ФГБОУ ВПО «Московский государственный университет имени
М. В. Ломоносова»
Механико-математический факультет

На правах рукописи

Родин Александр Алексеевич

О Р-множествах автоматных функций

01.01.09 — дискретная математика и математическая кибернетика

диссертация на соискание ученой степени
кандидата физико-математических наук

Научный руководитель:
доктор физико-математических наук,
профессор В. А. Буевич

МОСКВА – 2013

Содержание

ВВЕДЕНИЕ

Одной из важных проблем, рассматриваемых в дискретной математике и математической кибернетике, является проблема полноты для функциональных систем. Функциональная система (ф.с.) представляет собой множество функций и множество операций над этими функциями. Проблема полноты для ф.с. состоит в описании всех таких подмножеств функций, используя которые с помощью операций ф.с. можно выразить все принадлежащие ф.с функции.

С точки зрения алгебры, ф.с. могут рассматриваться как вариант универсальных алгебр. Существенной особенностью ф.с., выделяющей их из общего класса универсальных алгебр, является содержательная связь ф.с. с реальными кибернетическими моделями управляющих систем и отображение важнейших характеристик таких моделей: функционирования, правил построения более сложных систем из заданных, описания функционирования сложных систем по функционированию их компонент.

Центральное место среди ф.с. принадлежит итеративным ф.с., представляющим собой множество дискретных функций с операциями итерации — суперпозиции, обратной связи, а также их модификаций [21], [28]. В свою очередь, итеративные ф.с. могут быть разделены на два типа: истинностные ф.с. и последовательностные ф.с. В первом случае функции, принадлежащие ф.с., вычисляются без использования, а во втором — с использованием "памяти".

Важнейшим примером истинностных и последовательностных ф.с. являются $k-$значная логика с одной стороны и ф.с. автоматных функций с другой. Для $k-$значных логик (ф.с. P_k) основная проблема в теории итеративных ф.с. — проблема полноты, была решена. В 1921 г. Э. Постом была полностью описана структура замкнутых классов в двузначной логике. Это описание, изложенное в виде монографии в 1941 году [4], по существу эквивалентно решению проблемы полноты для произвольных двузначных логик, в которых в качестве операций выступают операции суперпозиции. Для произвольного $k \geq 3$ усилиями многих авторов (С.В. Яблонский [32], А.В. Кузнецов [24], И. Розенберг [5] и др.) в терминах сохранения отношений (предикатов) были последовательно в явном виде построены все предполные классы в P_k, образующие минимальную критериальную систему для распознавания полноты систем функций $k-$значной логики. Т.е., произвольное множество функций $k-$значной логики M является полным тогда и только тогда, когда M целиком не содержится ни в одном из предполных в P_k классов.

В наиболее общей постановке проблема полноты в классе автоматных отображений — о.-д. функций, изучалась в работах В.Б. Кудрявцева и М.И. Кратко.

Пусть $k \geq 2$ и P^k — множество всех о.-д. функций, переменные которых принимают значения на множестве бесконечных последовательностей, составленных их букв алфавита $E_k = \{0, 1, ..., k-1\}$. На множестве P^k определены две операции — операции суперпозиции и операция обратной связи. В работе [22] были рассмотрены две функциональные системы:

1. Функциональная система "суперпозиция" $(P^k)_\Sigma$;
2. Функциональная система "композиция" $(P^k)_K$.

Множество функций, определяемых в ф.с. $(P^k)_\Sigma$ и $(P^k)_K$, совпадает с множеством P^k. Операциями в ф.с. $(P^k)_K$ являются операции суперпозиции и обратной связи, а в $(P^k)_\Sigma$ — только операции суперпозиции.

При исследовании задачи о полноте в итеративных функциональных системах существуют два подхода — алгебраический и алгоритмический. Алгебраический подход связан с изучением структуры замкнутых классов в исследуемой функциональной системе, в частности, с описанием множества предполных классов, а алгоритмический — с решением вопроса о существовании алгоритма для распознавания полноты конечных систем. Как отмечено выше, в k-значной логике из возможности эффективного описания множества предполных классов следует и существование алгоритма для распознавания полноты конечных систем.

При изучении проблемы полноты в ф.с. $(P^k)_\Sigma$ и $(P^k)_K$ фундаментальный результат был получен В.Б. Кудрявцевым. Известно, что ф.с. $(P^k)_K$ является конечнопорожденной и, также как в $k-$значных логиках, множество всех предполных классов образует минимальную критериальную систему. Отсюда следует, что в принципе критерий полноты в $(P^k)_K$ может быть сформулирован в терминах предполных классов. Однако, в 1963 году В.Б. Кудрявцев показал [20], что мощность множества предполных классов в $(P^k)_\Sigma$ и $(P^k)_K$ равна континууму, и, следовательно, алгоритмический подход не дает эффективного критерия полноты. С этим согласуется результат М.И. Кратко, установившего [18] в 1964 году отсутствие алгоритма распознавания полноты конечных систем о.-д. функций.

Таким образом, возникает вопрос: всегда ли отсутствие эффективного критерия полноты с алгебраической точки зрения, т.е., например, континуальность минимальной критериальной системы, влечет за собой отсутствие алгоритма для распознавания полноты. В данной работе предпринимается попытка дать ответ на этот вопрос. Показано, в частности, что в ф.с. $(P^k)_\Sigma$, несмотря на наличие континуальных критериальных систем, существуют алгоритмы для распознавания полноты некоторых множеств о.-д. функций.

Негативные, с точки зрения эффективности, результаты по проблеме полноты для о.-д. функций в общем случае привели к тому, что различные авторы рассматривали некоторые модификации этой проблемы.

В реальности никакое вычислительное устройство не может работать бесконечно долго, рано или поздно оно должно остановиться. Поэтому представляет интерес о моделировании поведения автоматной функции на конечном отрезке времени. Отсюда естественным образом возникает понятие τ-полноты [13]. Множество о.-д. функций M является τ-полным, если для любой о.-д. функции f существует такая функция $f^M \in [M]$, что значения функций f и f^M совпадают на всех наборах данных длины τ. В [14] показано, что множество τ-предполных классов конечно, может быть эффективно описано и образует τ-критериальную систему. Таким образом, проблема τ-полноты разрешима для любого натурального τ.

С понятием τ-полноты связано понятие А-полноты. Множество о.-д. функций M

называется A-полным тогда и только тогда, когда оно является τ-полным для любого τ. В [11] установлено, что эта задача, как и задача об обычной полноте, также алгоритмически неразрешима. При этом оказалось, что число A-предполных классов счетно. Однако, при наличии некоторых дополнительных условий задача может стать разрешимой. Например, задача об A-полноте алгоритмически разрешима для систем автоматов, содержащих все булевы функции [14].

Алгоритмически разрешимые случаи распознавания полноты могут возникнуть при ограничении числа рассматриваемых о.-д. функций. А.А. Часовских рассматривал множество линейных автоматов. Автомат называется линейным, если и функции перехода, и функции выхода являются линейными функциям алгебры-логики. Оказалось, что задача о полноте в классе линейных автоматов алгоритмически разрешима, при этом количество предполных классов в рассматриваемой функциональной системе счетно [31].

Другие алгоритмически разрешимые случаи могут встретиться при наложении дополнительных условий на рассматриваемые системы. В 1992 году Д.Н. Бабин показал, что существует алгоритм распознавания полноты конечных систем, содержащих все булевы функции [9]. Отсюда естественным образом возникает задача о распознавании полноты систем, содержащих произвольный класс Поста. Все классы Поста разделяются на две части. Для одних задача о полноте алгоритмически разрешима, для классов из другой части — неразрешима. Установить такую классификацию классов Поста также удалось Д.Н. Бабину [10].

В предлагаемой диссертации вводятся и рассматриваются $P-$множества о.-д. функций (термин предложен В.Б. Кудрявцевым). Известно, что каждая о.-д. функция однозначно определяется своим множеством состояний $Q = \{q_1, \dots, q_m\}$, функцией перехода ϕ и множеством функций $k-$значной логики $F_1, \dots, F_m$, реализующихся в состояниях $\{q_1, \dots, q_m\}$ соответственно [22].

Пусть D — произвольный замкнутый класс в P_k. $P-$множество, порожденное классом D — это множество всех ограниченно-детерминированных функций, в каждом состоянии которых реализуется функция $k-$значной логики, принадлежащая D. Будем обозначать такое $P-$множество через P^k_D. Нетрудно видеть, что P^k_D замкнуто как в $(P^k)_\Sigma$, так и в $(P^k)_K$. К примеру, если взять $k = 2, D_1 = \{0, 1\}$, то в качестве $P-$множества получим все автоматы Мура. Если взять $k = 2, D_2 = \{0, 1, x, \bar{x}\}$, получим множество о.-д. функций, в каждом состоянии которых реализуется функция а.-л., зависящая не более, чем от одной переменной. Заметим, что любой класс Поста имеет конечный базис, поэтому при $k = 2$ любое $P-$множество образует рекурсивное подмножество множества всех о.-д. функций, однако, при $k \geq 3$ это, вообще говоря, не так.

В работе изучаются задачи о полноте некоторых систем о.-д. функций, связанных с $P-$множествами. Кроме того, рассматриваются вопросы о существовании базисов и свойствах полных систем в $P-$множествах.

Основные понятия и определения

Пусть $k \geq 2$, обозначим через P^k множество всех ограниченно-детерминированных функций (автоматных отображений), входные и выходные переменные которых определены на множестве бесконечных последовательностей, составленных из E_k, где $E_k = \{0, ... ,$k-1$\}$.

Будем считать, что на множестве P^k определены операции суперпозиции и обратной связи. В работе будут рассматриваться две функциональные системы — "суперпозиция" и "композиция" (присутствуют операции суперпозиции и обратной связи). Пусть $M \subseteq P^k$. Замыкание множества $M \subset P^k$ относительно операций суперпозиции обозначим через $[M]$, а замыкание относительно суперпозиции и обратной связи — через $[M]_K$. Функциональную систему "суперпозиция" над множеством P^k обозначим через $(P^k)_\Sigma$, а ф.с. "композиция" — через $(P^k)_K$.

Множество $N \subset P^k$ называется предполным классом в $(P^k)_\Sigma$, если $[N] \neq P^k$, но для любой о.-д. функции $f \notin N$, $[N \cup \{f\}] = P^k$. Аналогично определяются предполные классы в $(P^k)_K$.

Пусть $f(x_1, \dots , x_n)$ - о.д. функция из P_k, задаваемая системой канонических уравнений:

$$q(0) = q_0,$$

$$q(t+1) = \varphi(x_1(t), \dots , x_n(t), q(t)),$$

$$y(t) = \psi(x_1(t), \dots , x_n(t), q(t)),$$

где $Q = \{q_0, q_1, \dots , q_p\}$ - множество ее состояний, а q_0 - ее начальное состояние. Функцию $k-$значной логики, реализуемую в состоянии q_i обозначим через F_{q_i}.

Пусть $t \geq 1$, E_k^t- множество слов длины t, составленных из E_k. Пусть $i, j \in \{0, 1, ..., p\}$. Будем считать, что состояние q_i является t-достижимым из состояния q_j, если найдутся такие $a_1, a_2, ..., a_n \in E_k^t$, что $\varphi(a_1, \dots , a_n, q_j) = q_i$. Состояние q_i достижимо из состояния q_j, если q_i t-достижимо из q_j для некоторого t. Будем считать, что состояния q_i и q_j связны друг с другом, если состояние q_i достижимо из q_j и наоборот. При этом необязательно, чтобы $q_i \neq q_j$.

Пусть D — некоторое замкнутое множество функций $k-$значной логики. Тогда множество всех о.-д. функций из P^k, таких, что каждая из функций $F_{q_0}, F_{q_1}, \dots , F_{q_p}$ принадлежит множеству D, обозначим через P_D^k. Это множество называем P-множеством, порожденным классом D. Нетрудно видеть, что P_D^k — замкнутое множество как в $(P^k)_K$, так и в $(P^k)_\Sigma$.

Замечание. *Рассмотрим $P-$множество P_D^k, порожденное незамкнутым множеством $k-$значной логики $D \subset [D]$. Тогда P_D^k также окажется незамкнутым множеством в P^k. Нетрудно видеть, что замыкание множества P_D^k в обоих функциональных системах совпадает с $P_{[D]}^k$. Поэтому, наибольший интерес представляют $P-$множества, порожденные замкнутыми классами $k-$значной логики.*

Введем понятие А-полноты [11]. Пусть τ — произвольное натуральное число. О.-д. функции $g(x_1, \dots , x_n)$ и $h(x_1, \dots , x_n)$ являются τ-эквивалентными, если значения функций f и h совпадают на всех словах длины τ. Множество $M \subseteq P^k$ является τ-полным, если для любой о.-д. функции $f(x_1, \dots , x_n) \in P^k$ существует такая функция

$f^M(x_1, \dots, x_n), f^M \in [M]$, что f и f^M τ-эквивалентны. Множество $M \subseteq P^k$ называется А-полным, если оно τ-полно для любого натурального τ. Также будем говорить, что $f \in A[M]$ (А-замыкание), если для любого натурального τ существует функция $f^M \in [M]$ такая, что f^M τ-эквивалентна f.

Основные результаты

В первой главе решается вопрос о количестве предполных классов, содержащих определенное $P-$множество, и доказывается следующее утверждение.

Теорема 0.1. *Пусть $D \subset P_k$ и $D = [D]$. Тогда множество предполных классов в $(P^k)_K$, содержащих P_D^k, континуально и множество предполных классов в $(P^k)_\Sigma$, содержащих P_D^k, также континуально.*

Вторая глава посвящена вопросам существования алгоритмов распознавания полноты систем, содержащих $P-$множества. В качестве исследуемой функциональной системы выбирается $(P^2)_\Sigma$. Пусть $k = 2, D$ — произвольный замкнутый класс алгебры-логики. Пусть Ω^D — совокупность всех подмножеств M множества P (о.-д. функции), содержащих Р-множество P_D и таких, что $M \setminus P_D$ конечно. Рассматривается задача о существовании алгоритма распознавания полноты систем из Ω^D относительно операций суперпозиции.

Получены следующие результаты.

Теорема 0.2. *Если $D \subset P_2, D = [D]$ и D содержит тождественную функцию а.-л. и одну из констант, то в $(P^2)_\Sigma$ существует алгоритм распознавания полноты систем из Ω^D.*

Доказательство теоремы конструктивно, т.е. алгоритм для каждого D указан в явном виде.

При $D = \{0, 1, x, \bar{x}\}$ этот результат был получен С.В. Алешиным в 1977 году [8].

Для случаев, когда порождающее множество не содержит константную функцию, получить алгоритм распознавания полноты не удалось, поэтому были рассмотрены некоторые дополнительные ограничения на рассматриваемые системы.

Пусть $\Omega^D(f)$ — совокупность всех подмножеств M множества P, содержащих Ω^D и о.-д. функцию f, таких, что множество $M \setminus \Omega^D$ конечно.

Пусть о.-д. функции $G_0(x), G_1(x)$ — нулевая и единичная задержка соответственно. Обозначим $G = \{G_0(x), G_1(x)\}$.

Теорема 0.3. *Пусть множество D содержит тождественную функцию а.-л. Тогда в $(P^2)_\Sigma$ существует алгоритм распознавания полноты систем из $\Omega^D(C)$, где C –– константная о.-д. функция.*

Теорема 0.4. *Пусть множество D содержит тождественную функцию а.-л. Тогда в $(P^2)_\Sigma$ существует алгоритм распознавания полноты систем из $\Omega^D(g)$, где g принадлежит множеству G.*

На следующем рисунке изображена решетка замкнутых классов Поста, содержащих тождественную функцию а.-л. Жирными точками отмечены те классы Поста, для которых алгоритм был построен без каких-либо ограничений.

Случай, когда порождающее множество не содержит тождественную функцию а.-л., рассматривается отдельно.

Если $D = \{0\}$ или $D = \{1\}$, то не существует полных в $(P^2)_\Sigma$ систем из Ω^D, следовательно об алгоритме распознавания полноты говорить бессмысленно.

Пусть $D = \{0, 1\}$. Тогда полные системы в Ω^D существуют, но вместе с тем справедлива следующая теорема.

Теорема 0.5. *Пусть множество $D = \{0, 1\}$. Тогда в $(P^2)_\Sigma$ не существует эффективного критерия распознавания полноты систем из Ω^D.*

Наконец, в третьей главе $P-$множества рассматриваются как самостоятельные функциональные системы. В качестве операций используются операции суперпозиции. Доказываются следующие утверждения.

Теорема 0.6. *Пусть $0, 1 \in D$. Тогда в $(P_D^2)_\Sigma$ существует полная система, не содержащая базиса.*

Теорема 0.7. *Пусть $0, 1 \in D$. Тогда в $(P_D^2)_\Sigma$ существует базис.*

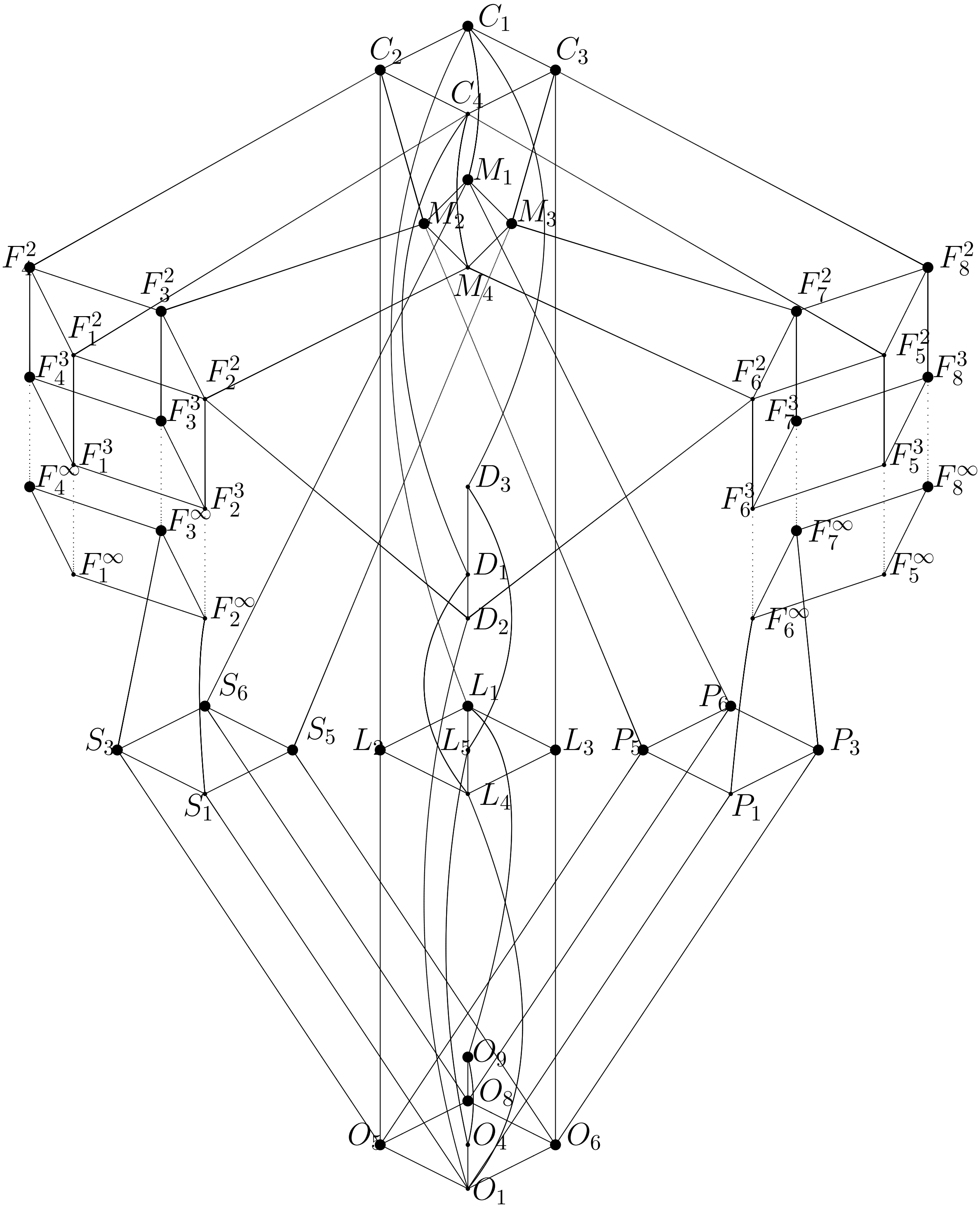

Рис. 1. Разрешимые случаи на решетке Поста

Теорема 0.8. *Пусть порождающее множество D содержит тождественную функцию а.-л. и отрицание. Тогда в $(P_D^2)_\Sigma$ существует полная система, не содержащая базиса.*

Теорема 0.9. *Пусть порождающее множество D содержит тождественную функцию а.-л. и отрицание. Тогда в $(P_D^2)_\Sigma$ существует базис.*

Автор выражает благодарность профессору В. А. Буевичу за постановку задачи, поддержку и руководство данной работой и академику, профессору В. Б. Кудрявцеву за внимание к ней.

Глава 1

О континуальности числа предполных классов, содержащих $P-$множество

Целью данной главы является доказательство следующего утверждения.

