О связи функций автомата и автоматной функции

В. Г. Гербуз

В статье исследуется зависимость между принадлежностью внутренних функций автомата к предполным классам булевых функций с реализацией автоматом словарной функции из того же класса.

Ключевые слова: теория автоматов, предполные классы, словарная функция.

Произвольный автомат можно рассматривать либо как словарную функцию, которую он реализует, либо с точки зрения его внутреннего устройства: функций переходов и выходов. В обоих случаях можно говорить о принадлежности указанных функций к некоторому классу Поста. Так, например, в статье [2] рассматривается возможность построения линейных кодировок класса переходных систем. В данной работе рассматривается аналогичная задача: для предполных классов P_2 устанавливается связь между принадлежностью автоматной функции к данному классу с возможностью кодировки внутренних функций автомата в том же классе.

Везде в данной статье, если явно не указано иное, под «автоматом» понимается приведенный инициальный конечный детерминированный автомат с одним выходом и булевыми входным и выходным алфавитами.

Определение 1. Пусть дан автомат $\langle E_2^k, E_2, Q, \varphi, \psi \rangle$. Инъективную функцию $Num : Q \to E_2^m$ назовем *кодированием* автомата, а сам автомат с заданной функцией Num — *автоматом с кодированием.*

Функции переходов и выходов кодированного автомата естественным образом порождают булевые функции переходов и выходов.

Пусть K — некоторый замкнутый класс булевых функций. Будем говорить, что автомат A *допускает кодировку из* K, если существует такое кодирование, в котором соответствующие функции перехода и выхода принадлежат классу K.

Определение 2. Замкнутый класс булевых функций K назовем обладающим свойством *прямого наследования*, если для любого автомата A, допускающего кодировку из K, выполнено $f_A \in K$, где f_A есть словарная функция, реализуемая данным автоматом.

Определение 3. Замкнутый класс булевых функций K назовем обладающим свойством *обратного наследования*, если любой автомат A со свойством $f_A \in K$ допускает кодировку из K.

Замечание 1. Из определений следует, что класс P_2 всех булевых функций имеет свойства прямого и обратного наследования.

В данной работе исследуются свойства наследования для предполных классов в P_2. Согласно [1] существует 5 указанных классов: классы функций, сохраняющих константы 0 и 1 — T_0 и T_1 соответственно, классы линейных L, самодвойственных S и монотонных M функций.

Теорема 1. *Для предполных классов в P_2 имеют место следующие утверждения:*

1) *класс L обладает свойством прямого наследования, но не обладает свойством обратного.*
2) *классы T_0, T_1, S обладают свойством обратного наследования, но не обладает свойством прямого наследования.*
3) *класс M обладает свойствами прямого и обратного наследования*

Доказательство данной теоремы приведем в виде серии теорем и лемм.

Лемма 1. *Если $0, 1 \in K$, то K обладает свойством прямого наследования.*

Доказательство. Пусть задан автомат $A = \langle E_2^k, E_2, Q, \varphi, \psi, q_0 \rangle$ с кодировкой, что равносильно представлению Q, как подмножества E_2^m для некоторого m. В этом представлении функции $\varphi : E_2^m \times E_2^k \to E_2^m$ и $\psi : E_2^m \times E_2^k \to E_2$ принадлежат классу K (в первом случае покомпонентно). Тогда рассмотрим автоматную функцию f_A, реализуемую данным автоматом:

$$f_A(x_1, \ldots, x_n) = \psi(\varphi(\ldots(\varphi(q_0, x_1), x_2), \ldots), x_n).$$

Так как $0, 1 \in K$, то $q_0 \in K$, откуда $f_A \in K$, как суперпозиция функций из K.

Следствие 1. *Классы L, M являются классами прямого наследования.*

Лемма 2. *Пусть K — замкнутый класс булевых функций, обладающий свойством: для любой функции $f \in P_2$ найдется функция $g_f \in K$ такая, что $f(\vec{x}) = g_f(\vec{x}, \vec{c})$, где $\vec{x} = (x_1, \dots, x_n)$ — переменные, а $\vec{c} = (c_1, \dots, c_m)$ — некоторый набор констант. Тогда любой автомат допускает кодировку из K.*

