таким образом, в (9) нет членов, дающих произведение $\prod_{i=1}^{n} x_i$.

Таким образом, семейство $\check{f}$ таково, что $\prod_{i=1}^{n} \check{f}_i$ содержит член $\prod_{i=1}^{n} x_i$, а $\prod_{i\in M} \check{f}_i$ не содержит члена $\prod_{i=1}^{n} x_i$ при любом $M \subset [1,n]$. Значит, согласно критерию Хаффмена, семейство f будет регулярным, и случай $I = \emptyset$ разобран полностью.

Пусть теперь $I \neq \emptyset$, $CI \neq \emptyset$ и ε_I – соответствующее произвольное множество констант. Покажем, что соответствующее семейство $\check{f}^0_{CI}$ будет регулярным.

Снова проверим выполнение критерия Хаффмена.

Рассмотрим $\Phi^0_{CI} = \prod_{i\in CI} (x_i + f^0_i)$.

Имеем

$$\Phi^0_{CI} = \prod_{i\in CI} x_i + \sum_{(L_1,L_2)} \prod_{i\in L_1} x_i \cdot \prod_{j\in L_2} f^0_j + \prod_{i\in CI} f^0_i, \qquad (11)$$

где сумма распространяется по всем непустым разбиениям L_1, L_2 множества CI.

Аналогично предыдущему, $\prod\limits_{i\in CI} f_i^0$ не содержит члена $\prod\limits_{i\in CI} x_i$, так как в противном случае множество переменных (x_i), $i \in CI$ было бы существенным для Φ_{CI}^0, а следовательно, существенным и для Φ_{CI}, что противоречило бы условию.

Далее, произведение $\prod\limits_{i\in L_1} x_i \cdot \prod\limits_{j\in L_2} f_j^0$ также не содержит члена $\prod\limits_{i\in CI} x_i$ при любых непустых L_1, L_2. Если это не так, например для фиксированного разбиения L_1, L_2, то в этом случае $\prod\limits_{j\in L_2} f_j^0$ содержит нечетное число членов, содержащих вхождение $\prod\limits_{i\in L_2} x_i$. Представляя $\prod\limits_{j\in L_2} f_j^0$ в виде

$$\prod_{i\in L_2} x_i \cdot Q_1((x_\lambda), \lambda \in L_1) + Q_2((x_\lambda), \lambda \in CI), \tag{12}$$

где Q_1 имеет нечетное число членов, Q_2 имеет степень по переменным x_λ, $\lambda \in L_2$ меньшую, чем $|L_2|$ и, полагая в (12) $x_\lambda = 1$, $\lambda \in L_1$, убеждаемся, что $\prod\limits_{j\in L_2} f_j^0$ существенно зависит от (x_i), $i \in L_2$. Значит и $\prod\limits_{j\in L_2} f_j$ существенно зависит от данного множества переменных. Последнее противоречит условию.

Значит, в (11) член $\prod\limits_{i\in CI} x_i$ не может уничтожиться.

Аналогично показывается, что функция $\Phi_M = \prod\limits_{i\in M} (x_i + f_i^0)$, где $M \subset CI$ – собственное подмножество, не содержит члена $\prod\limits_{i\in CI} x_i$. Имеем

$$\Phi_M = \prod_{i\in M} x_i + \sum_{(L_1,L_2)} \prod_{i\in L_1} x_i \cdot \prod_{j\in L_2} f_j^0 + \prod_{i\in M} f_i^0 \tag{13}$$

(сумма по всем непустым разбиениям (L_1, L_2) множества M).

Если произведение $\prod\limits_{i\in M} f_i^0$ дает член $\prod\limits_{i\in CI} x_i$, то аналогично предыдущему, множество переменных $x_M = (x_i)$, $i \in M$ будет существенным для $\prod\limits_{i\in M} f_i$, что противоречит условию.

Произведение $\prod\limits_{i\in L_1} x_i \cdot \prod\limits_{j\in L_2} f_j^0$ также не дает члена $\prod\limits_{i\in CI} x_i$ при любых непустых L_1, L_2. В противном случае $\Phi_{L_2}^0 = \prod\limits_{j\in L_2} f_j^0$ имеет нечетное число членов, содержащих вхождение $\prod\limits_{i\in CL_1} x_i$, CL_1 – дополнение L_1 в CI.

Полагая $x_\lambda = 1$, $\lambda \in CI$, $\lambda \notin CL_1$, в $\Phi_{L_2}^0$ получаем, что соответствующая функция $\Phi_{L_2}^{00}$ существенно зависит от множества переменных $x_{CL_1} = (x_i)$, $i \in CL_1$. Следовательно, эти переменные существенны и для Φ_{L_2}, а значит Φ_{L_2} существенно зависит от $x_{L_2} = (x_i)$, $i \in L_2$, поскольку $L_2 \subset CL_1$. Согласно (13), функция Φ_M не содержит члена $\prod\limits_{i \in CI} x_i$. По критерию Хаффмена семейство $\check{f}^0_{CI}$ будет регулярным, а значит, согласно отмеченному выше, исходное семейство будет правильным.

Теорема доказана.

Покажем теперь, что если $P \neq NP$, то для задачи проверки правильности произвольного семейства функций не существует полиномиальных разрешающих алгоритмов. Аналогичное явление имеет место и для задачи проверки регулярности [5].

Справедлива

Теорема 2 *Пусть дано семейство n булевых функций $f = (f_i)$, $i = \overline{1, n}$ от переменных $x_1, \ldots, x_n$, заданных в КНФ. Тогда задача проверки правильности семейства f является NP-трудной.*

Доказательство. Пусть $f(x_1, \ldots, x_n)$ – произвольная индивидуальная задача "выполнимость". Рассмотрим следующее семейство из $n + 1$ булевых функций $f^* = (\underbrace{1, \ldots, 1}_{n}, x_{n+1} \cdot f(x_1, \ldots, x_n))$, где x_{n+1} – новая переменная. Ясно, что семейство f^* строится по функции f за полиномиальное время. Нетрудно проверить, что семейство f^* будет правильным тогда и только тогда, когда функция f не выполнима. Значит, если имеется полиномиальный алгоритм проверки правильности произвольного семейства, то, применяя его к семейству f^*, получаем полиномиальный алгоритм проверки выполнимости произвольной КНФ, которая является NP-полной задачей [5].

Таким образом, установлено, что задача проверки регулярности неавтономного булевского автомата с разделенным входом сводится к проверке регулярности семейства булевых функций, получаемых на нулевом входе, и проверке правильности семейства булевых функций, получаемого при переходе к каноническим координатам.

Список литературы

[1] Клосс Б.М., Малышев В.А. Определение регулярности автомата по его каноническим уравнениям. ДАН СССР, 1967, т. 172, N 3, с. 543-546.

[2] Клосс Б.М., Нечипорук Э.И. О классификации функций многозначной логики. Пробл. кибернетики, 1963, вып. 3, с. 27-36.

[3] Применко Э.А., Скворцов Э.Ф. Об условиях регулярности конечных автономных автоматов. Дискретная математика, 1990, т. 2, вып. 1, с. 26-30.

[4] Кудрявцев В.Б., Подколзин А.С., Ушчумлич Ш. Введение в теорию абстрактных автоматов. МГУ, 1985.

[5] Алексеев В.Б., Носов В.А. NP-полные задачи и их полиномиальные варианты. Обзор. Обозрение прикладной и промышленной математики, 1997, т. 4, вып. 2, с. 165-193.

[6] Huffman D.A. Canonical forms for information lossless finite-state logical machines. IRE Trans. Circ. Theory, 1959, v. 6, p. 41-59.