Теорема 1.1. *Пусть $D \subset P_k$ и $D = [D]$. Тогда множество предполных классов в $(P^k)_K$, содержащих P_D^k, континуально и множество предполных классов в $(P^k)_\Sigma$, содержащих P_D^k, также континуально.*

1.1. Доказательство теоремы 1.1

Сначала приведем доказательство для функциональной системы $(P^k)_K$. Как известно, в этом случае существует универсальная о.-д. функция с двумя входами $u(x_1, x_2)$, через которою выражаются все остальные о.-д. функции [12]. Не ограничивая общности, будем считать, что D содержит тождественную функцию $x(x_1) = x_1$.

Пусть

$$p_1, p_2, ...$$

— последовательность всех простых чисел, больших трех, упорядоченная по возрастанию.

Пусть

$$L = (m_1, m_2, ...) \tag{1.1}$$

— последовательность чисел таких, что $m_i \in \{0, 1\}$ для любого $i \geq 1$.

Пусть о.-д. функция $h_{p_i}^{m_i}(x_1, x_2) = y$, такая что $y(t) = x_1(t)$, если $t = lp_i + m_i + 1$ для некоторого $l \geq 0$ и $y(t) = x_2(t)$ в противном случае. В качестве примера, на рис. 1.1 изображены диаграммы Мура функций h_5^0 и h_5^1, звездочками отмечены начальные состояния.

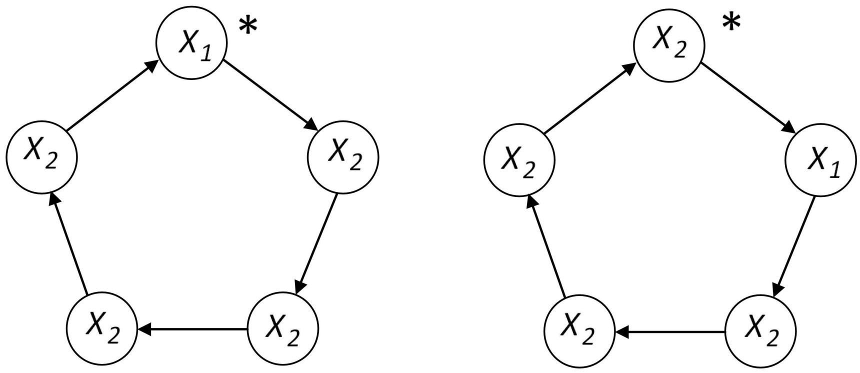

Рис. 1.1. О.-д. функции h_5^0 (слева) и h_5^1 (справа).

Пусть

$$g_{p_i}^{m_i}(x_1, x_2) = h_{p_i}^{m_i}(x_1, u(x_1, x_2)),$$

где $u(x_1, x_2)$ — универсальная функция в P^k. Из построения функции $g_{p_i}^{m_i}$ ясно, что при $t = lp_i + m_i + 1$ выход функции равен $x_1(t)$ и совпадает с выходом функции $u(x_1, x_2)$ в противном случае. Исходя из последовательности L, определим множество о.-д. функций

$$M_L = P_D^k \bigcup_{i \geq 1} \{g_{p_i}^{m_i}(x_1, x_2)\}.$$

Покажем, что для любой последовательности L вида (1.1) замыкание множества M_L не совпадает с P^k. Пусть

$$N = \{g_{p_{i_1}}^{m_{i_1}}(x_1, x_2) = y_1, \dots , g_{p_{i_s}}^{m_{i_s}}(x_1, x_2) = y_s\}$$

— произвольное конечное подмножество множества $M_L \setminus P_D^k$.

Покажем, что существует $t \geq 1$ такое, что $y_j(t + 1) = x_1(t + 1)$ для любого

$j \in \{1, \dots , s\}$. Возможны два случая. Пусть $m_{i_1} = ... = m_{i_s} = m$. Тогда

$$t = (p_{i_1}...p_{i_s}) + m.$$

Пусть теперь существует $j \in \{1, \dots , s\}$ такое, что $m_{i_1} \neq m_{i_j}$. Будем считать, что для некоторого $d, 1 \leq d \leq s - 1$,

$$m_{i_1} = ... = m_{i_d} = 0, \qquad m_{i_{d+1}} = ... = m_{i_s} = 1.$$

Тогда

$$t = (p_{i_1}...p_{i_d})^{(p_{i_{d+1}}-1)...(p_{i_{d+1}}-1)}.$$

Из малой теоремы Ферма следует, что по модулю любого из чисел $p_{i_{d+1}}, ..., p_{i_s}$ число t совпадает с единицей, и делится на любое из $p_{i_1}, ..., p_{i_d}$. Заметим, что существование такого момента t также следует из китайской теоремы об остатках.

Таким образом, из начального состояния любой о.-д. функции, принадлежащей $N \cup P^k_D$, t-достижимы лишь такие состояния, в которых реализуются функции $k-$значной логики, принадлежащие D. Это означает, что в момент t все функции из множества N будут находится в состояниях, в которых реализуется функции из D. Нетрудно видеть, что это свойство будет сохраняться при операциях суперпозиции над этим множеством, поскольку в момент t в суперпозиции будут участвовать только функции $k-$значной логики, принадлежащие состояниям t-достижимым из начального, т.е. функции из D. Операция обратной связи также сохраняет это свойство, поскольку обратная связь не может быть применена ко входу, от которого существенно зависит функция, реализуемая в каком-либо состоянии. Поэтому функции $k-$значной логики, реализуемые во всех состояниях, t-достижимых из начального, при обратной связи останутся неизменными, т.е. они будут принадлежать множеству D.

Следовательно, у любой композиции над множеством N t-достижимы лишь такие состояния, в которых реализуются функции $k-$значной логики, принадлежащие D. А поскольку в каждой композиции участвует лишь конечное число о.-д. функций, то в замыкании не может оказаться о.-д. функции, в каждом состоянии которой реализуется $k-$значная функция, не принадлежащая D. Отсюда следует, что $[M_L]_K \neq P^k$.

Рассмотрим объединение множеств M_L и $M_{L'}$ для любых отличных друг от друга двоичных последовательностей L и L'. Эти последовательности различны, пусть они различаются в i-м разряде. Это значит, что множеству $M_L \cup M_{L'}$ принадлежат функции $g^0_{p_i}(x_1, x_2)$ и $g^1_{p_i}(x_1, x_2)$. Нетрудно видеть, что с их помощью можно получить универсальную о.-д. функцию:

$$h^0_{p_i}(g^0_{p_i}(x_1, x_2), g^1_{p_i}(x_1, x_2)) = u(x_1, x_2).$$

Функция $h^0_{p_i}(x_1, x_2)$ принадлежит P^k_D (а значит, принадлежит и M_L, и $M_{L'}$), поскольку в состояниях $h^0_{p_i}(x_1, x_2)$ реализуются только селекторы $k-$значной логики, и они принадлежат порождающему множеству D. Итак, с помощью функций из объединения множеств M_L и $M_{L'}$ можно получить универсальную о.-д. функцию, поэтому $[M_L \cup M_{L'}]_K = P^k$.

Как было отмечено выше, в функциональной системе $(P^k)_K$ существует конечная полная система (например, о.-д. функция $u(x_1, x_2)$). Поэтому любой замкнутый класс в $(P^k)_K$ расширяется до предполного стандартным образом. Пусть $\widetilde{M}_L$ и $\widetilde{M}_{L'}$ — предполные классы, содержащие M_L и $M_{L'}$ соответственно. Как было показано ранее, для любых отличных друг от друга последовательностей L и L', $[M_L \cup M_{L'}]_K = P^k$. Поэтому M_L и $M_{L'}$ не могут одновременно содержаться в одном и том же предполном классе, т.е. $\widetilde{M}_L \neq \widetilde{M}_{L'}$. Следовательно, предполных классов должно быть не меньше, чем таких последовательностей. Известно, что существует континуум последовательностей вида (1.1). Таким образом, мощность множества предполных классов, содержащих P^k_D не менее, чем континуум. Вместе с тем, мощность всевозможных подмножеств множества P^k также равна континууму. Теорема доказана.

Замечание 1. *При доказательстве теоремы мы предположили, что множество* $k-$*значной логики* D *содержит тождественную функцию* $x(x_1) = x_1$. *Пусть это не так. Тогда рассмотрим* $D' = [D \cup x]$. *Понятно, что* D' *- замкнуто, и* $D' \neq P^k$, *т.к.* $D \neq P^k$. *Далее очевидно, что* $P_D^k \subset P_{D'}^k$. *Поэтому, если докажем, что существует континуум предполных классов, содержащих* $P_{D'}^k$, *то* P_D^k *тоже будет содержаться в тех же самых классах. Следовательно, для множества* D *теорема тоже будет верна. Итак, без ограничения общности, можно считать, что* $x \in D$.

Замечание 2. *Если же будем рассматривать функциональную систему* $(P^k)_\Sigma$, *ситуация будет несколько иная. Дело в том, что в этой системе нет универсальной функции, да и нет конечной полной системы вообще. Тем не менее теорема 1.1 справедлива и для этого случая. Приведенное выше доказательство теоремы останется без изменений, только вместо универсальной о.-д. функции* $u(x_1, x_2)$ *следует взять о.-д. функцию от двух переменных* $u'(x_1, x_2)$ *с одним состоянием, в котором реализуется какая-нибудь функция Вебба. Тогда* $[P_{D'}^k \cup u'(x_1, x_2)] = P^k$. *И, следовательно, любое множество, содержащее* $P-$*множество* P_D^k *можно расширить до предполного класса стандартным образом.*

Глава 2

Алгоритмы распознавания полноты систем, содержащих $P-$множества

В этой главе речь идет о задаче распознавания полноты некоторых систем автоматных функций, связанных с $P-$множествами. В ней рассматривается случай $k = 2$. Другими словами, рассматриваются такие о.-д. функции, входные и выходные переменные которых принимают значения из множества бесконечных последовательностей, составленных из нулей и единиц. Это объясняется тем, что любой класс из структуры замкнутых классов Поста имеет конечный базис [34] и, как легко видеть, при $k = 2$ всякое $P-$множество образует рекурсивное подмножество множества всех о.-д. функций.

В качестве функциональной системы выбирается $(P^2)_\Sigma$.

Пусть D - произвольный замкнутый класс алгебры-логики. Пусть Ω^D - совокупность всех подмножеств M множества P^2 (о.-д. функции), содержащих $P-$множество P^2_D и таких, что множество $M \setminus P^2_D$ конечно.

Для каждого D рассматривается задача о существовании алгоритма распознавания полноты множеств, принадлежащих совокупности Ω^D. Любая система M из Ω^D содержит P^2_D и конечное множество о.-д. функций, не принадлежащих P^2_D. По этой конечной добавке искомый алгоритм должен определить, полна система M или нет. Ясно, что наличие алгоритма должно зависеть от порождающего множества D. Например, для порождающего множества $\{0, 1, x, \bar{x}\}$ алгоритм существует [8]. Если в качестве порождающего рассмотреть множество, состоящее только из констант 0 и 1, полученное $P-$множество, будет являться множеством автоматов Мура. Как показано в этой главе, в данном случае алгоритма распознавания полноты не существует. Если же порождающее множество состоит только из одной константы (например, 0), то $P-$множество также будет состоять только из тождественного нуля. Поэтому любая система из $\Omega^{\{0\}}$ будет конечной и, следовательно, неполной относительно операции суперпозиции.

Таким образом, решетка Поста разбивается на две части - для классов Поста из одной части алгоритм существует, а из другой не существует, причем это разбиение нетривиально, т.е. обе части непусты. Оказывается, что если D, E — замкнутые множества функций алгебры-логики, такие что $D \subset E$, D содержит тождественную функцию а.-л. и для D существует алгоритм, то алгоритм существует и для E. Поэтому, если рассматривать решетку классов Поста, содержащих тождественную функцию а.-л., на ней должна существовать граница такая, что для классов Поста, расположенных выше границы существует алгоритм, а для классов, расположенных ниже или на границе алгоритма нет. В этом смысле главным случаем является тот, когда порождающее множество состоит только из тождественной функции, поскольку, если алгоритм существует здесь, то он существует и для остальных классов, содержащих тождественную функцию. Классы Поста, не содержащие тождественную функцию, рассматриваются отдельно.

В данной главе рассмотрены несколько возможных вариантов. Оказалось, что если порождающее множество содержит тождественную функцию и одну из констант, то алгоритм существует. Доказательство существования алгоритма конструктивно. Если порождающее множество не содержит тождественную функцию, алгоритма нет. В случае, когда порождающее множество состоит только из тождественной функции, алгоритм также был получен, но с некоторыми дополнительными условиями.

2.1. Принятые обозначения

Введем ряд понятий и обозначений.

Пусть $f(x_1, \ldots, x_n)$ - о.д. функция, задаваемая системой канонических уравнений:

$$q^f(0) = q_0^f,$$

$$q^f(t+1) = \varphi^f(x_1(t), \dots, x_n(t), q^f(t)),$$

$$y^f(t) = \psi^f(x_1(t), \dots, x_n(t), q^f(t)),$$

где $Q^f = \{q_0^f, q_1^f, \dots, q_p^f\}$ — множество ее состояний, а q_0^f - ее начальное состояние. В случае, когда ясно, о какой функции идет речь, верхний индекс, указывающий на функцию, к которой относится состояние, будем опускать. Функцию алгебры-логики, реализуемую в состоянии q_i обозначим через F_{q_i}.

Пусть D - некоторое замкнутое множество функций алгебры-логики и $f \in P_D^2$. Очевидно, что тогда

$$\{F_{q_0}, F_{q_1}, \dots, F_{q_i}\} \subseteq D.$$

Если F_{q_i} является функцией алгебры-логики, существенно зависящей не менее чем от двух переменных, состояние q_i будем называть существенным, иначе - несущественным.

Если F_{q_i} является линейной функцией алгебры-логики, состояние q_i будем называть линейным, иначе - нелинейным.

Если F_{q_i} является монотонной функцией алгебры-логики, состояние q_i будем называть монотонным, иначе - немонотонным.

Будем считать, что состояния q_i и q_j связны друг с другом, если состояние q_i достижимо из q_j и наоборот. При этом необязательно, чтобы $q_i \neq q_j$.

Подмножество $K \subset Q$ будем называть компонентой связности, если:

1) Для любых $q_i, q_j \in K$, q_i и q_j связны друг с другом.

2) Если $q_i \in K$ и существует состояние $q_j \in Q$, такое что q_i и q_j связны, то $q_j \in K$.

Из определения следует, что компоненты связности не могут пересекаться. Понятно, что задача об отыскании компонент связности может быть решена за конечное число операций. Заметим, что могут существовать состояния, не входящие ни в одну компоненту связности.

В качестве иллюстрации рассмотрим о.-д. функцию $a(x_1, x_2)$, диаграмма Мура которой изображена на рис. 2.1. У нее есть две компоненты связности. Одну из них образуют состояния q_2, q_3, q_4, а вторая состоит только из одного состояния q_5. Состояния q_0 и q_1 не принадлежат ни одной компоненте связанности.

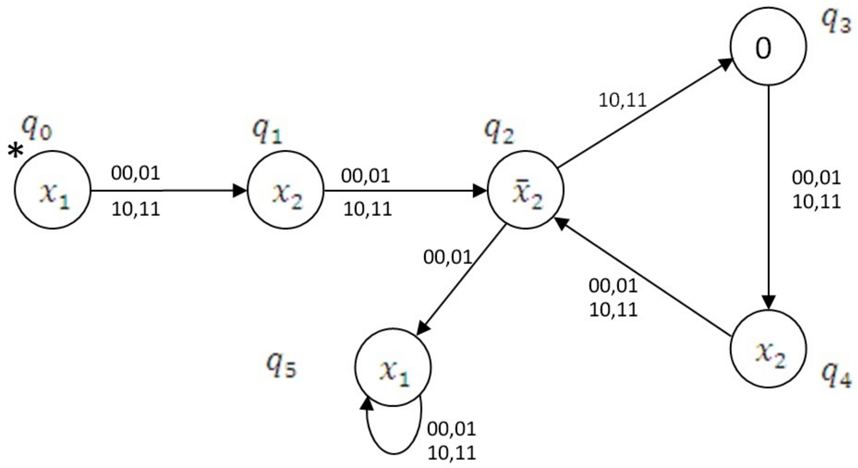

Рис. 2.1. О.-д. функция $a(x_1, x_2)$.

Рассмотрим произвольное состояние q функции f, принадлежащее какой-либо компоненте связности K. Для этого состояния определим множество $A(q) \in (E_2^1)^n$, где n - число переменных, от которых зависит функция f:

$$(\alpha_1, \dots, \alpha_n) \in A(q) \Leftrightarrow \phi(\alpha_1, \dots, \alpha_n, q) \in K$$

Т.е. $A(q)$ - это множество переходов, по которым из состояния q нельзя покинуть компоненту связности, в которой оно находится. Например, для состояния q_2 функции $a(x_1, x_2)$, множество переходов $A(q_2) = \{(10), (11)\}$.

Пусть

$$g_1(y_1, \dots, y_m), \dots, g_n(y_1, \dots, y_m)$$

— функции а.-л. Через $S(g_1, \dots, g_n)$ будем обозначать множество двоичных наборов, равное

$$\bigcup\{(g_1(\beta_1, \dots, \beta_m), \dots, g_n(\beta_1, \dots, \beta_m))\} \subseteq (E_2^1)^n,$$

где объединение берется по всем $(\beta_1, \dots, \beta_m)$ из $(E_2^1)^m$.

Состояние q будем называть локально нелинейным, если найдутся линейные функции а.-л.

$$g_1(y_1, \dots, y_m), \dots, g_n(y_1, \dots, y_m),$$

такие что $S(g_1, \dots, g_n) \subseteq A(q)$ и $F_q(g_1(y_1, \dots, y_m), \dots, g_n(y_1, \dots, y_m))$ является нелинейной функцией а.-л. Это означает, что на вход состояния q можно подать такие линейные функции а.-л., что оно останется нелинейным, но из него нельзя будет покинуть компоненту связности. Все остальные состояния назовем локально линейными. Заметим, что если состояние не принадлежит никакой компоненте связности, то оно локально линейно.

Состояние q будем называть локально существенным, если найдутся функции а.-л., существенно зависящие не более, чем от одной переменной,

$$g_1(y_1, \dots, y_m), \dots, g_n(y_1, \dots, y_m),$$

такие что $S(g_1, \dots, g_n) \subseteq A(q)$ и $F_q(g_1(y_1, \dots, y_m), \dots, g_n(y_1, \dots, y_m))$ является функцией а.-л., существенно зависящей не менее, чем от двух переменных.

Заметим, что локально нелинейное состояние не всегда является локально существенным, поскольку свойство локальной нелинейности проверяется на наборах произвольных линейных функций, а свойство локальной существенности - только на наборах функций, зависящих не более чем от одной переменной. Ниже приведен пример такой ситуации.

Будем говорить, что состояние q локально немонотонно, если найдутся монотонные функции а.-л.

$$g_1(y_1, \dots, y_m), \dots, g_n(y_1, \dots, y_m),$$

такие что $S(g_1, \dots , g_n) \subseteq A(q)$ и $F_q(g_1(y_1, \dots , y_m), \dots , g_n(y_1, \dots , y_m))$ является немонотонной функцией а.-л.

На рис. 2.2 приведена диаграмма Мура о.-д. функции $b(x, y, z)$, начальное состояние q_0. Она имеет две компоненты связности — $K_1 = \{q_0, q_1, q_2, q_3\}, K_2 = \{q_4\}$. Состояния q_0 и q_1 являются локально немонотонными, а q_3 не является, поскольку на наборах, по которым из q_3 нельзя покинуть компоненту связности K_1, свойство немонотонности не проявляется. Заметим, что состояние q_2 является локально нелинейным, поскольку в качестве переменной z можно подставить линейную функцию $x+y$, при этом из состояния q_2 нельзя будет покинуть компоненту связности, и в нем будет реализовываться функция а.-л. xy. В то же время, состояние q_2 не является локально существенным, так как для того, чтобы это состояние осталось существенным, из из него нельзя было бы покинуть компоненту, в качестве z потребуется взять функцию $x + y$, но эта функция зависит от двух переменных.

Обозначим через $Q(t)$ подмножество Q, состоящее из всех состояний, t-достижимых из начального. Рассмотрим последовательность множеств:

$$Q(0), Q(1), Q(2)...$$

Поскольку количество всевозможных подмножеств Q конечно, найдутся два таких различных натуральных числа i, j, что $Q(i) = Q(j)$. Ясно, что тогда $Q(i + 1) = Q(j + 1)$, т.е. начиная с какого-то момента T множества в этой последовательности будут чередоваться по циклу. Пусть s - длина этого цикла. Тогда определим

$$C_i = Q(T + i), i = 1, 2, \dots , s.$$

Длину цикла будем называть рангом функции f и обозначать через $s(f)$ или просто через s, если ясно, о какой функции идет речь.