Доказательство. Пусть задан произвольный автомат $A = \langle E_2^k, E_2, Q, \varphi, \psi, q_0\rangle$ с кодировкой $Num : Q \to E_2^m$. С учетом этой кодировки можно считать, что $\varphi(x) = (\varphi_1(x), \dots, \varphi_m(x))$ и $\varphi_1, \dots, \varphi_m, \psi : E_2^{k+m} \to E_2$. По условию леммы существуют функции и соответствующие константы такие, что $g_{\varphi_1}(x, c_1) = \varphi_1(x), \dots, g_{\varphi_m}(x, c_m) = \varphi_m(x), g_\psi(x, c_{m+1}) = \psi(x), g_0(x, c_{m+2}) = 0, g_1(x, c_{m+3}) = 1$, где $x \in E_2^{k+m}, c_1 \in E_2^{l_1}, \dots, c_{m+3} \in E_2^{l_{m+3}}$. Добавим к полученным функциям фиктивные переменные, чтобы они зависели от одного набора переменных. Пусть

$$
\begin{gathered}
h_{\varphi_1}(x, y_1, y_2, \dots, y_{m+3}) = g_{\varphi_1}(x, y_1) \\
h_{\varphi_2}(x, y_1, y_2, \dots, y_{m+3}) = g_{\varphi_2}(x, y_2) \\
\dots \\
h_{\varphi_m}(x, y_1, y_2, \dots, y_{m+3}) = g_{\varphi_m}(x, y_m) \\
h_\psi(x, y_1, y_2, \dots, y_{m+3}) = g_\psi(x, y_{m+1}) \\
h_0(x, y_1, y_2, \dots, y_{m+3}) = g_0(x, y_{m+2}) \\
h_1(x, y_1, y_2, \dots, y_{m+3}) = g_1(x, y_{m+3})
\end{gathered}
$$

Тогда введем новую кодировку состояний $Num' : Q \to E_2^{k+m+l_1+\ldots+l_{m+3}}$, а именно $Num'(q) = Num(q)c_1c_2\ldots c_{m+3}$ (то есть составим конкатенацию старого значения и константных векторов). Для константного вектора $d = (d_1, \dots, d_l) \in E_2^l$ обозначим через h_d вектор-функцию $h_d(x, y_1, y_2, \dots, y_{m+3}) = (h_{d_1}, \dots, h_{d_l})$, составленную из построенных выше функций h_0 и h_1. Тогда новыми функциями переходов и выходов автомата A станут

$$
\begin{gathered}
\varphi'(x, y_1, y_2, \dots, y_{m+3}) = (h_{\varphi_1}, \dots, h_{\varphi_m}, h_{c_1}, \dots, h_{c_{m+3}}), \\
\psi'(x, y_1, y_2, \dots, y_{m+3}) = h_\psi(x, y_1, y_2, \dots, y_{m+3}).
\end{gathered}
$$

Так как функции $g_* \in K$, а функции h_* получены из них добавлением фиктивных переменных, то эти функции лежат в K, а значит и φ', ψ' тоже принадлежат K.

Следствие 2. *В условиях предыдущей леммы если $K \neq P_2$, то он является классом обратного наследования и не является классом прямого наследования.*

Доказательство. Пусть A — некоторый автомат, реализующий автоматную функцию $f_A \in K$. По лемме 2 существует кодировка A из K, то есть K — класс обратного наследования.

Так как $K \neq P_2$, то найдется автомат такой, что $f_A \notin K$. Согласно лемме 2 для него существует кодировка из K, то есть K не является классом прямого наследования.

Следствие 3. *Классы T_0, T_1, S имеют свойство обратного наследования, но не являются классами прямого наследования.*

Доказательство. Пусть задана произвольная функция алгебры логики $f(\vec{x}) \in P_2$, тогда построим соответствующие функции g_f и константы c для каждого из классов T_0, T_1, S.

$T_0: \quad g_f(\vec{x}, y) = \begin{cases} f(\vec{x}), \text{ если } y = 1 \\ \quad 0, \text{ если } y = 0 \end{cases}, \quad \vec{c} = (1).$

Заметим, что $g_f(\vec{0}, 0) = 0$, то есть $g_f \in T_0$ и $f(\vec{x}) = g_f(\vec{x}, \vec{c}) = g_f(\vec{x}, 1)$. Аналогично строится функция g_f для класса

$T_1: \quad g_f(\vec{x}, y) = \begin{cases} f(\vec{x}), \text{ если } y = 0 \\ \quad 0, \text{ если } y = 1 \end{cases}, \quad \vec{c} = (0)$, которая также удовлетворяет условиям.

Для класса самодвойственных функций имеем:

$S: \quad g_f(\vec{x}, y) = \begin{cases} f(\vec{x}), \text{ если } y = 0 \\ \overline{f(\vec{x})}, \text{ если } y = 1 \end{cases}, \quad \vec{c} = (0).$

Тогда $f(\vec{x}) = g_f(\vec{x}, 0)$ и

$$\overline{g_f}(\,\overline{\vec{x}, y}\,) = \overline{g_f}(\,\overline{\vec{x}}, \overline{y}) = \\ = \begin{cases} \overline{\overline{f(\overline{\overline{\vec{x}}})}}, \text{ если } y = 0 \\ \overline{f(\overline{\vec{x}})}, \text{ если } y = 1 \end{cases} = \begin{cases} f(\vec{x}), \text{ если } y = 0 \\ \overline{f(\overline{\vec{x}})}, \text{ если } y = 1 \end{cases} = g_f(\vec{x}, y)$$

то есть $g_f \in S$ и удовлетворяет условию леммы с константой $c = 0$.

Чтобы показать, что класс линейных функций не является классом обратного наследования, достаточно привести пример автомата с линейной выходной функцией, у которого не существует линейной кодировки. Диаграмма такого автомата представлена на рисунке 1 [1].

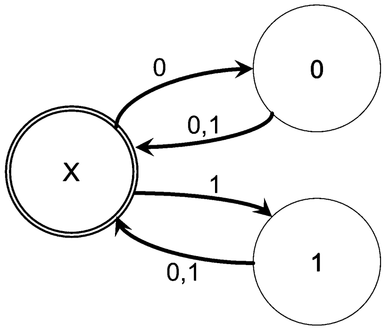

Рис. 1. Автомат без линейной кодировки.

Словарная функция данного автомата,

$$f_A(x_1, \ldots, x_n) = \begin{cases} x_{n-1}, & \text{если } n \text{ четное,} \\ x_n, & \text{если } n \text{ нечетное,} \end{cases}$$

как несложно заметить, является линейной при каждом значении n.

Допустим, что у некоторого автомата с m входами функция выходов ψ является линейной, тогда $\psi(x_1, \ldots, x_m, q) = L(x_1, \ldots, x_m) + l(q)$, где L и l — некоторые линейные функции, а q — некоторое кодирование состояний. Тогда в каждом фиксированном состоянии q_0 реализуется функция $\psi_{q_0}(x_1, \ldots, x_m) = L(x_1, \ldots, x_m) + C_{q_0}$, где $C_{q_0} = l(q_0)$ — константа, зависящая от q_0. Таким образом, в состояниях реализуется не более двух различных функций: с C_{q_0} равной 0 или 1.

Так как в состояниях автомата на рисунке 1 реализуется 3 различные функции, он не может иметь линейную функцию выхода при любом кодировании состояний.

Для доказательства теоремы 1 осталось показать, что M является классом обратного наследования. Для этого приведем алгоритм, который по заданному диаграммой Мура автомату A, реализующему монотонную автоматную функцию, строит монотонное кодирование данного автомата. Для начала докажем вспомогательную лемму.

Лемма 3 (О нумерации). *Для любого ориентированного графа* $F = \langle Q, E\rangle, n = |Q|$ *без циклов найдется* m *и инъективная функция нумерации его вершин* $Num:\ Q \to E_2^m$*, такая что* $Num(q_1) \preceq Num(q_2) \Leftrightarrow$ *существует путь из* q_1 *в* q_2*. Причем* $m \leqslant 2n-2$*, при* $n > 2$.

Доказательство. Для $P \subset Q$ введем обозначения: $q_1 \dashrightarrow q_2$, если существует путь из q_1 в q_2, $Gr(P) = \{q \in Q : \exists p \in P, p \dashrightarrow q\}$, $Ls(P) = \{q \in Q : \exists p \in P, q \dashrightarrow p\}$.