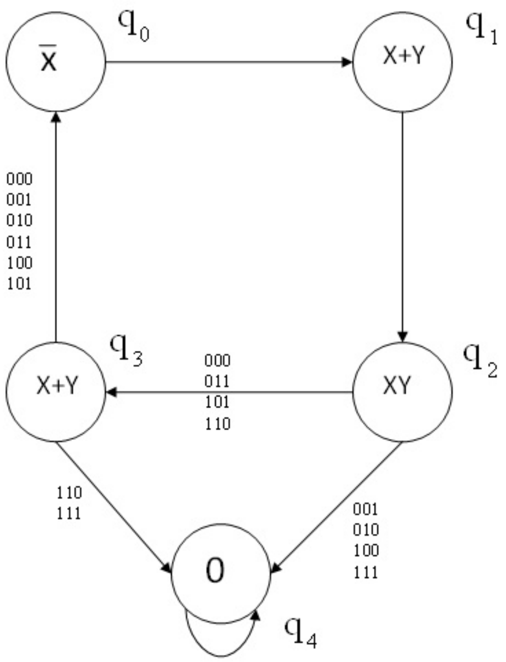

Рис. 2.2. О.-д. функция $b(x, y, z)$.

2.2. Порождающее множество содержит тождественную функцию и обе константы

Сначала рассмотрим случай, когда порождающее множество $D = [\{0, 1, x\}]$. Далее в этом параграфе под D будем понимать именно это множество, если не оговорено обратное. Ясно, что у каждой функции из P^2_D все состояния будут линейными, монотонными и несущественными.

Теорема 2.1. *Пусть $M = P^2_D \bigcup \{f(x_1, \dots, x_n)\}$. Система M полна тогда и только тогда, когда она A-полна и в каждом из множеств $C_i, i = 1, 2, \dots, s$ содержится хотя бы одно локально нелинейное, хотя бы одно локально существенное и хотя бы одно локально немонотонное состояние.*

Эта теорема будет являться критерием полноты в данном случае. Для того, что бы критерий был эффективным (т.е. алгоритмом), необходимо убедиться, что условия теоремы могут быть проверены за конечное число операций. Этому посвящен следующий параграф.

2.2.1. Проверка эффективности условий теоремы 2.1

Лемма 2.1. *Существует эффективный критерий проверки того, является состояние q локально нелинейным или нет.*

Доказательство. По определению, состояние q будет локально нелинейным только в том случае, если найдутся такие линейные функции а.-л.

$$g_1(y_1, \dots, y_m), \dots, g_n(y_1, \dots, y_m),$$

что

$$v(y_1, \dots, y_m) = F_q(g_1(y_1, \dots, y_m), \dots, g_n(y_1, \dots, y_m))$$

— нелинейная функция а.-л. и $S(g_1, \dots, g_n) \subseteq A(q)$. Как известно [33], для всякой нелинейной функции а.-л. можно выбрать некоторые ее переменные и подставить вместо них константы 0 или 1 таким образом, что получится нелинейная функция а.-л., зависящая от двух переменных. Пусть $v(y_1, y_2, c_1, \dots, c_{m-2})$, где $c_i \subseteq \{0, 1\}$ — нелинейная функция а.-л. Следовательно,

$$v(y_1, y_2, c_1, \dots, c_{m-2}) = F_q(g_1(y_1, y_2, c_1, \dots, c_{m-2}), \dots, g_n(y_1, y_2, c_1, \dots, c_{m-2})).$$

При этом ясно, что

$$\bigcup\{g_1(y_1, y_2, c_1, \dots, c_{m-2}), \dots, g_n(y_1, y_2, c_1, \dots, c_{m-2})\} \subseteq S(g_1, \dots, g_n)$$

Таким образом, если условие нелинейности функции $F_q(g_1, \dots, g_n)$ выполнено для некоторых линейных функций $g_1, \dots, g_n$ и $S(g_1, \dots, g_n) \subseteq A(q)$, то найдутся линейные функции а.-л. $g'_1, \dots, g'_n$, зависящие не более чем от двух переменных, для которых эти условия также выполнены. Тогда ясно, что при проверке локальной нелинейности, в качестве функций $g_1, \dots, g_n$ достаточно рассматривать функций а.-л., зависящие в совокупности не более, чем от двух переменных. Понятно, что можно перебрать все наборы $(g_1, \dots, g_n)$ таких функций. Если для какого-то из них условия определения будут выполнены, то состояние будет локально нелинейным, если нет — то не будет. Таким образом, эффективный критерий проверки локальной нелинейности состояния построен. $\square$

Лемма 2.2. *Существует эффективный критерий проверки, является ли состояние локально существенным.*

Доказательство. По определению, состояние q локально существенное только в том случае, если найдутся такие функции а.-л., существенно зависящие не более, чем от одной переменной,

$$g_1(y_1, \dots, y_m), \dots, g_n(y_1, \dots, y_m),$$

что

$$F_q(g_1(y_1, \dots, y_m), \dots, g_n(y_1, \dots, y_m))$$

является функцией а.-л., существенно зависящей не менее, чем от двух переменных. Количество функций а.-л., зависящих не более чем от одной переменной конечное число, поэтому можно перебрать все наборы $(g_1, \ldots, g_n)$ таких функций и проверить выполнение условий определения.

$\square$

Лемма 2.3. *Существует эффективный критерий проверки, является ли состояние локально немонотонным.*

Доказательство. Рассмотрим множество наборов $A(q)$. Здесь возможны два случая.

1)Существуют два набора

$$\widetilde{\alpha} = (\alpha_1, \ldots, \alpha_n), \widetilde{\beta} = (\beta_1, \ldots, \beta_n), \widetilde{\alpha}, \widetilde{\beta} \in A(q)$$

таких, что $\widetilde{\alpha} < \widetilde{\beta}$ и $F_q(\widetilde{\alpha}) > F_q(\widetilde{\beta})$. Покажем, что в этом случае состояние является локально немонотонным. Действительно, $\widetilde{\alpha} < \widetilde{\beta}$, без ограничения общности, можно считать

$$\alpha_1 < \beta_1, \ldots, \alpha_i < \beta_i, \alpha_{i+1} = \beta_{i+1}, \ldots, \alpha_n = \beta_n,$$

где $i \geq 1$. Тогда положим

$$g_1 = x, \ldots, g_i = x, g_{i+1} = \alpha_{i+1}, \ldots, g_m = \alpha_m.$$

Ясно, что $F_q(g_1, \ldots, g_n) = \overline{x}$ — немонотонная функция и

$$S(g_1, \ldots, g_n) = \{\widetilde{\alpha}, \widetilde{\beta}\} \subseteq A(q).$$

Это и означает, что состояние локально немонотонное.

2)Не существует двух наборов $\widetilde{\alpha}, \widetilde{\beta} \in A(q)$, таких что $\widetilde{\alpha} < \widetilde{\beta}$ и $F_q(\widetilde{\alpha}) > F_q(\widetilde{\beta})$.

Рассмотрим любые монотонные функции а.-л. $g_1(y_1, \ldots, y_m), \ldots, g_n(y_1, \ldots, y_m)$, такие что $S(g_1, \dots, g_n) \subseteq A(q)$. Пусть $\tilde{\gamma}, \tilde{\delta} \in E_2^m$ и $\tilde{\gamma} \le \tilde{\delta}$. Тогда

$$g_1(\tilde{\gamma}) \le g_1(\tilde{\delta}), \dots, g_n(\tilde{\gamma}) \le g_n(\tilde{\delta}).$$

В силу условия второго случая получим:

$$F_q(g_1(\tilde{\gamma}), \dots, g_n(\tilde{\gamma})) \le F_q(g_1(\tilde{\delta}), \dots, g_n(\tilde{\delta})).$$

Отсюда следует, что $F_q(g_1, \dots, g_n)$ — монотонная при всех монотонных $g_1, \dots, g_n$, удовлетворяющих условию $S(g_1, \dots, g_n) \in A(q)$. Таким образом, состояние q будет локально монотонным.

$\square$

Существование эффективной процедуры проверки А-полноты системы M следует из следующих двух лемм.

Лемма 2.4. *Система $M = P_D^2 \bigcup \{f(x_1, \dots, x_n)\}$ является А-полной тогда и только тогда, когда в каждом из множеств $Q(0), Q(1), Q(2)\dots$ и т.д., определенных для функции f, содержится хотя бы одно нелинейное и хотя бы одно немонотонное состояние.*

Доказательство. **Необходимость.** Предположим, во множестве $Q(t)$ не содержится ни одного нелинейного состояния. У функций из P_D^2 все состояния являются линейными. Это означает, что в момент времени t у всех функций системы M достижимы лишь линейные состояния. А следовательно, этим свойством будет обладать любая суперпозиция этих функций. Таким образом, в замыкании M не может содержаться функции, которая t-эквивалентна какой-либо о.-д. функции с одним состоянием, в котором реализуется нелинейная функция а.-л. Тогда система M не А-полна. В случае, когда во множестве $Q(t)$ не содержится немонотонного состояния, отсутствие А-полноты системы M доказывается абсолютно аналогично.

Достаточность. Предположим, во множестве $Q(T)$ для любого $T = 0, 1, 2, \dots$ содержится хотя бы одно нелинейное состояние $q_L(T)$ и одно немонотонное состояние

$q_M(T)$. Это значит, что состояние $q_L(T)$ достижимо из начального по набору входных данных длины T или

$$\varphi(\widetilde{\beta_1}, \dots , \widetilde{\beta_m}, q_0) = q_L(T),$$

где $\widetilde{\beta_1^1}, \dots , \widetilde{\beta_m^1} \in E_2^T$. Построим вспомогательные функции $j_1(x_1),\ \dots , j_n(x_n)$:

$q^{j_i}(1) = q_1^{j_i}$

$q^{j_i}(t+1) = q_{t+1}^{j_i}, y^{j_i}(t) = \widetilde{\beta}_i(t)$ при $t \leq T$. Здесь $\widetilde{\beta}_i(t)$ t-ая буква слова $\widetilde{\beta}_i$.

$q^{j_i}(t+1) = q_T^{j_i}, y^{j_i}(t) = x_i(t)$ при $t > T$.

То есть, функция $j_i(x_i)$ за первые T тактов выдает слово $\widetilde{\beta}_i$, а затем пропускает переменную x_i. Очевидно, что $j_i(x_i) \in P_D^2$ для $i = 1,\ \dots , n$.

Рассмотрим функцию

$$g_L(T) = f(j_1(x_1),\ \dots , j_n(x_n)).$$

Ясно, что $g_L(T) \in M$ и в момент T у нее достижимо только одно состояние, в котором реализуется нелинейная функция а.-л. F_L. Аналогичным образом построим функцию $g_M(T) \in M$, у которой в момент T достижимо ровно одно состояние и это состояние немонотонно. Пусть в нем реализуется функция а.-л. F_M. Кроме этого, в P_D^2 содержатся две функции c_0 и c_1 с одним состоянием , в котором реализуется константа — 0 или 1 соответственно. Пусть F - произвольная функция алгебры логики. Поскольку система $\{F_M, F_L, 0, 1\}$ полна в функциональной системе алгебры логики, то

$$F = B(\{F_M, F_L, 0, 1\}),$$

где B - некоторая формула над этой системой.

Рассмотрим о.-д. функцию

$$g_F(T) = B(\{g_M(T), g_L(T), c_0, c_1\})$$

— та же самая формула, только над системой о.-д. функций $(P^2)_\Sigma$. Ясно, что у $g_F(T)$

достижимо лишь одно состояние в момент T и в нем реализуется функция F, причем $g_F(T) \in [M]$.

Выберем любое натуральное τ и покажем, что система M τ-полна. Рассмотрим произвольную функцию $h(x_1, \ldots, x_m) \in P^2$. Пусть $W(i) = (E_2^i)^m$ — множество двоичных наборов из m слов, таких что все слова из одного набора имеют одинаковую длину i. Пусть $R = W(1) \cup \ldots \cup W(T)$. Определим о.-д. функцию $I(x_1, \ldots, x_m, y_0, \{y_\beta\})$, где β пробегает все множество R, имеющую $|R|+1$ состояние и зависящую от $m+|R|+1$ переменных , следующим образом:

$q(0) = q_0$;

$\phi(\widetilde{\alpha_1}, \ldots, \widetilde{\alpha_m}, \widetilde{\beta}_1, \ldots, \widetilde{\beta_{|R|+1}}, q_0) = q_{\widetilde{\alpha_1}, \ldots, \widetilde{\alpha_m}}$ если $(\widetilde{\alpha_1}, \ldots, \widetilde{\alpha_m}) \in R$;

$\phi(\widetilde{\alpha_1}, \ldots, \widetilde{\alpha_m}, \widetilde{\beta}_1, \ldots, \widetilde{\beta_{|R|+1}}, q_0) = q_0$ если $(\widetilde{\alpha_1}, \ldots, \widetilde{\alpha_m}) \notin R$.

Ясно, что таким образом все переходы определены. Пусть в состоянии q_α реализуется селектор y_α для любого $\alpha \in R$, а в состоянии q_0 реализуется y_0. Таким образом, функция I полностью задана. Очевидно, что $I \in M$.

Пусть $\beta \in W(i), i \leq T$. Через $q(\beta)$ обозначим $\phi^h(\beta, q_0^h)$ - состояние функции h, достижимое из начального по набору β. $F_{q(\beta)}(x_1, \ldots, x_m)$ — функция а.-л., реализуемая в этом состоянии. По доказанному выше, для каждого такого β, в замыкании системы M существует о.-д. функция $g_{F_{q(\beta)}}(i)$ такая, что в момент i у нее достижимо только одно состояние, в котором реализуется $F_{q(\beta)}(x_1, \ldots, x_m)$.

Рассмотрим функцию

$$h^M = I(x_1, \ldots, x_m, g_{F_{q_0}}, \{g_{F_{q(\beta)}}(i)\})$$

Понятно, что функции h и h^M τ-эквивалентны, а следовательно, M τ-полна. В силу произвольности выбора τ, утверждение будет выполнено для любого τ, откуда и следует А-полнота системы M.

□

Лемма 2.5. *Пусть* $M = P_D^2 \bigcup \{f(x_1, \ldots, x_n)\}$. *Существует эффективный критерий* *проверки, является ли эта система А-полной.*

Это утверждение следует непосредственно из Леммы 2.4: надо рассмотреть множества

$$Q_0(0), Q_0(1),\ ..., Q_0(T), C_1,\ ..., C_s$$

и проверить наличие в каждом из них локально нелинейного и локально немонотонного состояния. Более подробно вопрос об А-полноте обсуждается в разделе 2.4.1.

2.2.2. Доказательство теоремы 2.1

Пусть $U(h, q^h, s, j) \subseteq Q^h$ подмножество состояний о.-д. функции h, где q^h — некоторое состояние функции h, s — ранг функции h, а $j \in \{1, 2, \dots, s\}$. Будем считать, что $q_i^h \in U(h, q^h, s, j)$ тогда и только тогда, когда q_i^h достижимо из q^h и $q_i^h \in Q^h(T + sl + j)$ для некоторого l. Если среди состояний из множества $U(h, q^h, s, j)$ не окажется существенных состояний, состояние q^h будем называть $j-$несущественным.

Лемма 2.6. *Пусть* $M = P_D^2 \bigcup \{f(x_1, \dots, x_n)\}$ *и во множестве* C_j *для некоторого* $j \in \{1, 2, \dots, s\}$ *не содержится ни одного локально существенного состояния. Тогда для каждой функции* $w(x_1,\ \dots, x_m) \in [M]$ *из любого ее состояния* q^w *достижимо* $j-$*несущественное состояние.*

Доказательство. Заметим, что любое состояние, достижимое из $j-$несущественного состояния также будет $j-$несущественным.

Будем доказывать утверждение леммы индукцией по глубине суперпозиции. В качестве базы индукции выберем о.-д. функции из системы M. Нетрудно видеть, что для них утверждение леммы верно.

Рассмотрим теперь какую-либо суперпозицию

$$H(g_1,\ \dots, g_m) = w(x_1,\ \dots, x_k)$$

над системой M. Пусть для функций

$$g_1(x_1, \dots, x_k), \dots, g_m(x_1, \dots, x_k), h(y_1, \dots, y_m)$$

предположение индукции верно, покажем, что оно верно для $w(x_1, \dots, x_k)$.

Рассмотрим произвольное состояние q^w функции $w(x_1, \dots, x_k)$. Пусть оно достижимо из начального состояния q_0^w по набору $\widetilde{\alpha} = (\widetilde{\alpha_1}, \dots, \widetilde{\alpha_k}) \in (E_2^\tau)^k$.

Рассмотрим состояние $q_1^{g_1} = \varphi^{g_1}(\widetilde{\alpha}, q_0^{g_1})$.

Согласно предположению, существует такое τ_1 и такое $\widetilde{\alpha^1} = (\widetilde{\alpha_1^1}, \dots, \widetilde{\alpha_n^1}) \in (E_2^{\tau_1})^k$, что $\varphi^{g_1}(\widetilde{\alpha^1}, q_1^{g_1})$ — $j-$несущественное.

Рассмотрим набор $\widetilde{\beta^1} = (\widetilde{\beta_1^1}, \dots, \widetilde{\beta_k^1})$, где $\widetilde{\beta_i^1} = \widetilde{\alpha_i \alpha_i^1} \in E_2^{\tau+\tau_1}$ - конкатенация двух слов.

Пусть $q_i^{g_2} = \varphi^{g_2}(\widetilde{\beta_1^1}, \dots, \widetilde{\beta_k^1}, q_0^{g_2})$. По предположению, существует такой набор

$$\widetilde{\alpha^2} = (\widetilde{\alpha_1^2}, \dots, \widetilde{\alpha_n^2}) \in E_2^{\tau_2},$$

что $\varphi^{g_2}(\widetilde{\alpha^2}, q_i^{g_2})$ - $j-$несущественное.

Пусть $\widetilde{\beta^2} = (\widetilde{\beta_1^2}, \dots, \widetilde{\beta_k^2})$, где $\widetilde{\beta_i^2} = \widetilde{\beta_i^1 \alpha_i^2} \in E_2^{\tau+\tau_1+\tau_2}$ - конкатенация двух слов. Ясно, что состояния $\varphi^{g_1}(\widetilde{\beta^2}, q_0^{g_1})$ и $\varphi^{g_2}(\widetilde{\beta^2}, q_0^{g_2})$ являются $j-$несущественные состояниями функций g_1 и g_2 соответственно.

Точно таким же образом построим набор $\widetilde{\beta^m} \in (E_2^{\tau+\tau_1+\dots+\tau_m})^k$ такой, что состояния $\varphi^{g_i}(\widetilde{\beta^m}, q_0^{g_i})$ есть $j-$несущественные состояния соответствующих функций. Это означает, что при подаче набора $\widetilde{\beta^m}$ на вход суперпозиции, в дальнейшем на вход состояния функции h будут подаваться несущественные функции а.-л. в моменты $T + j + sl$. Рассмотрим состояние

$$q^h = \varphi^h(g_1(\widetilde{\beta^m}), \dots, g_m(\widetilde{\beta^m}), q_0^h)$$

в котором оказалась функция h.

Итак, по условию леммы, у функции h в моменты $T + j + sl$ достижимы лишь локально несущественные состояния. Это могут быть состояния трех типов:

1)несущественные состояния, принадлежащие некоторой компоненте связности;

2)существенные состояния, принадлежащие компоненте, которые не являются локально существенными;

3)состояния, лежащие вне компонент связности.

Будем считать, что $\tau + \tau_1 + \dots + \tau_k > T + j$. Несложно видеть, что τ_i можно выбрать сколь угодно большими.

Если состояние q^h является $j-$несущественным состоянием функции h, то ясно, что состояние $\varphi^w(\widetilde{\beta^m}, q^w)$ $j-$несущественно и достижимо из q^w, следовательно, предположение индукции верно.

Пусть

$$S(q^h) = \bigcup\{\varphi^h(g_1(\widetilde{A}), \dots , g_m(\widetilde{A}), q^h)\}$$

- множество состояний функции h, достижимых из q^h по некоторому набору

$$g_1(\widetilde{A}), \dots , g_m(\widetilde{A}),$$

объединение берется по всевозможным $\widetilde{A} \in (E_2^t)^k$. Рассмотрим множество

$$US(q^h) = U(h, q^h, s, j) \cap S(q^h).$$

Если в нем содержатся лишь несущественные состояния функции h, то состояние $\varphi^w(\widetilde{\beta^m}, q^w)$ $j-$несущественное состояние функции w и достижимо из q^w, следовательно, предположение индукции верно.

Пусть это не так. Здесь могут быть два случая.

1)Пусть в $US(q^h)$ нет состояний третьего типа, но оказалось состояние второго типа q_i^h, в котором реализуется функция а.-л.

$$F_{q_i^h}(F_{q^{g_1}}, \dots , F_{q^{g_m}}),$$

существенно зависящая не менее, чем от двух переменных, и достижимое из q^h по некоторому набору

$$(g_1(\widetilde{A}), \dots , g_m(\widetilde{A}))$$

По доказанному выше, функции а.-л.

$$F_{q^{g_1}}, \dots , F_{q^{g_m}},$$

будут существенно зависеть не более, чем от одной переменной. Тогда существует такие

$$a_1, \ \dots , a_k \in E_2,$$

что

$$F_{q^{g_1}}(a_1, \ \dots , a_k), \ \dots , F_{q^{g_m}}(a_1, \ \dots , a_k) \notin A(q_i^h),$$

поскольку состояние q_i^h не является локально существенным. Это означает, что при подаче на вход функции w, находящейся в этом состоянии, набора $a = (a_1, \ \dots , a_k)$, функция h покидает компоненту, в которой содержится q_i^h. Обратно в эту компоненту функция h не может вернутся, что следует из определения компоненты. Рассмотрим набор

$$\widetilde{\gamma}_1 = \widetilde{A}a = (A_1a_1, \dots , A_ka_k).$$

Ясно, что

$$q_i^h \notin U(h, \phi^h(g_1(\widetilde{\gamma}_1), \dots , g_m(\widetilde{\gamma}_1)), q^h), s, j),$$

т.к. функция h при таких начальных значениях входных данных уже побывала в компоненте, где лежит q_i^h, вышла из нее и обратно вернутся уже не может. Если в $US(\phi^h(g_1(\widetilde{\gamma}_1), \dots , g_m(\widetilde{\gamma}_1)), q^h))$ содержится еще какое-либо существенное состояние функции h, действуем таким же образом. Состояний второго типа конечное число, поэтому рано или поздно получим такой набор B, что $US(\phi^h(g_1(\widetilde{B}), \dots , g_m(\widetilde{B})), q^h)$ не содержит ни одного существенного состояния функции h. Это означает, что состояние $US(\phi^w(g_1(\widetilde{B}), \dots, g_m(\widetilde{B})), q^w)$ функции w $j-$несущественно и достижимо из q^w, откуда следует справедливость предположения индукции.

2)Пусть во множестве $US(q^h)$ есть хотя бы одно состояние третьего типа q_i^h. Рассмотрим набор $\widetilde{\gamma'} = \widetilde{A}a$, где $\widetilde{A}$ - такой набор входных данных, по которому из состояния q^h можно перейти в q_i^hи a-произвольный набор входных данных длины 1. Ясно, что

$$q_i^h \notin U(h, \phi^h(g_1(\widetilde{\gamma'}), \dots, g_m(\widetilde{\gamma'})), s, j),$$

т.к. иначе состояние q_i^h принадлежало бы какой-либо компоненте связности. Понятно, что аналогично можно построить набор B', такой что в

$$U(h, \phi^h(g_1(\widetilde{B'}), \dots, g_m(\widetilde{B'}))s, j)$$

не содержится ни одного состояния третьего типа. Таким образом, этот случай сводится к случаю 1. $\square$

Непосредственно из леммы 2.6 следует, что система не полна, если в каком-то из множеств $C_i, i = 1, 2, \dots, s$ не содержится ни одного локально существенного состояния. Например, для сумматора по модулю два утверждение леммы 2.6 не выполнено и, следовательно, он не может содержаться в замыкании M.

Лемма 2.7. *Пусть* $M = P_D^2 \bigcup \{f(x_1, \dots, x_n)\}$. *Если в каком-то из множеств* $C_i, i = 1, 2, \dots, s$ *не содержится ни одного локально нелинейного состояния, то система* M *не полна.*

Лемма 2.8. *Пусть* $M = P_D^2 \bigcup \{f(x_1, \dots, x_n)\}$. *Если в каком-то из множеств* $C_i, i = 1, 2, \dots, s$ *не содержится ни одного локально немонотонного состояния, то система* M *не полна.*

Доказательство этих двух лемм полностью аналогично доказательству леммы 2.6.

Таким образом, необходимость условий теоремы 2.1 доказана. Перейдем к доказательству достаточности.

Лемма 2.9. *Пусть* $M = P_D^2 \bigcup \{f(x_1, \dots, x_n)\}$. *Если в каждом из множеств* C_i *содержится хотя бы одно локально немонотонное состояние и система A-полна, то в замыкании системы содержится о.-д. функция отрицания.*

Доказательство. Итак, множество C_i содержит локально немонотонное состояние q. Это означает, что состояние q достижимо из начального за время $T + i + sN$ для любого целого $N \geq 0$. Поскольку q — локально немонотонное состояние, то существуют монотонные функции а.-л.

$$g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m),$$

такие, что функция

$$F_q(g_1(\dots), \dots, g_n(\dots))$$

немонотонна, причем $S(g_1, \dots, g_n) \in A(q)$. Это означает, что для любого набора $a \in (E_2^1)^m$ существует набор из n слов

$$(e_1(a), \dots, e_n(a)) \in (E_2^{d(a)})^n,$$

таких что

$$\phi(g_1(a)e_1(a), \dots, g_n(a)e_n(a), q) = q.$$

Пусть $K = \text{НОК}(d(a) + 1, s)$, НОК берется по всем $d(a)$. Пусть

$$g_i(x_1, \dots, x_m) \in \{0, 1, x\}, i = 1, 2, , \dots, n,$$

в лемме 2.3 показано, что функции g_i можно выбрать таким образом.

Пусть $a_1, \dots, a_n \in E_2^{T+i}$ таковы, что $q = \phi(a_1, \dots, a_n, q_0)$. Построим вспомогательные о.-д. функции

$$h_1(y_1, \dots, y_m), \dots, h_n(y_1, \dots, y_m)$$

следующим образом. Для функции h_j:

$q(0) = q_0$;

$\phi(*, q_t) = q_{t+1}$, $\psi(*, q_t) = a_j(t+1)$ для всех $t < T+i$, здесь * - любой набор входных данных длины 1, т.е. переходы безусловны;

$\phi(a, q_{T+i}) = q_{a,1}$, $\psi(a, q_{T+i}) = g_j(a)$;

$\phi(*, q_{a,l}) = q_{a,l+1}$, $\psi(*, q_{a,l}) = e_j(a)(l)$ для $1 \leq l < K-1, l \neq 0(mod(d(a)+1))$, здесь $e_j(a)(l)$ - буква слова $e_j(a)$, имеющая порядковый номер, равный остатку числа l по модулю $d(a)+1$;

$\phi(*, q_{a,l}) = q_{a,l+1}$, $\psi(*, q_{a,l}) = g_j(a)$ для $1 \leq l < K-1, l = 0(mod(d(a)+1))$,

$\phi(*, q_{a,l}) = q_{T+i}$, $\psi(*, q_{a,l}) = e_j(a)(l)$ для $l = K-1$.

Полученная функция имеет только одно состояние, в котором реализуется функция а.-л., отличная от константы - состояние q_{T+i}, в котором реализуется функция из множества $\{0, 1, x\}$. Очевидно, функции $h_j \in P_D^2, j = 1, 2, \ldots, n$, и если подать их на вход функции f вместо переменных x_j соответственно, получим функцию f_1, у которой в моменты $T+i+KN$ достижимо только одно состояние(одинаковое для всех моментов), в котором реализуется отрицание. Аналогичным образом можно построить функцию f_2, которая находится в немонотонном состоянии в моменты $T+i+s+KN$ и т.д. Используя функции из P_D^2, можно получить такую функцию F^i, у которой реализуется отрицание в моменты $T+i+sN$. Но это можно сделать для любого i, т.к. в каждом из множеств D_i содержится локально немонотонное состояние. А тогда можно получить такую функцию, у которой реализуется отрицание в любой момент времени, начиная с T. Учитывая А-полноту, о.-д. функцию отрицания. $\square$

Лемма 2.10. *Пусть $M = P_D^2 \bigcup \{f(x_1, \ldots, x_n)\}$. Если в каждом из множеств C_i содержится хотя бы одно локально существенное состояние, система А-полна и в замыкании M содержится о.-д. функция отрицания, то в замыкании системы содержится сумматор по модулю два.*

Доказательство. Аналогично предыдущей лемме построим функции

$$h_1(y_1, \dots , y_m), \dots , h_n(y_1, \dots , y_m)$$

в каждом состоянии которых реализуется функция а.-л., существенно зависящая не более чем от одной переменной. Ясно, что они принадлежат замыканию объединения M и истинностного отрицания. Далее, аналогично лемме 2.9, построим функцию, в каждом состоянии которой реализуется функция, существенно зависящая не менее чем от двух переменных, начиная с момента T. Учитывая А-полноту, получим сумматор по модулю два. □

Лемма 2.11. *Пусть* $M = P_D^2 \bigcup \{f(x_1, \dots , x_n)\}$. *Если в каждом из множеств* C_i *содержится хотя бы одно локально нелинейное состояние, система А-полна и в замыкании* M *содержится сумматор по модулю два, то система полна.*

Доказательство. Аналогично предыдущим двум леммам, получим какую-либо истинностную функцию, в состоянии которой реализуется некоторая нелинейная функция а.-л. Используя сумматор по модулю два, тождественный 0 и тождественную 1, несложно получить о.-д. функцию, в каждом состоянии которой реализуется штрих Шеффера. Тогда, как нетрудно видеть, система M полна. □

Таким образом, теорема 2.1 полностью доказана.

2.2.3. Следствия из теоремы 2.1

В теореме 2.1 рассмотрен случай, когда порождающее множество состоит только из нуля, единицы и тождественной функции а.-л., а система M содержит только одну о.-д. функцию, не принадлежащую $P-$множеству P_D. В этом разделе рассматривается случай, когда в качестве порождающего выбирается произвольное множество функций а.-л., содержащее $\{0,1,x\}$ и

$$M = P_D^2 \bigcup \{f_1(x_1, \dots, x_n)\ , \dots,\ f_m(x_1, \dots, x_n)\}.$$

Пусть

$$Q^M(T) = Q^{f_1}(T) \cup\ \dots\ \cup Q^{f_m}(T).$$

Рассмотрим последовательность множеств

$$Q^M(0), Q^M(1), Q^M(2)...$$

Эта последовательность множеств также периодична. Пусть s^M— длина периода этой последовательности, T^M — длина предпериода. Тогда определим

$$C_i^M = Q^M(T+i), i = 1, 2, \dots, s^M.$$

Теорема 2.2. *Пусть D =\{0,1,x\}, $M = P_D^2 \bigcup \{f_1(x_1, \dots, x_n)\ , \dots,\ f_m(x_1, \dots, x_n)\}$. Система M полна тогда и только тогда, когда она A-полна и в каждом из множеств $C_i^M, i = 1, 2, \dots, s$ содержится хотя бы одно локально нелинейное, хотя бы одно локально существенное и хотя бы одно локально немонотонное состояние.*

Доказательство теоремы 2.1 легко переносится на этот случай, нужно показать справедливость аналогичных одиннадцати лемм, которые формулируются и доказываются точно таким же образом.

Перейдем теперь к основному случаю данного раздела. Пусть D — произвольный замкнутый класс а.-л., содержащий множество $\{0,1,x\}$ и

$$M = P_D^2 \bigcup \{f_1(x_1, \dots, x_n)\ , \dots,\ f_m(x_1, \dots, x_n)\}.$$

Во множестве D могут содержаться нелинейные, немонотонные и существенные функции а.-л. Определим о.-д. функцию $f_L(D)$. Если в D содержится какая-либо нелинейная функция а.-л. F_l, то $f_L(D)$ - функция с одним состоянием, в котором реализуется F_l. В противном случае, $f_L(D)$ - функция с одним состоянием, в котором реализуется константа 0. Аналогичным образом определим о.-д. функции $f_M(D)$ и $f_s(D)$. Пусть

$$M' = P_D^2 \bigcup \{f_1(x_1, \dots, x_n)\ , \dots,\ f_m(x_1, \dots, x_n\} \cup \{f_L(D)\} \cup \{f_s(D)\} \cup \{f_M(D)\}.$$

Нетрудно видеть, что все о.-.д. функции $f_L(D), f_s(D), f_M(D)$ содержатся в P_D, поэтому $[M] \supset [M']$. С другой стороны, по построению, $[M] \subset [M']$, следовательно, замыкание системы M' совпадает с замыканием M. Для системы M' справедливо следующее утверждение.

Теорема 2.3. *Пусть*

$$M' = P_D^2 \bigcup \{f_1(x_1, \dots, x_n)\ , \dots,\ f_m(x_1, \dots, x_n)\} \cup \{f_L(D)\} \cup \{f_s(D)\} \cup \{f_M(D)\}.$$

Система M' полна тогда и только тогда, когда она А-полна и в каждом из множеств $C_i^{M'}, i = 1, 2, \dots, s$ содержится хотя бы одно локально нелинейное, хотя бы одно локально существенное и хотя бы одно локально немонотонное состояние.

Доказательство. Действительно, если в каком-то из C_i нет, к примеру, локально существенного состояния, это означает, что множество D не содержит ни одной существенной функции а.-л. и доказательство неполноты в этом случае аналогично доказательству Леммы2.6. Если в каждом из C_i есть состояния указанных типов, то, по аналогии с доказательством теоремы 2.1, можно получить полную систему. □

Поскольку $[M] = [M']$, то теорема 2.3 и будет являться эффективным критерием распознавания полноты для системы M.

2.3. Порождающее множество содержит тождественную функцию и одну из констант

Рассмотрим теперь случай, когда порождающее множество D состоит из тождественной функции а.-л. и одной из констант. Основной целью данного раздела является доказательство следующего утверждения.

Теорема 2.4. *Пусть порождающее множество D содержит тождественную функцию алгебры-логики и одну из констант. Тогда существует алгоритм распознавания полноты систем из Ω^D.*

Без ограничения общности, можно считать, что $D = \{0, x\}$, в разделе 2.3. через D обозначено именно это множество. Пусть

$$M = P_D^2 \bigcup \{f(x_1, \dots, x_n)\}.$$

Тогда для определения полноты этой системы достаточно проверить, существует ли в замыкании M тождественная единица. Если существует, то задача будет сведена к случаю $D = \{0, 1, x\}$, которая, как показано выше, алгоритмически разрешима. Если же в замыкании M не существует истинностной единицы, то система не полна. Таким образом, целью этого раздела является построение алгоритма проверки того, принадлежит ли тождественная единица замыканию M.

Введем несколько новых определений.

Константную о.-д. функцию, выход которой не зависит от входных переменных и является периодической последовательностью будем обозначать через $p_1p_2...p_l\langle c_1c_2...c_s\rangle$, где $p_1p_2...p_l$-предпериод, а $c_1c_2...c_s$-период (не обязательно простой) выходной последовательности. Например, тождественную единицу в этих терминах можно обозначить через $\langle 1\rangle$ или $\langle 11\rangle$ или $1\langle 11\rangle$.

Выведем несколько простых свойств таких функций.

Свойство 1. *Пусть $M = P_D^2 \bigcup \{f(x_1, \dots, x_n)\}$ и $\langle 1\rangle \in A[M], \tilde{\alpha_0}\langle\tilde{\alpha}\rangle \in [M]$, где $\tilde{\alpha} \in E_2^s, \tilde{\alpha_0} \in E_2^T$ для некоторых натуральных T, s. Тогда $\tilde{\beta}_0\langle\tilde{\alpha}\rangle \in [M]$ для любого $\tilde{\beta}_0 \in E_2^{T+ks}, k \geq 0$.*

Свойство 2. *Пусть* $M = P_D^2 \bigcup \{f(x_1, \dots, x_n)\}$ *и* $\tilde{\alpha_0}\langle\tilde{\alpha}\rangle \in [M]$, *где* $\tilde{\alpha} \in E_2^s, \tilde{\alpha_0} \in E_2^T$ *для некоторых натуральных* T, s. *Тогда* $\tilde{\alpha_0}\langle\tilde{\beta_1} \dots \tilde{\beta_n}\rangle \in [M]$ *для любых* $\tilde{\beta_1}, \dots, \tilde{\beta_n} \in E_2^s, \tilde{\beta} \leq \tilde{\alpha}, n > 0$.

Пусть $B \subseteq E_2^s$. Обозначим через $\Gamma_T(B)$ множество всех бесконечных последовательностей, представимых в виде $ab_1b_2\dots$, где $a \in E_2^T, b_i \in B$.

Пусть $\lceil\Gamma_T(B)\rceil$ - множество бесконечных последовательностей. Будем считать, что $\gamma \in \lceil\Gamma_T(B)\rceil$ тогда и только тогда, когда существует $\gamma' \in \Gamma_T(B)$ такая, что γ и γ' различаются не более чем в конечном числе разрядов.

Состояния о.-д. функции f, в которых реализуются функции а.-л., не сохраняющие ноль будем называть несохраняющими ноль.

Пусть, как и ранее, $Q(t)$ - множество состояний функции f, достижимых из начального за t шагов, $Q(t) = C_j$ если t представимо в виде $T + j - 1 + ks$, где T — длина предпериода, s — ранг функции f, $k \geq 0, j \in \{1, 2, \dots, s\}$.

Зафиксируем некоторое множество двоичных наборов

$$A = \{\alpha_1, \dots, \alpha_m\} \subseteq E_2^s.$$

Построим ориентированный граф $G_f(A)$ с пометками на ребрах, вершинами которого являются состояния из множества C_1. Пусть $q, p \in C_1$. В $G_f(A)$ существует ребро, ведущее из q в p если и только если существуют $\{\beta_1, \dots, \beta_n\} \in A$ такие, что $\varphi(\beta_1, \dots, \beta_n, q) = p$. Припишем этому ребру пометку $\overline{\psi}(\beta_1, \dots, \beta_n, q)$, т.е. тот набор который является выходом функции f, находящейся в состоянии q, по наборам $\beta_1, \dots, \beta_n$. Таким образом, в графе могут быть кратные ребра и петли. Очевидно, что граф конечен, поэтому в нем можно найти все простые циклы за конечное время. Выберем двоичные наборы, приписанные ребрам, которые входят хотя бы в один простой цикл и обозначим их множество через $I_f(A)$ — образ набора A относительно функции f.

Множество наборов $A \subseteq E_2^s$ будем называть 0-полным, если для любых $\tilde{\alpha}, \tilde{\beta} \in E_2^s$ таких, что $\tilde{\alpha} \geq \tilde{\beta}$ и $\tilde{\alpha} \in A$ выполнено $\tilde{\beta} \in A$.

Теперь можно сформулировать основную теорему этой части.

Теорема 2.5. *Пусть* $M = P_D^2 \bigcup \{f(x_1, \dots, x_n)\}$. *Тогда* M *содержит тождественную единицу тогда и только тогда, когда* $\langle 1 \rangle \in A[M]$ *и для любого 0-полного* $A \subset E_2^{s(f)}$ *выполнено* $I_f(A) \setminus A \neq \emptyset$.

Аналогом лемм про А-полноту в этом случае является лемма 2.12. Необходимость и достаточность условий следуют из последующих трех лемм.

Лемма 2.12. *Пусть* $M = P_D^2 \bigcup \{f(x_1, \dots, x_n)\}$. *Тогда* $\langle 1 \rangle \in A[M]$ *в том и только в том случае, когда в каждом из множеств* $Q(0), Q(1) \dots, Q(T+s)$ *существует состояние, несохраняюшее ноль.*

Доказательство. Действительно, если для некоторого $i \in \{0, 1, \dots, T+s\}$ во множестве $Q(i)$ нет состояний, несохраняющих ноль, то в момент i все функции системы M будут находится в состояниях, в которых реализуются функции, сохраняющие ноль. Следовательно, этим свойством будет обладать и любая суперпозиция над этой системой. Очевидно, что тогда в [M] не может содержаться функция i+1-эквивалентная функции $\langle 1 \rangle$.

Доказательство в другую сторону проведем индукцией по τ. По условию, $Q(0) = \{q_0\}$ и в $Q(0)$ существует состояние, не сохраняющее ноль, следовательно начальное состояние не сохраняет ноль. Тогда выход функции $h = f(\langle 0 \rangle, \dots, \langle 0 \rangle)$ равен 1 в первый момент. Т .е., h 1-эквивалентна функции $\langle 1 \rangle$, $h \in [M]$, поскольку $\langle 0 \rangle, f \in [M]$. Таким образом, база индукции верна.

Пусть утверждение леммы верно для $\tau = k$, т.е. существует о.-д. функция $f^{(k)} \in [M]$ такая, что $f^{(k)}$ k-эквивалентна $\langle 1 \rangle$. Докажем утверждение для $\tau = k+1$. По условию, во множестве $Q(k)$ содержится состояние, не сохраняющее ноль, поскольку

$$Q(k) \in \{Q(0), Q(1) \dots, Q(T+s)\}.$$

Обозначим это состояние через q, оно достижимо из начального по некоторому набору слов длины k:

$$\varphi(\alpha_1, \dots, \alpha_n, q_0) = q, \qquad \alpha_1, \dots, \alpha_n \in E_2^k.$$

Построим функции $h_i(x_1, x_2), i \in \{1, \dots, n\}$ следующим образом.

При $t < k$:

$q(0) = q_0$, $q(t+1) = q_{t+1}$,

$F_{q_t}(x_1, x_2) = x_1$ если $\alpha_i(t+1) = 0$, $F_{q_t}(x_1, x_2) = x_2$ если $\alpha_i(t+1) = 1$.

При $t \geq k$:

$q(t+1) = q_k$, $F_{q_i}(x_1, x_2) = 0$.