Утверждение леммы докажем индукцией по n. Для $n = 2$ в случае двух несвязных вершин $m = 2$: коды 01 и 10. Пусть доказано для всех $n < n_0$. Докажем для n_0. Рассмотрим любую вершину q_0, в которую не входит ни одно ребро. Удалим ее со всеми исходящими ребрами из графа F, получим граф F'. По предположению индукции, существует нумерация Num' графа F'. Тогда в графе F введем следующую нумерацию: $Num(q_0) = \underbrace{00\ldots0}_{|Num'|}10$, $\forall q \in Gr(q_0)\ Num(q) = Num'(q)11$, $\forall q \in Q \setminus Gr(q_0) Num(q) = Num'(q)01$, где $|Num'|$ — размерность булева куба — образа Num'.

Покажем, что это нумерация удовлетворяет условию. $Q = q_0 \cup Gr(q_0) \cup Q \setminus (Gr(q_0) \cup q_0)$. По построению функции Num, $Num(q_0) \preceq Num(q) \Leftrightarrow q \in Gr(q_0)$ и $\overline{\exists} q \in Q q \preceq q_0$, то есть для q_0 условие выполнено. Рассмотрим $q_1 \in Gr(q_0), q_2 \in Q \setminus (q_0 \cup Gr(q_0))$. Если $Num'(q_2) \preceq Num'(q_1)$, то $Num'(q_2)01 \preceq Num'(q_1)11 \Rightarrow Num(q_2) \preceq Num(q_1)$. $Num'(q_1) \preceq Num'(q_2)$ не может быть, так как в этом случае $q_2 \in Gr(q_1) \subset Gr(q_0)$. А если $Num'(q_1)$ и $Num'(q_2)$ несравнимы, то $Num(q_1)$ и $Num(q_2)$ тоже несравнимы. Таким образом, нумерация Num удовлетворяет условию леммы. Также заметим, что $|Num| = |Num'| + 2 \leqslant 2(n-1) - 2 + 2 = 2n - 2$.

Теорема 2. *Для любого (приведенного) автомата, реализующего монотонную автоматную функцию, существует монотонное кодирование данного автомата.*

Доказательство. Пусть диаграмма Мура приведенного конечного детерминированного автомата $A = \langle E_2^k, E_2, Q, \varphi, \psi\rangle$ задана в виде ориентированного графа $G = \langle Q, E\rangle$, где вершины из Q являются состояниями автомата A, а ребра из E показывают переходы между состояниями. Каждому ребру (q_1, q_2) приписана пара $(\alpha, \beta), \alpha \in E_2^k, \beta \in E_2$. Причем, $\varphi(q_1, \alpha) = q_2, \psi(q_1, \alpha) = \beta$. Будем строить новый ориентированный граф $F = \langle Q, M\rangle$, у которого множество вершин совпадает с множеством состояний данного автомата. Для начала в качестве множества ребер M рассмотрим множество упорядоченных пар $M_0 = \{(q,q)|q \in Q\}$. На k-ом шаге алгоритма рассмотрим множество

$$M_k = M_{k-1} \bigcup \Big\{(q_1,q_2)\Big| q_1,q_2 \in Q, \exists \tilde{q_1}, \tilde{q_2} \in Q, \alpha, \beta \in E_2,$$
$$(\tilde{q_1}, \tilde{q_2}) \in M_{k-1}, \alpha \preceq \beta, q_1 = \varphi(\tilde{q_1}, \alpha), q_2 = \varphi(\tilde{q_2}, \beta)\Big\}$$

Алгоритм завершает работу, если $M_k = M_{k-1}$, то есть к множеству M не добавилось новых элементов. Тогда все последующие множества $M_l = M_{k-1}, l > k$. Это сразу следует из построения множества M_k через M_{k-1}. Тогда примем $M = M_k$.

Покажем, что алгоритм совершит конечное число шагов.

Всего есть n^2 упорядоченных пар $(q_1,q_2), q_1,q_2 \in Q$. В силу критерия остановки алгоритма и по построению, $|M_k| > |M_{k-1}|$ и в то же время $|M_k| \leqslant n^2$ и $|M_0| = n$, значит в последовательности $\{M_k\}$ не более $n^2 - n = n(n-1)$ различных множеств, и алгоритм завершит работу за конечное число шагов, не превышающее $n(n-1)$.

Для дальнейшего построения кодировки и доказательства её корректности нам понадобятся несколько вспомогательных утверждений.