Таким образом, функция h_i полностью определена, она имеет $k+1$ состояний и, как несложно видеть, принадлежит замыканию M. Далее, видно что $h_i(\langle 0 \rangle, f^{(k)}) = \alpha_i\langle 0 \rangle$, откуда следует, что $\alpha_i\langle 0 \rangle$ также принадлежит $[M]$. Рассмотрим $f(\alpha_1\langle 0 \rangle, \dots, \alpha_n\langle 0 \rangle) = g$. Через k тактов после начала работы функция f окажется в состоянии q, в момент $k+1$ на его вход будут поданы нули, следовательно выход функции g равен единице в момент $k+1$. Введем вспомогательную функцию $h_0(x_1, x_2)$:

$q(0) = q_0$, $q(t+1) = q_{t+1}$, $F_{q_t}(x_1, x_2) = x_1$ при $t < k$,

$q(t+1) = q_k$, $F_{q_t}(x_1, x_2) = x_2$ при $t \geq k$.

Заметим, что $h_0(x_1, x_2)$ принадлежит $[M]$ и выход функции $h_0(f^{(k)}, g)$ равен единице в первые $k+1$ моментов времени. Таким образом, переход индукции и лемма в целом полностью доказаны. Нетрудно видеть, что проверка условий леммы может быть осуществлена за конечное число операций. □

Лемма 2.13. *Пусть $M = P_D^2 \bigcup \{f(x_1, \dots, x_n)\}$. Если существует некоторое 0-полное множество $A \subset E_2^{s(f)}$ такое, что $I_f(A) \setminus A = \emptyset$, то M не содержит истинностную единицу.*

Доказательство. Докажем, что в этом случае все функции системы M сохраняют множество бесконечных последовательностей $\lceil \Gamma_T(A) \rceil$. Рассмотрим бесконечную последовательность $f(\gamma_1, \dots, \gamma_n)$, где $\gamma_1, \dots, \gamma_n \in \lceil \Gamma_T(A) \rceil$. По определению, существует такое натуральное k, что $\gamma_i \in \Gamma_{T+sk}(A), i = 1, \dots, n$. Тогда в момент $T + sk$ функция f находится в одном из состояний множества C_1. В следующие s моментов выход f равен одному из наборов, приписанных ребрам графа $G_f(A)$, в послеследующие s моментов имеем аналогичную ситуацию и т.д. Учитывая то, что по ребрам, не входящим ни в один цикл, можно пройти не более чем один раз, получаем

$$f(\gamma_1, \dots, \gamma_n) \in \lceil \Gamma_{T+sk}(I_f(A)) \rceil \subseteq \lceil \Gamma_T(A) \rceil.$$

Ясно, что если все функции системы сохраняют $\lceil \Gamma_T(A) \rceil$, то и любая их суперпозиция сохраняет это множество. Отсюда следует, что истинностная единица не принадлежит замыканию M, поскольку она не сохраняет $\lceil \Gamma_T(A) \rceil$ ни для какого 0-полного $A \subset E_2^{s(f)}$. □

Лемма 2.14. *Пусть* $M = P_D^2 \bigcup \{f(x_1, \dots, x_n), \langle 1 \rangle \in A[M]$. *Пусть* $A \subset E_2^{s(f)}$ *0-полное множество такое, что* $I_f(A) \setminus A \neq \emptyset$ *и* $p_1 p_2 \dots p_T \langle \tilde{\alpha} \rangle \in [M]$ *при всех* $p_1, p_2, \dots, p_T \in E_2$, *при всех* $\tilde{\alpha} \in A$. *Тогда существует 0-полное множество* $B \supset A$ *такое, что* $p_1 p_2 \dots p_T \langle \tilde{\beta} \rangle \in [M]$ *при всех* $p_1, p_2, \dots, p_T \in E_2$, *при всех* $\tilde{\beta} \in B$.

Доказательство. Из того, что $I_f(A) \setminus A \neq \emptyset$ следует, что в графе $G_f(A)$ существует ребро с пометкой $\tilde{\alpha} \in E_2^s, \tilde{\alpha} \notin A$, причем это ребро принадлежит некоторому простому циклу. Пусть длина этого цикла равна l. Тогда ясно, что для любого $k = 0, \dots, l-1$ существуют такие о.-д. функции

$$g_1^k = \tilde{\gamma_1^0} \langle \tilde{\gamma_1^1} \dots \tilde{\gamma_1^l} \rangle, \dots, g_n^k = \tilde{\gamma_n^0} \langle \tilde{\gamma_n^1} \dots \tilde{\gamma_n^l} \rangle, \tilde{\gamma_i^0} \in E_2^T + ks, \tilde{\gamma_i^j} \in A$$

что $f(g_1^k, \dots, g_n^k) = \tilde{\alpha_k^0} \langle \tilde{\alpha^1} \dots \tilde{\alpha^l} \rangle$, где $\tilde{\alpha^1} = \tilde{\alpha}, \tilde{\alpha_k^0} \in E_2^{T+sk}$. Это следует из определения графа $G_f(A)$ и того, что любое состояние множества C_1 достижимо из начального за время $T + sk$. Согласно свойствам 1 и 2, $g_1^k, \dots, g_n^k \in [M]$, следовательно, $\tilde{\alpha_k^0} \langle \tilde{\alpha^1} \dots \tilde{\alpha^l} \rangle \in [M]$.

Рассмотрим о.-д. функцию $h(x_1, \dots, x_l) = y$. Положим, $y(t) = x_i(t)$, если t представимо в виде $T+Nls+(i-1)s+d+1, d < s$ для некоторого натурального N и $y(t) = x_1$, если $t \leq T$. Ясно, что $h(x_1, \dots, x_l) \in P_D^2$ и $h(\tilde{\alpha_0^0}\langle\tilde{\alpha^1}\dots\tilde{\alpha^l}\rangle, \dots, \tilde{\alpha_l^0}\langle\tilde{\alpha^1}\dots\tilde{\alpha^l}\rangle) = \tilde{\alpha_0^0}\langle\tilde{\alpha}\rangle \in [M]$. Отсюда, по свойству 2 следует, что $\tilde{\beta^0}\langle\tilde{\beta}\rangle \in [M]$ для всех $\tilde{\beta^0} \in E_2^T, \tilde{\beta} \leq \tilde{\alpha}$. Возьмем в качестве B множество наборов $\tilde{\beta}$ таких, что либо $\tilde{\beta} \leq \tilde{\alpha}$, либо $\tilde{\beta} \in A$ и получим, что для него утверждение леммы верно. □

Лемма 2.15. *Пусть* $M = P_D^2 \bigcup \{f(x_1, \dots, x_n)\}$, $\langle 1\rangle \in A[M]$ *и для любого 0-полного* $A \subset E_2^{s(f)}$ *выполнено* $I_f(A) \setminus A \neq \emptyset$. *Тогда* $[M]$ *содержит истинностную единицу.*

Доказательство. Рассмотрим $A(0) = \{0^{s(f)}\}$. Ясно, что $A(0)$ 0-полное и $\tilde{\alpha_0}\langle\tilde{\alpha}\rangle \in [M]$ для любых $\tilde{\alpha_0} \in E_2^T, \tilde{\alpha} \in A(0)$. Тогда, по лемме 2.14 получим, что существует некоторое 0-полное $A(1) \supset A(0)$, обладающее такими же свойствами. Другими словами, можно построить цепочку вложений $A(0) \subset A(1) \subset A(2) \subset \dots$ такую, что все множества 0-полны и $\tilde{\alpha_0}\langle\tilde{\alpha}\rangle \in [M]$ для любых $\tilde{\alpha_0} \in E_2^T, \tilde{\alpha} \in A(k), k \geq 0$. Поскольку всевозможных подмножеств множества $E_2^{s(f)}$ конечное число, на некотором шаге получим $A(i) = E_2^{s(f)}$. Отсюда и будет следовать, что $\langle 1\rangle \in [M]$.

Таким образом, теорема 2.5 полностью доказана. □

Доказательство теоремы 2.5 легко переносится на более общий случай, справедливо следующее утверждение.

Теорема 2.6. *Пусть* $M = P_D^2 \bigcup \{f_1(x_1, \dots, x_n)\ , \dots,\ f_m(x_1, \dots, x_n)\}$. *Тогда* M *содержит истинностную единицу если и только если* $\langle 1\rangle \in A[M]$ *и для любого 0-полного* $A \subset E_2^{s^M}$ *существует* $i \in \{1, \dots, m\}$ *такое, что* $I_{f_i}(A) \setminus A \neq \emptyset$.

Итак, в данном разделе приведен алгоритм проверки того, принадлежит ли замыканию системы

$$M = P_D^2 \bigcup \{f_1(x_1, \dots, x_n)\ , \dots,\ f_m(x_1, \dots, x_n)\}$$

тождественная единица. Если не принадлежит, то, естественно, система M не полна.

Пусть истинностная единица принадлежит $[M]$, тогда рассмотрим

$$M' = P^2_{\{0,1,x\}} \bigcup \{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\}.$$

Несложно видеть, что $[M] = [M']$, а критерий распознавания полноты системы M' существует, он описан в параграфе 2.2. Из приведенных рассуждений следует справедливость теоремы 2.4.

2.4. Порождающее множество содержит тождественную функцию

Рассмотрим теперь более общий случай, а именно тот, когда множество D состоит только из тождественной функции а.-л. Множество $P^2_{\{x\}}$ будем обозначать через P_0.

Пусть

$$M = P^2_0 \bigcup \{f(x_1, \dots, x_n)\}.$$

Тогда для определения полноты этой системы достаточно проверить, существуют ли в замыкании M истинностные константы. Если существуют, то задача будет сведена к случаю $D = \{0, 1, x\}$, которая, как показано выше, алгоритмически разрешима. В противном случае система не полна. Для общего случая получить эффективный критерий не удалось, поэтому были рассмотрены несколько более узких случаев.

В параграфе 2.4.1. получен алгоритм для А-полноты. В параграфе 2.4.2. построен эффективный критерий полноты при условии, что система M содержит произвольную константную функцию. В параграфе 2.4.3. построен эффективный критерий полноты при условии, что система M содержит функцию задержки.

2.4.1. Критерий А-полноты

В этом разделе приводится эффективный критерий распознавания А-полноты систем из Ω^D.

Лемма 2.16. *Пусть $M = P_0 \bigcup \{f(x_1, \dots, x_n)\}$. Тогда M является А-полной в том и только в том случае, когда в каждом из множеств $Q_0(0), Q_0(1) \dots, Q_0(T+s)$ существует состояние, не сохраняющее ноль, не сохраняющее единицу, а также нелинейное, немонотонное и несамодвойственное состояние.*

Доказательство. Действительно, если для некоторого $i \in \{0, 1, \dots, T+s\}$ во множестве $Q_0(i)$ нет состояний, к примеру, несохраняющих ноль, то в момент i все функции системы M будут находится в состояниях, в которых реализуются функции а.-л., сохраняющие ноль. Следовательно, этим свойством будет обладать и любая композиция над этой системой. Очевидно, что тогда в $[M]$ не может содержаться функция i+1-эквивалентная истинностной единице. Следовательно, система M не А-полна.

Доказательство в другую сторону проведем индукцией по τ. По условию, $Q_0(0) = \{q_0\}$ и F_{q_0} не сохранят ноль, единицу, немонотонна, нелинейна и несамодвойственна. Другими словами, F_{q_0} - шефферова функция а.-л. Пусть H - произвольная о.-д. функция, в начальном состоянии которой реализуется функция а.-л. h_0. Как нетрудно видеть, существует о.-д. функция $H^M \in [M]$, такая что в начальном состоянии функции H^M тоже реализуется функция h_0. Тогда H 1-эквивалентна H^M и система $[M]$ 1-полна. Таким образом, база индукции верна.

Пусть утверждение леммы верно для $\tau = k$, т.е. $[M]$ k-полна. Докажем утверждение для $\tau = k+1$. По условию, во множестве $Q_0(k)$ содержится состояние, не сохраняющее ноль, поскольку

$$Q_0(k) \in \{Q_0(0), Q_0(1) \dots, Q_0(T+s)\}.$$

Обозначим это состояние через q, оно достижимо из начального по некоторому набору слов длины k:

$$\varphi(\alpha_1, \dots, \alpha_n, q_0) = q, \qquad \alpha_1, \dots, \alpha_n \in E_2^k$$

Построим для каждого слова α_i функцию $h_i(y_1, y_2, x_i), i \in \{1, \dots, n\}$ следующим образом.

При $t < k$:

$q(0) = q_0$, $q(t+1) = q_{t+1}$,

$F_{q_t}(y_1, y_2, x_i) = y_1$ если $\alpha_i(t+1) = 0$,

$F_{q_t}(y_1, y_2, x_i) = y_2$ если $\alpha_i(t+1) = 1$.

При $t \geq k$:

$q(t+1) = q_k$, $F_{q_i}(y_1, y_2, x_i) = x_i$.

Таким образом, функция h_i полностью определена, она имеет $k+1$ состояний и, как несложно видеть, принадлежит замыканию M (поскольку принадлежит P_0). Пусть $0^k, 1^k \in [M]$ - о.-д. функции, k-эквивалентные истинностным константам. Рассмотрим о.-д. функцию $e_i(x_i) = h_i(0^k, 1^k, x_i)$. Первые k тактов функция e_i выдает символы слова α_i, а начиная с $k+1$ такта пропускает переменную x_i. Рассмотрим о.-д. функцию $f_0^{k+1}(x_1, \dots, x_n) = f(e_1(x_1), \dots, e_n(x_n))$. Через k тактов после начала работы функция f окажется в состоянии q, в момент $k+1$ на его вход будут поданы переменные $x_1, \dots, x_n$. Следовательно, в момент $k+1$ у функции f_0^{k+1} достижимое только одно состояние, в котором реализуется функция а.-л., не сохраняющая ноль. Из построения следует, что $f_0^{k+1} \in [M]$.

Аналогичным образом получим о.-д. функции $f_1^{k+1}, f_L^{k+1}, f_M^{k+1}, f_s^{k+1}$ у каждой из которых достижимо только одно состояние в $k+1$ момент, в котором реализуется функция а.л. несохраняющая единицу, нелинейная функция, немонотонная или несамодвойственная соответственно.

Пусть $H(x_1, \dots, x_m)$ - произвольная о.-д. функция. Построим функцию $H^{k+1} \in [M]$ такую, что H^{k+1} $(k+1)$-эквивалентна H. Пусть в момент $k+1$ у функции H достижимы состояния $q_1, \dots, q_r$, в которых реализуются функции а.-л. $h_1, \dots, h_r$. С помощью суперпозиции из функций $f_0^{k+1}, f_1^{k+1}, f_L^{k+1}, f_M^{k+1}, f_s^{k+1}$ можно получить о.-д. функцию $f_{h_i}^{k+1}$ у которой в момент $k+1$ реализуется функция $h_i, i = 1, \dots, r$.

Рассмотрим о.-д. функцию $H_0(x_1, \dots x_m, y_1, \dots, y_r)$, которая задается следующим образом. Состояния функции H_0 и функция переходов между состояниями такие же, как у функции H, в состояниях $q_1, \dots , q_r$ реализуются переменные $y_1, \dots , y_r$ соответственно, а в остальных состояниях реализуется переменная x_1. Очевидно, что $H_0 \in P_0$. Пусть $H_1 = H_0(x_1, \dots x_m, f^{k+1}_{h_1}, \dots , f^{k+1}_{h_r})$. Как нетрудно видеть, выход функции H_1 совпадает с выходом функции H в момент $k + 1$ и $H_1 \in [M]$.

Для завершения доказательства осталось рассмотреть о.-д. функцию $e^{k+1}(x_1, x_2) \in [P_0]$, удовлетворяющую следующим условиям:

$q(0) = q_0$, $q(t + 1) = q_{t+1}$, $F_{q_t}(x_1, x_2) = x_1$ при $t < k$

$q(t + 1) = q_k$, $F_{q_t}(x_1, x_2) = x_2$ при $t \geq k$

В первые k тактов функция e^{k+1} пропускает переменную x_1, а начиная с момента $k + 1$ пропускает x_2.

Положим $H^{k+1} = e^{k+1}(H^k, H_1)$. Очевидно, что $H^{k+1} \in [M]$ и H^{k+1} $(k + 1)$-эквивалентна H. Таким образом, переход индукции и лемма в целом полностью доказаны. Нетрудно видеть, что проверка условий леммы может быть осуществлена за конечное число операций. □

Пусть теперь $M = P_0 \bigcup \{f_1(x_1, \dots , x_n)\ , \dots,\ f_m(x_1, \dots , x_n)\}$.

Пусть

$$Q^M(T) = Q^{f_1}(T) \cup \ \dots\ \cup Q^{f_m}(T).$$

Рассмотрим последовательность

$$Q^M(0), Q^M(1), Q^M(2) \dots$$

Эта последовательность периодична, пусть T^M — длина предпериода, s^M — длина периода, будем называть этот параметр рангом совокупности функций из M.

Лемма 2.17. *Пусть* $M = P_0 \bigcup \{f_1(x_1, \dots , x_n)\ , \dots,\ f_m(x_1, \dots , x_n)\}$. *Система* M *А-полна тогда и только тогда, когда в каждом из множеств* $Q^M_0(i)$, $i = 0, 1, \dots , T^M + s^M$ *содержится хотя бы одно нелинейное, несамодвойственное и немонотонное состояние, а также хотя бы одно состояние, несохраняющее ноль и состояние, несохраняющее единицу.*

Доказательство этой полностью аналогично доказательству леммы 2.16.

Перейдем теперь к общему случаю. Пусть D - произвольный замкнутый класс а.-л., содержащий тождественную функцию и

$$M = P_D^2 \cup \{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\}.$$

Поскольку D - замкнутый класс а.-л., в нем можно выделить конечный базис. Рассмотри функции а.-л. $r_1, \dots, r_d$, которые образуют этот базис. Пусть о.-д. функция R_i имеет только одно состояние, в котором реализуется функция $r_i, i \in \{1, \dots, d\}$.

Пусть

$$M = P_D^2 \cup \{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\}$$

$$M' = P_0^2 \cup \{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\} \cup \{R_1, \dots, R_d\}.$$

Ясно, что $[M] = [M']$. Сформулируем основную теорему этой части.

Теорема 2.7. *Пусть*

$$M = P_D^2 \cup \{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\},$$

$$M' = P_0^2 \cup \{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\} \cup \{R_1, \dots, R_d\}.$$

Система M полна тогда и только тогда, когда в каждом из множеств $Q_0^{M'}(i), i = 0, 1, \dots, T^{M'} + s^{M'}$ содержится хотя бы одно нелинейное, несамодвойственное и немонотонное состояние, а также хотя бы одно состояние, несохраняющее ноль и состояние, несохраняющее единицу.

Справедливость теоремы 2.7 следует из приведенных выше рассуждений. Нетрудно видеть, что проверка условий теоремы может быть осуществлена за конечное число операций. Таким образом, эффективный критерий распознавания А-полноты построен. Заметим, что доказательство предшествующих двух лемм не зависит от наличия операции обратной связи. Поэтому, теорема 2.7 будет верна и для случая, когда рассматривается операция композиции (при наличии обратной связи).

2.4.2. Система M содержит константную функцию

Константную о.-д. функцию, выход которой не зависит от входных переменных и является периодической последовательностью будем обозначать через $p_1p_2...p_l\langle c_1c_2...c_m\rangle$, где $p_1p_2...p_l$-предпериод, а $c_1c_2...c_m$-период (не обязательно простой) выходной последовательности. Например, истинностную единицу в этих терминах можно обозначить через $\langle 1\rangle$ или $\langle 11\rangle$ или $1\langle 11\rangle$.

Пусть

$$M = P_0^2 \bigcup \{f(x_1, \dots , x_n), K\},$$

где $K = p_1p_2...p_l\langle c_1c_2...c_m\rangle$ - константная функция.

Выведем несколько простых свойств таких систем.

Свойство 3. *Пусть* $M = P_0^2 \bigcup \{f(x_1, \dots , x_n), K\}, M$ *A-полна и* $\tilde{\alpha}_0\langle\tilde{\alpha}\rangle \in [M]$, *где* $\tilde{\alpha} \in E_2^s, \tilde{\alpha}_0 \in E_2^T$ *для некоторых натуральных* T, s. *Тогда* $\tilde{\beta}_0\langle\tilde{\alpha}\rangle \in [M]$ *для любого* $\tilde{\beta}_0 \in E_2^{T+ks}, k \geq 0$.

Свойство 4. *Пусть* $M = P_0^2 \bigcup \{f(x_1, \dots , x_n), K\}, K = p_1p_2...p_l\langle c_1c_2...c_m\rangle$ *и* $\tilde{\alpha}_0\langle\tilde{\alpha}\rangle \in [M]$, *где* $\tilde{\alpha} \in E_2^m, \tilde{\alpha}_0 \in E_2^l$. *Тогда* $\tilde{\alpha}_0\langle\tilde{\beta}\rangle \in [M]$ *для любого* $\tilde{\beta} \in E_2^m$,*такого что* $\tilde{\beta}(i) \in \{\tilde{\alpha}(i), c_i\}, i = \{1, \dots , m\}$.

Пусть $B \subseteq E_2^s$. Обозначим через $\Gamma_T(B)$ множество всех бесконечных последовательностей, представимых в виде $ab_1b_2...$, где $a \in E_2^T, b_i \in B$.

Пусть $\lceil\Gamma_T(B)\rceil$ - множество бесконечных последовательностей. Будем считать, что $\gamma \in \lceil\Gamma_T(B)\rceil$ тогда и только тогда, когда существует $\gamma' \in \Gamma_T(B)$ такая, что γ и γ' различаются не более чем в конечном числе разрядов.

Состояния о.-д. функции f, в которых реализуются функции а.-л., не сохраняющие ноль будем называть несохраняющими ноль.

Пусть, как и ранее, $Q(0), Q(1), \dots$ — последовательность подмножеств состояний функции f. Ранее показано, что $Q(t) =_j$ если t представимо в виде $T + j - 1 + ks$, где T — длина предпериода, $s(f)$ — длина периода, $k \geq 0, j \in \{1, 2, \dots , s\}$.

Число $s = s(f) \cdot m$ (m — длина периода функции K) также будет периодом этой последовательности и периодом функции K.

Зафиксируем некоторое множество двоичных наборов $A = \{\alpha_1, \dots, \alpha_r\} \subseteq E_2^s$. Построим ориентированный граф $G_f(A)$ с пометками на ребрах, вершинами которого являются состояния из множества C_1. Пусть $q, p \in C_1$. В $G_f(A)$ существует ребро, ведущее из q в p если и только если существуют $\{\beta_1, \dots, \beta_n\} \in A$ такие, что $\varphi(\beta_1, \dots, \beta_n, q) = p$. Припишем этому ребру пометку $\overline{\psi}(\beta_1, \dots, \beta_n, q)$, т.е. тот набор который является выходом функции f, находящейся в состоянии q, по наборам $\beta_1, \dots, \beta_n$. Таким образом, в графе могут быть кратные ребра и петли. Очевидно, что граф конечен, поэтому в нем можно найти все простые циклы за конечное время. Выберем двоичные наборы, приписанные ребрам, которые входят хотя бы в один простой цикл и обозначим их множество через $I_f(A)$ — образ набора A относительно функции f.

Множество наборов $A \subseteq E_2^s$ будем называть K-полным, если для любых $\tilde{\alpha}, \tilde{\beta} \in E_2^s$ таких, что $\tilde{\beta}(i) \in \{\tilde{\alpha}(i), c_i\}, i = 1, \dots, s$ и $\tilde{\alpha} \in A$ выполнено $\tilde{\beta} \in A$.

Теперь можно сформулировать основную теорему этой части.

Теорема 2.8. *Пусть $M = P_0 \bigcup \{f(x_1, \dots, x_n), K\}$. Тогда M содержит обе истинностные константы если и только если M A-полна и для любого 0-полного $A \subset E_2^s$ выполнено $I_f(A) \setminus A \neq \emptyset$.*

Необходимость условий следуют из леммы 2.18, а достаточность — из лемм 2.19,2.20.

Лемма 2.18. *Пусть $M = P_0 \bigcup \{f(x_1, \dots, x_n), K\}$. Если существует некоторое K-полное множество $A \subset E_2^{s(f)}$ такое, что $I_f(A) \setminus A = \emptyset$, то M не полна.*

Доказательство. Докажем, что в этом случае все функции системы M сохраняют множество бесконечных последовательностей $\lceil \Gamma_T(A) \rceil$. Рассмотрим бесконечную последовательность $f(\gamma_1, \dots, \gamma_n)$, где $\gamma_1, \dots, \gamma_n \in \lceil \Gamma_T(A) \rceil$. По определению, существует такое натуральное k, что $\gamma_i \in \Gamma_{T+sk}(A), i = 1, \dots, n$. Тогда в момент $T + sk$ функция f находится в одном из состояний множества C_1. В следующие s моментов выход f равен одному из наборов, приписанных ребрам графа $G_f(A)$, в последующие s моментов имеем аналогичную ситуацию и т.д. Учитывая то, что по ребрам, не входящим ни в один цикл, можно пройти не более чем один раз, получаем

$$f(\gamma_1, \dots, \gamma_n) \in \lceil \Gamma_{T+sk}(I_f(A)) \rceil \subseteq \lceil \Gamma_T(A) \rceil$$

Ясно, что если все функции системы сохраняют $\lceil \Gamma_T(A) \rceil$, то и любая их суперпозиция сохраняет это множество. Отсюда и следует, что M не полна. $\square$

Лемма 2.19. *Пусть $M = P_0 \bigcup \{f(x_1, \dots, x_n), K\}, M$ A-полна. Пусть $A \subset E_2^s$ K-полное множество такое, что $I_f(A) \setminus A \neq \emptyset$ и $p_1 p_2 ... p_T \langle \tilde{\alpha} \rangle \in [M]$ при всех $p_1, p_2, ..., p_T \in E_2$, при всех $\tilde{\alpha} \in A$. Тогда существует K-полное множество $B \supset A$ такое, что $p_1 p_2 ... p_T \langle \tilde{\beta} \rangle \in [M]$ при всех $p_1, p_2, ..., p_T \in E_2$, при всех $\tilde{\beta} \in B$.*

Доказательство. Из того, что $I_f(A) \setminus A \neq \emptyset$ следует, что в графе $G_f(A)$ существует ребро с пометкой $\tilde{\alpha} \in E_2^s, \tilde{\alpha} \notin A$, принадлежащее некоторому простому циклу. Пусть длина этого цикла равна l. Тогда ясно, что для любого $k = 0, \dots, l-1$ существуют такие о.-д. функции

$$g_1^k = \tilde{\gamma_1^0} \langle \tilde{\gamma_1^1} ... \tilde{\gamma_1^l} \rangle, \dots, g_n^k = \tilde{\gamma_n^0} \langle \tilde{\gamma_n^1} ... \tilde{\gamma_n^l} \rangle, \tilde{\gamma_i^0} \in E_2^T + ks, \tilde{\gamma_i^j} \in A$$

что $f(g_1^k, \dots, g_n^k) = \tilde{\alpha_k^0} \langle \tilde{\alpha^1} ... \tilde{\alpha^l} \rangle$, где $\tilde{\alpha^1} = \tilde{\alpha}, \tilde{\alpha_k^0} \in E_2^{T+sk}$. Это следует из определения графа $G_f(A)$ и того, что любое состояние множества C_1 достижимо из начального за время $T+sk$. Согласно свойствам 1 и 2, $g_1^k, \dots, g_n^k \in [M]$, следовательно, $\tilde{\alpha_k^0} \langle \tilde{\alpha^1} ... \tilde{\alpha^l} \rangle \in [M]$.

Рассмотрим о.-д. функцию $h(x_1, \dots, x_l) = y$. Положим, $y(t) = x_i(t)$, если t представимо в виде $T + Nls + (i-1)s + d + 1, d = \{0, 1, ..., s-1\}$ для некоторого натурального N и $y(t) = x_1$, если $t \leq T$. Ясно, что $h(x_1, \dots, x_l) \in P_0^2$ и $h(\tilde{\alpha_0^0} \langle \tilde{\alpha^1} ... \tilde{\alpha^l} \rangle, \dots, \tilde{\alpha_l^0} \langle \tilde{\alpha^1} ... \tilde{\alpha^l} \rangle) = \tilde{\alpha_0^0} \langle \tilde{\alpha} \rangle \in [M]$. Отсюда из свойства 4 следует, что $\tilde{\beta}^0 \langle \tilde{\beta} \rangle \in [M]$ для всех $\tilde{\beta}^0 \in E_2^T, \tilde{\beta} \in E_2^s$ таких, что $\tilde{\beta}(i) \in \{\tilde{\alpha}(i), c_i\}, i = 1, \dots, s$.

Возьмем в качестве B множество наборов $\tilde{\beta}$ таких, что либо $\tilde{\beta}(i) \in \{\tilde{\alpha}(i), c_i\}, i = 1, \dots, s$, либо $\tilde{\beta} \in A$ и получим, что для него утверждение леммы верно. $\square$

Лемма 2.20. *Пусть* $M = P_0 \bigcup \{f(x_1, \dots, x_n), K\}$, M *А-полна и для любого К-полного* $A \subset E_2^s$ *выполнено* $I_f(A) \setminus A \neq \emptyset$. *Тогда* $[M]$ *содержит обе истинностные константы.*

Доказательство. Рассмотрим $A(0) = \{c_1, \dots, c_s\}$. Ясно, что $A(0)$ К-полно и $\tilde{\alpha_0}\langle\tilde{\alpha}\rangle \in [M]$ для любых $\tilde{\alpha_0} \in E_2^T, \tilde{\alpha} \in A(0)$. Тогда, по предыдущей лемме получим, что существует некоторое К-полное $A(1) \supset A(0)$, обладающее такими же свойствами. Другими словами, можно построить цепочку вложений $A(0) \subset A(1) \subset A(2) \subset \dots$ такую, что все множества К-полны и $\tilde{\alpha_0}\langle\tilde{\alpha}\rangle \in [M]$ для любых $\tilde{\alpha_0} \in E_2^T, \tilde{\alpha} \in A(k), k \geq 0$. Поскольку всевозможных подмножеств множества E_2^s конечное число, на некотором шаге получим $A(i) = E_2^s$. Отсюда и будет следовать, что $\langle 0\rangle, \langle 1\rangle \in [M]$. □

Таким образом, теорема 2.8 полностью доказана.

Доказательство теоремы 2.8 легко переносится на более общий случай, справедливо следующее утверждение.

Теорема 2.9. *Пусть* $M = P_0 \bigcup \{f_1(x_1, \dots, x_n)\ , \dots,\ f_m(x_1, \dots, x_n), K\}$. *Тогда* M *содержит истинностные константы если и только если* M *А-полна и для любого К-полного* $A \subset E_2^{s^M}$ *существует* $i \in \{1, \dots, n\}$ *такое, что* $I_{f_i}(A) \setminus A \neq \emptyset$.

Пусть $\Omega^D(f)$ — совокупность всех подмножеств M о.-д. функций, содержащих Ω^D и о.-д. функцию f, таких, что множество $M \setminus \Omega^D$ конечно.

Из предыдущей теоремы следует следующее утверждение.

Теорема 2.10. *Пусть множество* D *содержит тождественную функцию а.-л. Тогда существует эффективный критерий распознавания полноты систем из* $\Omega^D(C)$, *где* C *— константная о.-д. функция.*

2.4.3. Система M содержит функцию задержки

Без ограничения общности можно считать, что M содержит нулевую задержку G_0. Покажем, что существует алгоритм проверки существования в $[M]$ тождественного нуля. Тогда задача распознавания полноты M будет сведена к случаю, рассмотренному в разделе 2.3., который, как показано ранее, алгоритмически разрешим.

Введем несколько новых определений.

Рассмотрим о.-д. функцию $h_k^\alpha(x_1, \dots, x_n) = y, \alpha \in E_2, k$ - натуральное число. Положим $y(t) = \alpha$, если выполнено хотя бы одно из следующих условий:

1) $t \leq k$.

2) существуют числа $i \in \{1, \dots, n\}, \tau \in \{t-k, t-k+1, \dots, t-1\}$ такие, что $x_i(\tau) = \alpha$.

Положим $y(t) = \overline{\alpha}$ во всех остальных случаях.

Например, функция $h_1^0(x)$ является нулевой задержкой G_0.

Лемма 2.21. *$h_k^0(x_1, \dots, x_n) \in [P_0 \cup \{G_0\}]$ для любых k, n.*

Доказательство. Рассмотрим о.-д. функцию $H(x_1, \dots, x_n, x_{11}, \dots, x_{1k}, \dots, x_{n1}, \dots, x_{nk})$, диаграмма Мура этой функции схематично изображена на Рис.2.3. H имеет nk состояний, в каждом из которых реализуется одна из переменных x_{ij}. Переходы между состояниями зависят только от значений переменных $x_1, \dots, x_n$. На рисунке для каждого состояния указаны переходы, которые реализуются, если все переменные $x_1, \dots, x_n$ принимают значение 1. Переходы по всем остальным наборам ведут из любого состояния в состояние x_{11}, если $x_1 = 0$; в x_{21}, если $x_1 = 1, x_2 = 0$ и т.д. Состояние, в котором реализуется переменная x_{11} является начальным. Очевидно, $H \in P_0$.

Рассмотрим суперпозицию

$$F(x_1, \dots, x_n) = H(x_1, \dots, x_n, G_0(x_1), \dots, G_0^k(x_1), \dots, G_0(x_n), \dots, G_0^k(x_n)).$$

Как нетрудно видеть, $F(x_1, \dots, x_n) = h_k^\alpha(x_1, \dots, x_n)$, таким образом, лемма доказана. $\square$

Аналогично формулируется и доказывается следующая лемма.

Лемма 2.22. *$h_k^1(x_1, \dots, x_n) \in [P_0 \cup \{G_1\}]$ для любых k, n.*

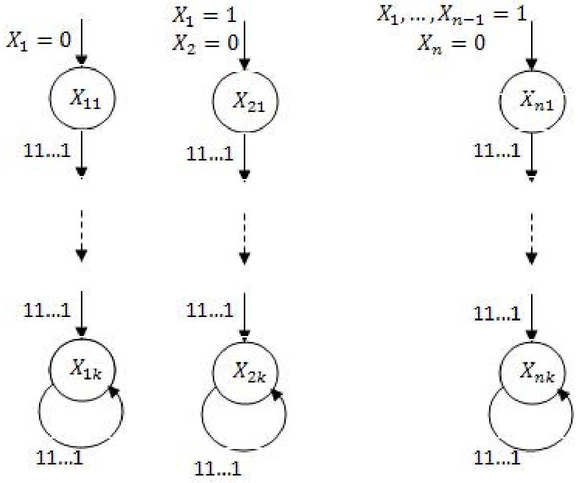

Рис. 2.3.

Пусть Q - множество состояний о.-д. функции $f(x_1, \dots, x_n)$. Будем говорить, что состояния $p, q \in Q$ 1-связны, если p достижимо из q, либо q достижимо из p по набору слов $a_1, \dots, a_n \in E_2^m$ состоящих только из единиц.

Подмножество $K^1 \subseteq Q$ будем называть компонентой 1-связности, если:

1) Для любых $q, p \in K^1$ существует $r \in K^1$ такое, что q 1-связно с r и p 1-связно с r.

2) Если $q \in K^1$ и существует состояние $p \in Q$, такое что q и p связны, то $p \in K^1$.

Все множество состояний Q разбивается на непересекающиеся компоненты 1-связности. Рассмотрим некоторую компоненту 1-связности K^1. Она задает ориентированный граф $G(K^1)$, вершинами которого являются состояния компоненты. Существует ребро графа, ведущее из состояния p в состояние q тогда и только тогда, когда

$$q = \varphi^f(1, \dots, 1, p).$$

Очевидно, что из каждой вершины графа выходит ровно по одному ребру и граф связен, если рассматривать его как неориентированный. Поэтому в графе будет ровно один цикл. Будем называть множество состояний, являющихся вершинами этого ориентированного цикла, ядром компоненты K^1 и обозначать через $Ker(K^1)$. Мощность ядра компоненты будет равна длине цикла.

Компоненту 1-связности K^1 будем называть несохраняющей единицу, если хотя бы одно состояние из ядра K^1 не сохраняет единицу. Будем называть компоненту K^1 сохраняющей единицу в противном случае.

Аналогичным образом вводятся понятия компоненты 0-связности и ядра компоненты 0-связности.

Пусть K^0 -компонента 0-связности, K^1 -компонента 1-связности. Будем говорить, что эти компоненты взаимносвязаны, если существуют $q \in Ker(K^0), p \in Ker(K^1)$ такие, что q достижимо из p и p достижимо из q.

В следующих двух леммах приводятся достаточные условия существования в $[M]$ константной функции.

Лемма 2.23. *Пусть* $M = P_0 \bigcup \{f_1(x_1, \dots, x_n), G_0\}, M$ *A-полна. Если существуют две взаимосвязанные компоненты* K^1, K^0 *1- и 0-связности соответственно, такие что* K^1 *не сохраняет единицу, то в замыкании M содержится истинностный ноль.*

Доказательство. По определению, существуют состояния $q \in Ker(K^1), p \in Ker(K^0)$ и наборы слов $a_1, \dots, a_n \in E_2^m, b_1, \dots, b_n \in E_2^l$ такие, что

$$p = \varphi^f(a_1, \dots, a_n, q),$$

$$q = \varphi^f(b_1, \dots, b_n, p).$$

Пусть мощность $Ker(K^1)$ равна C_1, (т.е. $q = \varphi^f(1^{C_1}, \dots, 1^{C_1}, q)$), а мощность $Ker(K^0)$ равна C_0. Пусть состояние q достижимо из начального по набору $e_1, \dots, e_n \in E_2^T$. Рассмотрим о.-д. функцию

$$H(x_1, \dots, x_n, x_1^1, \dots, x_{c_1}^1, x_1^2, \dots, x_{c_2}^2, x_1^3, \dots, x_m^3, x_1^4, \dots, x_l^4, x_1^5, \dots, x_T^5),$$

диаграмма Мура которой изображена на рис.2.4. Переходы между состояниями зависят только от значений переменных $x_1, \dots, x_n$. Переходы из состояний $x^1_{c_1}, x^2_{c_2}, x^3_m, x^4_l$ зависят только от того, присутствует ли в наборе $x_1(t), \dots, x_n(t)$ единица. Переходы из остальных состояний безусловны. Очевидно, что $H \in P_0$.

Поскольку система M А-полна и $G_0 \in M$, то и $G_1 \in M$.

Выберем некоторое натуральное число $N > c_0 + c_1 + m + l + T$. Для каждого $i = \{1, \dots, n\}$ построим суперпозицию $H_i(x_1, \dots, x_n)$. Для этого сделаем подстановку в функцию H:

$$x^5_1 \leftarrow h^{e_i(1)}_N(x_1, \dots, x_n), \dots, x^5_T \leftarrow h^{e_i(T)}_N(x_1, \dots, x_n),$$

$$x^1_1 \leftarrow h^1_N(x_1, \dots, x_n), \dots, x^1_{c1} \leftarrow h^1_N(x_1, \dots, x_n),$$

$$x^2_1 \leftarrow h^0_N(x_1, \dots, x_n), \dots, x^2_{c2} \leftarrow h^0_N(x_1, \dots, x_n),$$

$$x^3_1 \leftarrow h^{a_i(1)}_N(x_1, \dots, x_n), \dots, x^3_m \leftarrow h^{a_i(m)}_N(x_1, \dots, x_n),$$

$$x^4_1 \leftarrow h^{b_i(1)}_N(x_1, \dots, x_n), \dots, x^4_l \leftarrow h^{b_i(l)}_N(x_1, \dots, x_n).$$

Рассмотрим суперпозицию

$$g(x_1, \dots, x_n) = f(H_1(x_1, \dots, x_n), \dots, H_n(x_1, \dots, x_n)).$$

Через $T + c_1$ тактов после начала работы функция f окажется в состоянии q.

Если в следующий момент среди значений входных переменных присутствует единица, то в следующие c_1 тактов все функции $H_1, \dots, H_n$ будут выдавать единицу, и функция f опять окажется в состоянии q. Если значения всех входных переменных равны нулю, то в следующие m тактов функции $H_1, \dots, H_n$ будут выдавать слова $a_1, \dots, a_n$ соответственно, и функция f окажется в состоянии p.

Для состояния p также возможны два варианта. Если в следующий момент среди значений входных переменных присутствует единица, то функции $H_1, \dots, H_n$ будут

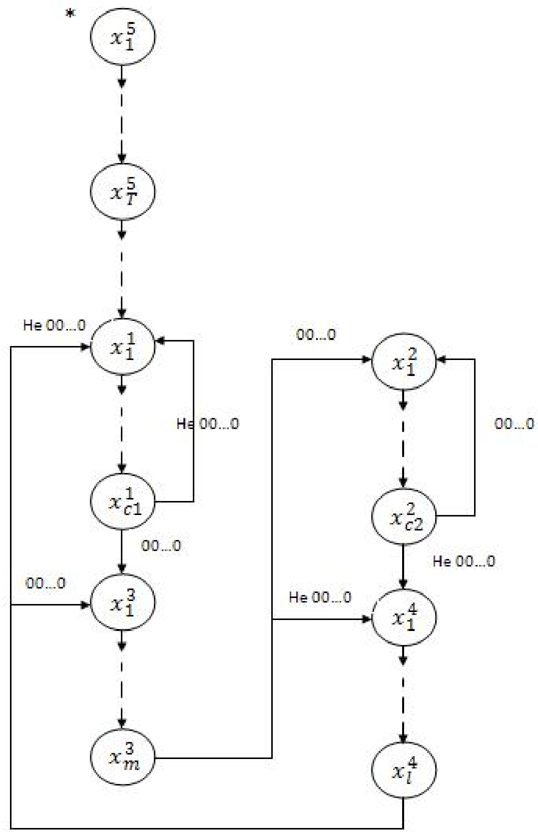

Рис. 2.4.

выдавать слова $b_1, \dots, b_n$ соответственно в следующие l тактов и функция f перейдет в состояние q. В противном случае в следующие c_2 тактов на все входы функции f будут поступать нули, и она вернется в состояние p.

Заметим, что если значения всех переменных $x_1(t), \dots, x_n(t)$ принимают единичные значения на некотором промежутке длины $N, t \in [K, K+N-1]$, то существует $t_1 \in [K, K+N]$ такое, что $g(x_1, \dots, x_n)(t_1) = 0$. Это следует из того, что компонента K^1 не сохраняет единицу.