Утверждение 1. *В полученном графе F: $(q_1,q_2) \in M \iff$ найдутся $q \in Q$ и слова α, β одинаковой длины такие, что*

$$\alpha \preceq \beta, \quad q_1 = \varphi(q,\alpha), \quad q_2 = \varphi(q,\beta). \tag{1}$$

Доказательство. ($\Rightarrow$) Доказательство проведем индукцией по k, где $(q_1,q_2) \in M_K \setminus M_{k-1}$ (M_{-1} полагаем $\varnothing$).

Для $(q_1,q_2) \in M_0$ утверждение очевидно, так как $q_1 = q_2$ и можно положить $q = q_1, \alpha = \beta = \Lambda$ — пустое слово.

Пусть утверждение верно для всех ребер из множества M_{k-1} и $(q_1,q_2) \in M_k \setminus M_{k-1}$. По построению M_k, существует $(\tilde{q}_1, \tilde{q}_2) \in M_{k-1}$ и $a, b \in E_2$, такие что $a \leqslant b$, $q_1 = \varphi(\tilde{q}_1, a), q_2 = \varphi(\tilde{q}_2, b)$. По предположению индукции найдутся $q \in Q$, $\tilde{\alpha}, \tilde{\beta} \in E_2^*$, удовлетворяющие 1 для $(\tilde{q}_1, \tilde{q}_2)$. Тогда $\varphi(q, \tilde{\alpha}a) = \varphi(\tilde{q}_1, a) = q_1$, $\varphi(q, \tilde{\beta}b) = \varphi(\tilde{q}_2, b) = q_2$, то есть положив $\alpha = \tilde{\alpha}a$, $\beta = \tilde{\beta}b$, получаем требуемое условие для (q_1,q_2).

($\Leftarrow$) Следует из построения множества M.

Замечание 2. Для пары состояний (q_1, q_2) из условия 1 и монотонности словарной функции следует, что

$$f_{q_1} \leqslant f_{q_2}, \tag{2}$$

где f_{q_1} и f_{q_2} — словарные функции, реализуемые автоматом A с начальным состоянием q_1 и q_2 соответственно.

Утверждение 2. *Полученный граф F не содержит ориентированных циклов.*

Доказательство. Допустим, что в F существует ориентированный цикл $(q_1, \ldots, q_n)$, тогда согласно замечанию 2 имеем:$f_{q_1} \leqslant f_{q_2} \leqslant \ldots \leqslant f_{q_n} \leqslant f_{q_1}$, откуда $f_{q_1} = f_{q_2} = \ldots = f_{q_n}$, то есть состояния $q_1, \ldots, q_n$ — неразличимы, что противоречит предположению о приведенности исходного автомата.

(Продолжение доказательства теоремы 2.) Так как в графе F нет циклов, то по лемме о нумерации существует его вложение в булев куб с сохранением монотонности. То есть существует нумерация этого графа такая, что $Num(q_1) \leqslant Num(q_2) \Leftrightarrow (q_1, q_2) \in M$.

Используем полученную нумерацию для состояний автомата A и покажем, что соответствующие функции переходов и выходов являются монотонными. $\varphi(q, \alpha)$ монотонна по α, так как на первом шаге алгоритма из пары (q, q) при $\alpha \preceq \beta$ получим пару $(\varphi(q, \alpha), \varphi(q, \beta)) \in M$, откуда по построению нумераци $\varphi(q, \alpha) \preceq \varphi(q, \beta)$. Монотонность по q покажем так: пусть $q_1 \preceq q_2$, что равносильно $(q_1, q_2) \in M$, откуда $(\varphi(q_1, \alpha), \varphi(q_2, \alpha)) \in M \Rightarrow \varphi(q_1, \alpha) \preceq \varphi(q_2, \alpha)$. Монотонность функции выходов $\psi(q, \alpha)$ в каждом состоянии следует из условия, что автоматная функция f_A монотонна. Пусть $q_1 \preceq q_2$, тогда $(q_1, q_2) \in M$ и согласно замечанию 2 $f_{q_1} \leqslant f_{q_2}$,то есть ψ монотонна по q.

Автор выражает благодарность своему научному руководителю профессору Бабину Д. Н. за постановку задачи, помощь и консультации при написании этой статьи.

Список литературы

[1] Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986.

[2] Родин С. Б. Линейно реализуемые переходные системы // Интеллектуальные системы. — 2010. Т. 14, вып. 1–4. — С. 491–502.