Следовательно, суперпозиция $h_N^0(x_1, \dots, x_n, g(x_1, \dots, x_n))$ является тождественным нулем, что и требовалось доказать. □

Аналогичным образом доказывается лемма4.

Лемма 2.24. *Пусть* $M = P_0 \bigcup \{f_1(x_1, \dots, x_n), G_0\}, M$ *A-полна. Если существуют две взаимосвязанные компоненты* K^1, K^0 *1- и 0-связности соответственно, такие что* K^0 *не сохраняет ноль, то в замыкании* M *содержится истинностная единица.*

Теперь осталось показать, что эти достаточные условия являются и необходимыми.

Лемма 2.25. *Пусть* $M = P_0 \bigcup \{f_1(x_1, \dots, x_n), G_0\}, M$*. Если не существуют двух взаимосвязанных компонент* K^1, K^0 *1- и 0-связности соответственно таких, что либо* K^0 *не сохраняет ноль, либо* K^1 *не сохраняет единицу, то* $[M]$ *не содержит истинностных констант.*

Доказательство. Для доказательства леммы введем еще одно понятие.

Пусть B - множество бесконечных последовательностей, составленных из элементов E_2. Будем говорить, что B обладает (0,1)-свойством, если для любого натурального L существует t_1 такое, что для любого $b \in B$ выполнено $b(t_1+1) = 1, \dots, b(t_1+L) = 1$ и существует t_0 такое, что для любого $b \in B$ выполнено $b(t_0+1) = 0, \dots, b(t_0+L) = 0$. Как несложно видеть, множества, обладающие (0,1)-свойством существуют, например, $B = \{010011000111...\}$.

Пусть B - некоторое максимальное (0,1)-множество. Т.е. такое, которое нельзя расширить без потери свойства (0,1). Покажем, что любая функция из M сохраняет B.

Для функций из P_0 это утверждение очевидно.

Пусть $b \in B$, покажем что $G_0(b) \in B$. Зафиксируем произвольное L. По определению, существует такое t_0, что $a(t_0+1) = 0, \dots, a(t_0+L+1) = 0$ для любых $a \in B$. Тогда $G_0(b)(t_0+2) = 0, \dots, G_0(b)(t_0+L+1) = 0$, т.е. для любого $i \in [t_0+2, t_0+L+1]$, для любого $a \in B \cup \{G_0(b)\}$ выполнено $a(i) = 0$. Аналогично и для единиц. Т.е. $B \cup \{G_0(b)\}$ обладает (0,1) - свойством, но поскольку B - максимальное (0,1) - множество, то $G_0(b) \in B$.

Пусть $b_1, \dots, b_n \in B$, покажем что $f(b_1, \dots, b_n) \in B$. Пусть функция f имеет N состояний. Из определения (0,1)-свойства, следует, что существует счетное множество V_0 натуральных чисел такое, что все последовательности из B равны нулю на любом промежутке $[t - N, t]$ при $t \in V_0$. Каждому такому промежутку сопоставим компоненту 0-связности $K^0(t)$, в которой находится функция f в момент t при подстановке значений $b_1, \dots, b_n$ в качестве входных переменных. Ясно, что в этот момент текущее состояние функции f принадлежит ядру компоненты $K^0(t)$.

Пусть A^0 - компонента 0-связности, несохраняющая ноль. Пусть $A^0 = K^0(t_0)$ для некоторого $t_0 \in V_0$. По определению, существует $t_1 > t_0$ такое, что все последовательности из B равны единице на промежутке $[t_1 - N, t_1]$. Это означает что функция f в момент t_1 находится в одном из состояний ядра некоторой компоненты 1-связности A^1. Отсюда следует, что $A^0 \neq K^0(t)$ для любого $t > t_1$, иначе компоненты A^0 и A^1 были бы взаимосвязаны, что противоречит условию леммы. Следовательно, можно указать такое значение T_0, что функция f будет находится в компоненте 0-связности, сохраняющей ноль в любой момент времени, больший T_0.

Аналогично доказывается, что существует значение T_1 такое, что функция f будет находится в компоненте 1-связности, сохраняющей единицу в любой момент времени, больший T_1. Пусть $T = max(T_0, T_1)$

Покажем теперь, что $f(b_1, \dots, b_n) \in B$. Зафиксируем любое натуральное L. Из определения (0,1)-свойства следует, что существует $t > T$ такое, что все последовательности из B равны нулю на промежутке $[t, t + N + L]$. По доказанному ранее, на этом промежутке времени функция f находится в некоторой компоненте 0-связности, сохраняющей ноль. В момент $t + N$ функция будет находится в ядре этой компоненты, следовательно последовательность $f(b_1, \dots, b_n)$ равна нулю на промежутке $[t + N, t + N + L]$ (поскольку $b_1, \dots, b_n$ равны нулю на этом промежутке и текущая компонента 0-связности сохраняет ноль). Похожим образом доказывается, что найдется и некоторое значение t_1 такое, что все последовательности из B и $f(b_1, \dots, b_n)$ равны единице на промежутке $[t_1, t_1 + L]$. Следовательно, множество $B \cup \{f(b_1, \dots, b_n)\}$

обладает (0,1)-свойством. Из того, что B - максимальное (0,1)-множество, следует, что $f(b_1, \dots, b_n) \in B$.

Все функции системы M сохраняют множество B, следовательно, любая их суперпозиция тоже сохраняет это множество. Тогда истинностный ноль и истинностная единица не могут содержаться в $[M]$. $\square$

Сформулируем теперь основную теорему этого параграфа.

Теорема 2.11. *Пусть $M = P_0 \bigcup \{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n), G_0\}$, M А-полна. M содержит истинностную константу тогда и только тогда, когда хотя бы одна из функций $f_1, \dots, f_m$ имеет взаимосвязанные компоненты K^1, K^0 1- и 0-связности соответственно такие, что либо K^0 не сохраняет ноль, либо K^1 не сохраняет единицу.*

Справедливость теоремы следует из предыдущих лемм.

Таким образом, для проверки полноты системы M в этом случае, сначала нужно проверить выполнение условий теоремы 2.11. Если условия выполнены, переходим к случаю, когда M содержит константную функцию, который алгоритмически разрешим. Если условия не выполнены, то система не полна.

Случай, когда система M содержит единичную задержку абсолютно симметричен.

Пусть $\Omega^D(f)$ — совокупность всех подмножеств M множества P, содержащих Ω^D и о.-д. функцию f, таких, что множество $M \setminus \Omega^D$ конечно. Пусть о.-д. функции $G_0(x), G_1(x)$ — нулевая и единичная задержка соответственно. Обозначим $G = \{G_0(x), G_1(x)\}$.

Следовательно, справедливо следующее утверждение.

Теорема 2.12. *Пусть множество D содержит тождественную функцию а.-л. Тогда существует эффективный критерий распознавания полноты систем из $\Omega^D(g)$, где g принадлежит множеству G.*

2.5. Порождающее множество не содержит тождественную функцию

Пусть порождающее множество D не содержит тождественную функцию а.-л. Покажем, что тогда не существует алгоритма распознавания полноты систем из Ω^D.

Из строения решетки замкнутых классов Поста следует, что если порождающее множество не содержит тождественную функцию, то возможны только три P-множества: $P_{\{0\}}, P_{\{1\}}, P_{\{0,1\}}$. Первые два из них состоят только из одной о.-д. функции — тождественного нуля и единицы соответственно. Поскольку в P^2 не существует конечной полной системы относительно суперпозиции, то говорить об алгоритме распознавания полноты в этих случаях бессмысленно. Любая система из $\Omega^{\{1\}}$ или из $\Omega^{\{0\}}$ неполна. Третий случай — $P_{\{0,1\}}$ или автоматы Мура. Его стоит рассмотреть подробнее.

Следующая теорема показывает, что вопрос о существовании алгоритма имеет смысл в данном случае.

Теорема 2.13. *Среди систем о.-д. функций из $\Omega^{\{0,1\}}$ существуют полные и неполные системы.*

Доказательство. В качестве примера неполной системы рассмотрим

$$M_1 = P_{\{0,1\}} \cup \{0\}.$$

Очевидно, что M_1 принадлежит множеству автоматов Мура, поэтому она неполна.

Теперь приведем пример полной системы. Пусть $h(x_1, x_2)$ — истинностная о.-д. функция, в каждом состоянии которой реализуется штрих Шеффера. Рассмотрим систему

$$M_2 = P_{\{0,1\}} \cup \{h\}.$$

Покажем, что эта система полна. Для этого выберем произвольную о.-д. функцию $f(x_1, \dots, x_n)$ и покажем, что она выразима через систему M_2.

Пусть функция $f(x_1, \dots, x_n)$ имеет p состояний $q_1, \dots, q_p$. Построим p о.-д. функций $g_1(x_1, \dots, x_n), \dots, g_p(x_1, \dots, x_n)$. Множество состояний и функция переходов функции g_i такие же, как у функции f. Отличается только функция выхода, а именно, в состоянии q_i реализуется единица, а во всех остальных состояниях ноль. Таким образом, функция g_i определяет, находится ли функция f в состоянии q_i. Очевидно, g_i является автоматом Мура и, следовательно, принадлежит $P-$множеству $P_{\{0,1\}}$. Рассмотрим функцию а.-л. $a(x_1, \dots, x_n, y_1, \dots, y_p)$, которая определяется следующим образом:

$a(x_1, \dots, x_n, \alpha_1, \dots, \alpha_p) = F_{q_i}(x_1, \dots, x_n)$ при $\alpha_i = 1, \alpha_j = 0, i <> j$;

$a(x_1, \dots, x_n, \alpha_1, \dots, \alpha_p) = 0$ в противном случае.

Переменные $y_1, \dots, y_p$ являются управляющими, от их значений зависит, какая из функций F_{q_i} будет моделироваться на остальных переменных.

Пусть $A(x_1, \dots, x_n, y_1, \dots, y_p)$ — о.-д. функция, в каждом состоянии которой реализуется $a(x_1, \dots, x_n, y_1, \dots, y_p)$. Очевидно, ее можно выразить из $h(x_1, x_2)$. Рассмотрим суперпозицию

$$A(x_1, \dots, x_n, g_1(x_1, \dots, x_n), \dots, g_p(x_1, \dots, x_n)).$$

Несложно видеть, что выход этой суперозиции совпадает с выходом функции f на любых наборах данных. Функции $g_1, \dots, g_p$ "указывают", в каком состоянии находится функция f, а затем функция a реализует ту же самую функцию а.-л., которая в данный момент реализуется у f. Следовательно, функция f выразима через систему M_2. Поскольку, в качестве f была выбрана произвольная о.-д. функция, то система M_2 полна. □

С помощью модификации доказательства алгоритмической неразрешимости полноты конечных во множестве автоматных отображений, приведенного в [22], доказывается следующее утверждение.

Теорема 2.14. *Не существует алгоритма распознавания полноты систем из* $\Omega^{\{0,1\}}$.

Доказательство. Для доказательства неразрешимости полноты будем использовать понятие однородной системы продукций Поста [27]. Для каждой однородной системы продукций Поста можно поставить задачу о существовании алгоритма распознавания остановки этой системы. Оказывается, что существуют системы с неразрешимой проблемой остановки. Пусть $T_0 =< D_0, V_0, w_0 >$ — однородная система продукций Поста, для которой проблема остановки неразрешима.

Теперь перейдем к задаче о полноте о.-д. функций. Пусть $D_0 = \{d_1, \dots, d_k\}$. Закодируем буквы алфавита D_0 следующим образом:

$$d_i \to 1^i 0^{k-i+1} 1, i = 1, \dots, k.$$

Длина каждого кода равняется $k + 2$. Код буквы $a \in D_0$ будем обозначать через $\tilde{a}$. Если $A \in D_0^*, A = a_1 ... a_s$, через $\tilde{A}$ обозначим код слова A — набор $\tilde{a_1} ... \tilde{a_s}$.

Бесконечную последовательность α назовем правильной, если она представима в виде

$$\alpha = 0^n \alpha' 0^\infty,$$

где α' — код некоторого слова, $n \geq 0$.

Для каждого $i = 1, \dots, k$ рассмотрим о.-д. функцию $f_i(x)$, обладающая следующими свойствами:

1) если $a \in \{0, 1\}, a_1, \dots, a_l \in D_0, \beta = a 0^n \tilde{d_i} \tilde{a_1} ... \tilde{a_l} 0^\infty$ и $l >= w_0 - 1$, то $f_i(\beta) = a 0^{n + w_0(k+2)} \tilde{a_{w_0}} ... \tilde{a_l} \tilde{R_i} 0^\infty$, где $R_i \in D_0^*$ таково, что пара (d_i, R_i) принадлежит V_0;

2) если $a \in \{0, 1\}, a_1, \dots, a_l \in D_0, \beta = a 0^n \tilde{d_i} \tilde{a_1} ... \tilde{a_l} 0^\infty$ и $l < w_0 - 1$, то $f_i(\beta) = a 0^\infty$;

3)$f_i(a 0^\infty) = a 0^\infty$;

4) если β не представимо в виде $a 0^n \tilde{d_i} \tilde{a_1} ... \tilde{a_l} 0^\infty$ или в виде $a 0^n \tilde{d_i} \tilde{a_1} \tilde{a_2} ...$, то для некоторого t выполнено $f_i(\beta) = \gamma = \gamma(1)\gamma(2)...\gamma(t)111...$

Нетрудно видеть, что такие о.-д. функции существуют.

Рассмотрим еще две о.-д. функции — $f_y(x_1, x_2, x_3)$ и $f_H(x_1, x_2)$. Диаграммы Мура для этих функций представлены на рис. 2.5. Обозначим через $f_u(x_1, x_2)$ о.-д. функ-

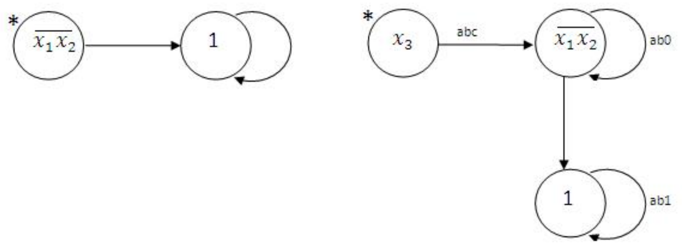

Рис. 2.5. Функции f_H(слева) и f_y(справа)

цию с одним состоянием, в котором реализуется функция а.-л. $\overline{x_1 \& x_2}$. Если на третий вход функции f_y подать сверхслово, отличное от $a0^\infty$, то через конечное время она перейдет в состояние, в котором реализуется единица, и больше оттуда уже не выйдет.

Заметим также, что если $f^0(x)$ — такая о.-д. функция, что для любых $a \in \{0,1\}, \gamma \in \{0,1\}^\infty$ имеет место $f^0(a\gamma) = a0^\infty$, то

$$f_u(x_1, x_2) = f_y(x_1, x_2, f^0(f_H(x_1, x_2))).$$

Наконец, пусть $\xi \in D_0^*$. Рассмотрим, о.-д. функцию $f_\xi(x)$, такую, что для любых $a \in \{0,1\}, \gamma \in \{0,1\}^\infty$ имеет место $f_\xi(a\gamma) = a\tilde{\xi}0^\infty$. Для произвольного $\xi \in D_0^*$ рассмотрим систему о.-д. функций

$$\Sigma_\xi = P_{\{0,1\}} \cup \{f_y(x_1, x_2, x_3), f_H(x_1, x_2), f_\xi(x), f_i(x), i = 1, \dots, k\}.$$

Покажем, что она является полной в P_2 относительно суперпозиции тогда и только тогда, когда система T_0-продукций слова ξ конечна.

а) Пусть множество T_0-продукций ξ конечно. Это означает, что последовательность T_0-продукций

$$\xi = \xi_1 \to \xi_2 \to ... \to \xi_s$$

обрывается на слове ξ_s, длина которого меньше w_0.

Пусть числа $j_i, i = 1, ...s$ выбраны таким образом, что начальная буква слова ξ_j есть буква d_{j_i}. Несложно видеть, что

$$f_{i_s}(f_{i_{s-1}}(...(f_{i_1}(f_\xi(x))...)) = f^0(x).$$

Поскольку $f_u(x_1, x_2) = f_y(x_1, x_2, f^0(f_H(x_1, x_2)))$, то функция $f_u(x_1, x_2)$ принадлежит замыкания системы Σ_ξ. Следовательно, по предыдущей теореме, она является полной.

б) Пусть система Σ_ξ полна. Тогда над ней можно построить схему S, котороая реализует $f_u(x_1, x_2)$. Пусть F — "последний" элемент в этой схеме, выход которого является выходом схемы S. Очевидно, что F не есть элемент $f_H, f_i, i = 1, ...k$ и f_ξ, поскольку во второй момент времени каждая из этих функций находится в состоянии, в котором реализуется константа. Следовательно, последним элементом является f_y. Будем строить последовательность элементов $e_1, e_2, ...$ схемы S, начиная с элемента F, т.е. $e_1 = F$. В качестве e_2 возьмем элемент, выход которого соединен с третьим входом e_1. Если это — элемент f_ξ, f_H или автомат Мура (т.е., принадлежит $P-$множеству $P_{\{0,1\}}$), закончим построение, если f_y, то e_3 — элемент, выход которого соединен с третьим входом e_2, если e_2 — один из элементов f_i, то e_3— элемент, выход которого соединен с входом e_2 и т.д. Очевидно, что эта последовательность конечна, поскольку схема S конечна, а операция обратной связи в рассматриваемой функциональной системе отсутствует.

Последовательность $e_1, e_2, ...$ не может оборваться на элементе f_H, поскольку в этом случае на выходе всей схемы реализуются только последовательности, оканчивающиеся бесконечным сверхсловом из единиц. Также она не может оборваться на элементе из $P_{\{0,1\}}$, поскольку тогда у всей схемы в первый момент времени будет реализовываться константа. Следовательно, последовательность $e_1, e_2, ...$ оканчивается на элементе f_ξ, либо вход последнего элемента является входом схемы S. В последнем случае, подавая на этот вход последовательность 1^∞, на выходе схемы получим последовательность, оканчивающуюся на сверхслово 1^∞. Это противоречит тому, что схема S реализует функцию $f_u(x_1, x_2)$. Осталось рассмотреть один случай — когда цепочка $e_1, e_2, ...$ оканчивается элементом f_ξ. Тогда, пройдя вниз по этой цепочки, начиная с f_ξ, получим суперпозицию

$$g(x) = f_{i_s}(f - i_{s-1}(...f_{i_1}(f_\xi))...)).$$

Нетрудно видеть, что функция $g(x)$ совпадает с $f^0(x)$, поскольку в противном случае на выходе схемы S реализуется сверхслово, оканчивающе на бесконечное число единиц. Далее, из равенства $g(x) = f^0(x)$ следует, что множество T_0-продукций слова ξ конечно.

Из приведенных выше рассуждений следует, что задача об остановке в T_0 может быть сведена к задаче о полноте системы Σ_ξ. Система продукций T_0 была выбрана таким образом, что проблема остановки для нее алгоритмически неразрашима. Отсюда следует неразрешимость полноты системы Σ_ξ.

□

2.6. Эффективный критерий А-выразимости для систем, содержащих $P-$множества

Наряду с задачей о полноте, интерес представляет и более общая (и более сложная) задача о выразимости. Будем говорить, что о.-д. функция f выразима через систему M, если $f \in [M]$. Аналогично, о.-д. функция f А-выразима через систему M тогда и только тогда, когда $f \in A[M]$.

Исследуем вопрос о том, в каких случаях существует эффективный критерий выразимости для систем, принадлежащих совокупности Ω^D. Требуется построить алгоритм, который по произвольной о.-д. функции f и по системе $M \in \Omega^D$ должен определить, выразима ли f через M. Либо нужно установить, что для данного D такого критерия не существует. Аналогично ставится и задача об А-выразимости.

Теорема 2.15. *Пусть множество функций а.-л. D содержит тождественную функцию и обе константы, тогда существует эффективный критерий А-выразимости для систем, принадлежащих совокупности Ω^D.*

Доказательство этой теоремы конструктивно, т.е. алгоритм распознавания выразимости построен. Для формулировки критерия потребуется ввести еще несколько определений.

Рассмотрим произвольную о.-д. функцию f. Обозначим через $Q = \{q_0, q_1, \dots, q_p\}$ – множество ее состояний, где q_0 – начальное состояние. Функцию алгебры-логики, реализуемую в состоянии q_i обозначим через F_{q_i}. Обозначим через $Q(t)$ подмножество Q, состоящее из всех состояний, t-достижимых из начального. Пусть

$$F_{Q(t)} = \bigcup_{q \in Q(t)} \{F_q\}.$$

Рассмотрим периодическую последовательность множеств состояний функции f:

$$Q(0), Q(1), Q(2)...$$

Пусть T — длина ее предпериода, s – длина периода. Для функции f построим характеристическую последовательность множеств функций а.-л.:

$$\Psi^f = ([F_{Q(0)}], [F_{Q(1)}], \dots).$$

Из вышесказанного следует, что число различных элементов в этой последовательности конечно и она также периодична, T является предпериодом, а s — периодом (возможно, кратным). Через $\Psi^f(t)$ будем обозначать элемент последовательности с номером t, т.е. $[F_{Q(t)}]$.

Пусть теперь $M = P_D^2 \bigcup \{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\}$.

Пусть

$$Q^M(t) = Q^{f_1}(t) \cup \dots \cup Q^{f_m}(t),$$

$$F^M_{Q(t)} = F_{Q^{f_1}(t)} \cup \dots \cup F_{Q^{f_m}(t)}.$$

Построим характеристическую последовательность для M:

$$\Psi^M = ([F_{Q^M(0)} \cup D], [F_{Q^M(1)} \cup D], \dots).$$

Несложно видеть что у любой функции $g \in [M]$ в момент времени t достижимы только такие состояния, в которых реализуются функции а.-л. из $[F_{Q^M(t)} \cup D]$. Справедлива следующая теорема.

Теорема 2.16. *Пусть порождающее множество D содержит тождественную функцию а.-л. и обе константы (0 и 1). Пусть $M = P_D^2 \bigcup \{f_1, \dots, f_m\}$. Тогда о.-д. функция f А-выразима через систему M тогда и только тогда, когда $\Psi^f(t) \subseteq \Psi^M(t)$ для любых t.*

Поскольку характеристические последовательности периодичны, осуществить проверку выполнения условий теоремы можно за конечное число операций, т.е. критерий является алгоритмом.

Доказательство этой теоремы почти дословно повторяет доказательство леммы 2.4. Если условия теоремы выполнены, то с помощью механизма, описанного в доказательстве леммы 2.4, может быть построена функция f. В противном случае, как несложно видеть, функция f не является А-выразимой из M.

Глава 3

Полные системы в $P-$множествах

Очевидно, $P-$множество можно рассматривать, как самостоятельную функциональную систему, и тогда возникает ряд стандартных для функциональных систем задач. В [22] показано, что в $(P^2)_\Sigma$ существует полная система, не содержащая базиса, вместе с тем, в $(P^2)_\Sigma$ можно выделить базис. С этой точки зрения интерес представляет аналогичная задача для функциональной системы $(P^2_D)_\Sigma$, порожденной произвольным множеством D.

3.1. Порождающее множество содержит обе константы

Пусть D— замкнутый класс а.-л., содержащий тождественную функцию и обе константы. Рассмотрим вопрос о существовании базиса в $(P^2_D)_\Sigma$. Понятно, что конечного базиса не существует, поскольку в противном случае существовал бы конечный базис и в P^2. Следовательно, если базис в $(P^2_D)_\Sigma$ существует, то он бесконечный.

Теорема 3.1. *Пусть $0, 1 \in D$. Тогда в $(P^2_D)_\Sigma$ существует полная система, не содержащая базиса.*

Доказательство. Пусть $\rho = \{\rho_1,\ ..., \rho_d\}$ — множество функций а.-л., которое является базисом в D. Согласно [30], такой базис всегда можно эффективно построить. Обозначим через $R = \{R_1,\ ..., R_d\}$ множество о.-д. функций с одним состоянием, таких, что в состоянии функции R_i реализуется функция а.-л. ρ_i. Очевидно, что тождественные 0 и 1 принадлежат замыканию R.

Зафиксируем произвольное натуральное число m и рассмотрим произвольные 2^m о.-д. функций. Пусть в совокупности они зависят от переменных $x_1,\ ..., x_n$. Каждой функции можно взаимнооднозначно сопоставить двоичный набор длины m. Т.е. в качестве номера функции будем рассматривать значение этого набора. Обозначим эти о.-д. функции через $f_{00..0},\ ..., f_{11..1}$.

Рассмотрим схему, изображенную на рис. 3.1., которая реализует некоторую о.-д. функцию $h(x_1,\ ..., x_n, y_1,\ ..., y_m, z)$. В блоках, обозначенных $F_{00..0},\ ..., F_{11..1}$, реализуются о.-.д функции $f_{00..0},\ ..., f_{11..1}$ соответственно. В блоке M_α, где α — двоичный набор длины m, реализуется такая о.-д. функция, что ее значение в первый момент времени равно 1 тогда и только тогда, когда двоичный набор значений входных переменных в первый момент времени равен α, т.е. $(y_1(1),\ ..., y_m(1)) = \alpha$. Выход функции в блоке M_α в остальные моменты времени всегда равен 0. Блок M_x реализует о.-д. функцию от одной переменной, которая пропускает значение переменной в первый момент времени и выдает 0 во все последующие моменты. В блоках, обозначенных $\vee$, реализуется дизъюнкция, в блоках & — конъюнкция, в блоках G_0 — нулевая задержка.

Пусть в первый момент времени набор входных переменных $(y_1(1),\ ..., y_m(1))$ принимает значение α. Это означает, что на выходе блока M_α реализуется единица в первый момент времени, а выход всех остальных блоков $M_\beta, \beta \neq \alpha$ равен нулю в первый момент. Следовательно, в первый момент времени на выходе схемы появляется значение $z(1)$, а в остальные моменты на входы последней дизъюнкции подается только одно значение, отличное от тождественного нуля, это значение функции f_α. Таким образом, начиная со второго момента времени, функция h "работает"как одна из функций $f_{00..0},\ ..., f_{11..1}$. Какая конкретно функция получится, зависит от значений переменных $y_1,\ ..., y_m$ в первый момент времени.

Проверим, что $h \in P_D$. Для это нужно рассмотреть функции а.-л., которые реализуются в состояниях h. В первый момент реализуется z — тождественная функция а.-л. Во все остальные моменты реализуется функция а.-л., которая также реализуется в одном из состояний о.-.д функции f_α, которая принадлежит P_D. Следовательно, h также принадлежит P_D.

Покажем, что $f_{00..0},\ ..., f_{11..1} \in [h \cup R]$. Рассмотрим произвольную функцию f_α. Пусть в начальном состоянии f_α реализуется функция а.-л. $a(x_1,\ ..., x_n)$. Пусть $A(x_1,\ ..., x_n)$ — о.-д. функция с одним состоянием, в котором реализуется a. Пусть

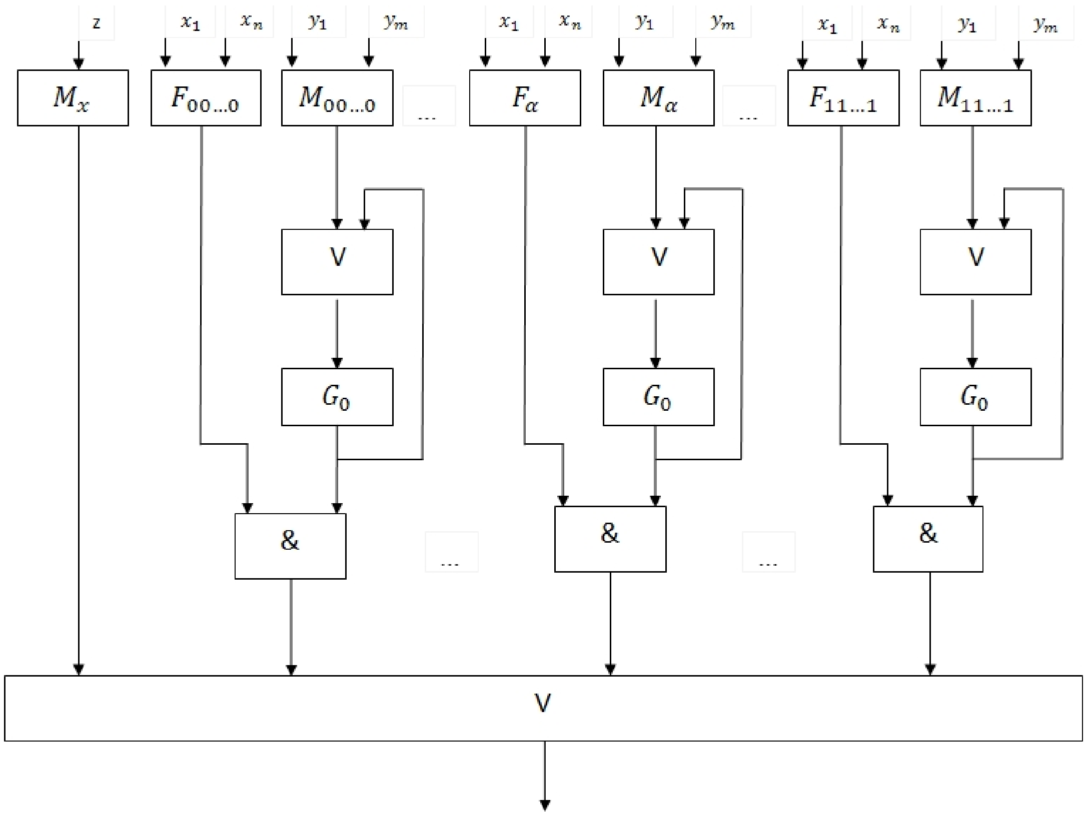
z
x_1
x_n
y_1
y_m
x_1
x_n
y_1
y_m
x_1
x_n
y_1
y_m
M_x
$F_{00\dots0}$
$M_{00\dots0}$
...
F_α
M_α
...
$F_{11\dots1}$
$M_{11\dots1}$
V
V
V
G_0
G_0
G_0
&
...
&
...
&
V

Рис. 3.1.

C_i — тождественный ноль, если i-й разряд набора α равен 0, и C_i — тождественная единица в противном случае, $i \in \{1, \ ..., m\}$. Очевидно, $A, C_i \in R$. Рассмотрим суперпозицию

$$h(x_1, \ ..., x_n, C_1, \ ..., C_m, A(x_1, \ ..., x_n)).$$

Из определения функции h следует, что выход такой суперпозиции совпадает с выходом f_α в любой момент времени.

Функцию h будем называть генератором для функций $f_{00..0}, \ ..., f_{11..1}$.

Перенумеруем некоторым образом все функции из $P_D \backslash R$. Это можно сделать, поскольку P_D содержит счетное число функций. Построим нумерацию таким образом, чтобы для любого натурального $m > 0$ функция с номером $2^m + 1$ являлась генератором для всех функций с номерами, не превосходящими 2^m. Будем обозначать функцию с номером $2^m + 1$ через h_m. Рассмотрим бесконечную систему функций

$$N = R \bigcup_{i \geq 1} \{h_i\}.$$

Очевидно, система N полна. Предположим, из нее можно выделить базис. Функции из R обязательно должны присутствовать в базисе, поскольку все функции h_m пропускают значение переменной z в первый момент времени. Поскольку базис не может быть конечным, в нем присутствуют хотя бы две функции $h_i, h_j, i < j$. Но, по построению, $h_i \in [R \cup h_j]$. Следовательно, функцию h_i можно исключить из базиса без потери свойства полноты. Следовательно, это не базис. Теорема доказана. $\square$

В [22](стр. 175-178) приведен пример базиса в P относительно суперпозиции. Покажем, что конструкция, описанная там, с некоторыми модификациями переносится и на рассматриваемый случай. Для этого нам понадобится понятие F-свойства, введенное в [20].

Пусть $f(x_1, \dots, x_n)$ — о.-д. функции из P_D. Будем считать, что переменная x_i функции f обладает F-свойством на сверхслове γ, если существуют момент времени

t_0 такой, что для любых сверхслов $b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_n$ значение

$$b = f(b_1, \dots, b_{i-1}, \gamma, b_{i+1}, \dots, b_n)$$

таково, что $\gamma(t) = b(t)$ для любого $t > t_0$.

Иначе говоря, если подать сверхслово γ на i-й вход функции f, она постепенно превратится в проводник и будет пропускать переменную x_i.

Введенное понятие позволяет кодировать автомат с помощью ключа, которым является бесконечная последовательность (сверхслово). Периодическое сверхслово можно рассматривать как константную о.-д. функцию. Очевидно, что все константные функции принадлежат P_D, поскольку в каждом состоянии константной о.-д. функции реализуется либо 0, либо 1, и $0, 1 \in D$.

Лемма 3.1. *Пусть $f(x_1, \dots, x_n)$ — о.-д. функция из P_D, γ — сверхслово. Существует о.-д. функция $f(x_1, \dots, x_n, z) \in P_D$ такая, что выполнены следующие условия:*

1) $f'(x_1, \dots, x_n, \gamma) = f(x_1, \dots, x_n)$;

2) Переменная z функции h обладает F-свойстом на любой последовательности, отличной от γ.

Доказательство. Рассмотрим следующую схему, реализующую f'. Здесь символом ρ отмечена подсхема, реализующая истинностную о.-.д. функцию, в состояниях которой реализуется функция а.-л. $\rho(x_1, x_2) = x_1 x_2 \vee \bar{x_1} \bar{x_2}$, символом & обозначена конъюнкция, а символом v функция $v(x_1, x_2, x_3) = x_1 x_3 \vee x_2 \bar{x_3}$, G_1 — единичная задержка, γ — константная о.-д. функция, реализующая бесконечную последовательность γ.

До тех пор, пока на вход z поступает последовательность γ, на третий вход блока v будет поступать 1, и на выходе системы будет реализовываться значение функции f. Таким образом, первое условие выполнено.

Пусть на вход z подается последовательность γ', отличная от $\gamma, \gamma'(t_0) \neq \gamma(t_0)$. Тогда на третий вход блока v будет поступать значение 0 в любой момент времени, больший t_0. Отсюда следует, что на выходе схемы будет реализовываться последо-

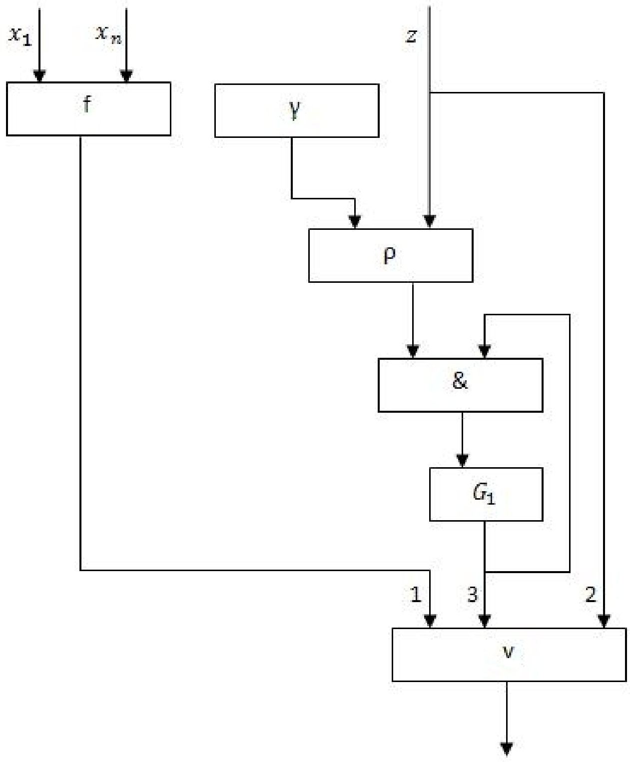

Рис. 3.2.

вательность, отличная от γ' лишь в конечном числе разрядов, что означает справедливость второго условия.

Осталось проверить, что функция f', построенная таким образом, принадлежит P_D. Действительно, если на третий вход блока v поступает значение 1, то на выход функции f' поступает значение f в этот момент времени. Функция а.-л., реализуемая в состоянии функции f, принадлежит D, поскольку $f \in P_D$. Если на третий вход блока v поступает значение 0, то функция f' находится в состоянии, в котором реализуется либо 0, либо 1. Т.е., у функции f' достижимы только те состояния, в которых реализуются функции из D. Лемма доказана. $\square$

Будем писать $h = K(f, \gamma)$, если h кодирует f с помощью ключа γ.

Теорема 3.2. *Пусть* $0, 1 \in D$. *Тогда в* P_D *существует базис.*

Доказательство. Для построения базиса рассмотрим систему $N = R \cup \{h_1, h_2 ...\}$, описанную в доказательстве теоремы 3.1. Обозначим через Z_i замыкание множества $R \cup \{h_i\}, i > 0$, через Z_0 обозначим $[R]$.

Пусть Z — конечное множество о.-д. функций. Выберем из этого множества о.-д. функцию, имеющую наибольшее число состояний и обозначим это число через $n(Z)$. Пусть H_n — множество всех периодических последовательностей, у которых длины периодов образуют множество чисел, представимых в виде $p_1^{s_1} p_2^{s_2} ...\ p_m^{s_m}$, где все $p_j, j = 1, ... , m$ — простые числа, не превосходящие n. Рассмотрим цепочку вложенных множеств

$$Z_0 \subseteq Z_1 \subseteq Z_2 \subseteq ...$$

Несложно видеть, что из этой цепочки можно выделить бесконечную подцепочку

$$Z_0 \subseteq Z_{i_1} \subseteq Z_{i_2} \subseteq ...$$

такую, что для любого натурального j во множестве $Z_{i_j} \setminus Z_{i_{j-1}}$ содержится хотя бы одна константная о.-д. функция C_{i_j}, период которой является простым числом, превосходящим $n(Z_{i_{j-1}})$.

Очевидно, что система $N' = R \cup \{h_{i_1}, h_{i_2}...\}$ также полна. Рассмотрим систему

$$N'' = R \cup \{K(h_{i_1}, C_0), K(h_{i_2}, C_{i_1}), \dots, K(h_{i_{j+1}}, C_{i_j})...\},$$

где C_0 — тождественный ноль. Она также полна, поскольку через нее выразима система N'. Покажем, что N'' является базисом. Никакую функцию из R нельзя исключить без потери свойства полноты, поскольку все функции, не принадлежащие R пропускают значение одной из входных переменных в первый момент времени. Рассмотрим множество

$$N''_j = R \cup \{K(h_{i_1}, C_0), K(h_{i_2}, C_{i_1}), \dots, K(h_{i_j}, C_{i_{j-1}})\}.$$

По построению, оно сохраняет множество бесконечных последовательностей $H_{n(Z_j)}$. С другой стороны, любая функция $K(h_{i_{k+1}}, C_{i_k}), k > j$ также сохраняет $H_{n(Z_j)}$. Поэтому $N'' \setminus K(h_{i_{j+1}}, C_{i_j})$ неполна для любого j. Следовательно, N'' является базисом. $\square$

3.2. Порождающее множество содержит тождественную функцию и отрицание

Пусть теперь D— замкнутый класс а.-л., содержащий тождественную функцию и обе константы. Покажем справедливость аналогичных результатов для данного случая.

Теорема 3.3. *Пусть порождающее множество D содержит тождественную функцию а.-л. и отрицание. Тогда в P_D существует полная система, не содержащая базиса.*

Доказательство. Пусть $\rho = \{\rho_1, \dots, \rho_d\}$ — множество функций а.-л., которое является базисом в D. Обозначим через $R = \{R_1, \dots, R_d\}$ множество о.-д. функций с одним состоянием, таких, что в состоянии функции R_i реализуется функция а.-л. ρ_i. Очевидно, что тождественное отрицание принадлежат замыканию R.

Зафиксируем произвольное натуральное число m и рассмотрим произвольные 2^m о.-д. функций. Пусть в совокупности они зависят от переменных $x_1,\ ...,x_n$. Каждой функции можно взаимнооднозначно сопоставить двоичный набор длины m. Т.е. в качестве номера функции будем рассматривать значение этого набора. Обозначим эти о.-д. функции через $f_{00..0},\ ...,f_{11..1}$.

Рассмотрим схему, изображенную на рис. 3.2., которая реализует некоторую о.-д. функцию $h(x_1,\ ...,x_n,y_1,\ ...,y_{2m},z)$. В блоках, обозначенных $F_{00..0},\ ...,F_{11..1}$, реализуются о.-.д функции $f_{00..0},\ ...,f_{11..1}$ соответственно. В блоке M_α, где $\alpha=(\alpha_1,\ ...,\alpha_m)$ — двоичный набор длины m, реализуется такая о.-д. функция, что ее значение в первый момент времени равно 1 тогда и только тогда, когда двоичный набор значений входных переменных в первый момент времени удовлетворяет следующим условиям:

$$y_1(1)+y_2(1)=\alpha_1,\ ...,y_{2m-1}(1)+y_{2m}(1)=\alpha_m.$$

Выход функции в блоке M_α в остальные моменты времени всегда равен 0. Блок M_x реализует о.-д. функцию от одной переменной, которая пропускает значение переменной в первый момент времени и выдает 0 во все последующие моменты. В блоках, обозначенных $\vee$, реализуется дизъюнкция, в блоках & — конъюнкция, в блоках G_0 — нулевая задержка.

Пусть в первый момент времени двоичный набор $(y_1(1)+y_2(1),\ ...,y_{2m-1}(1)+y_{2m}(1))$ принимает значение α. Это означает, что на выходе блока M_α реализуется единица в первый момент времени, а выход всех остальных блоков $M_\beta,\beta\neq\alpha$ равен нулю в первый момент. Следовательно, в первый момент времени на выходе схемы появляется значение $z(1)$, а в остальные моменты на входы последней дизъюнкции подается только одно значение, отличное от тождественного нуля, это значение функции f_α. Таким образом, начиная со второго момента времени, функция h "работает"как одна из функций $f_{00..0},\ ...,f_{11..1}$. Какая конкретно функция получится, зависит от значений переменных $y_1,\ ...,y_{2m}$ в первый момент времени.

Проверим, что $h\in P_D$. Для это нужно рассмотреть функции а.-л., которые реа-

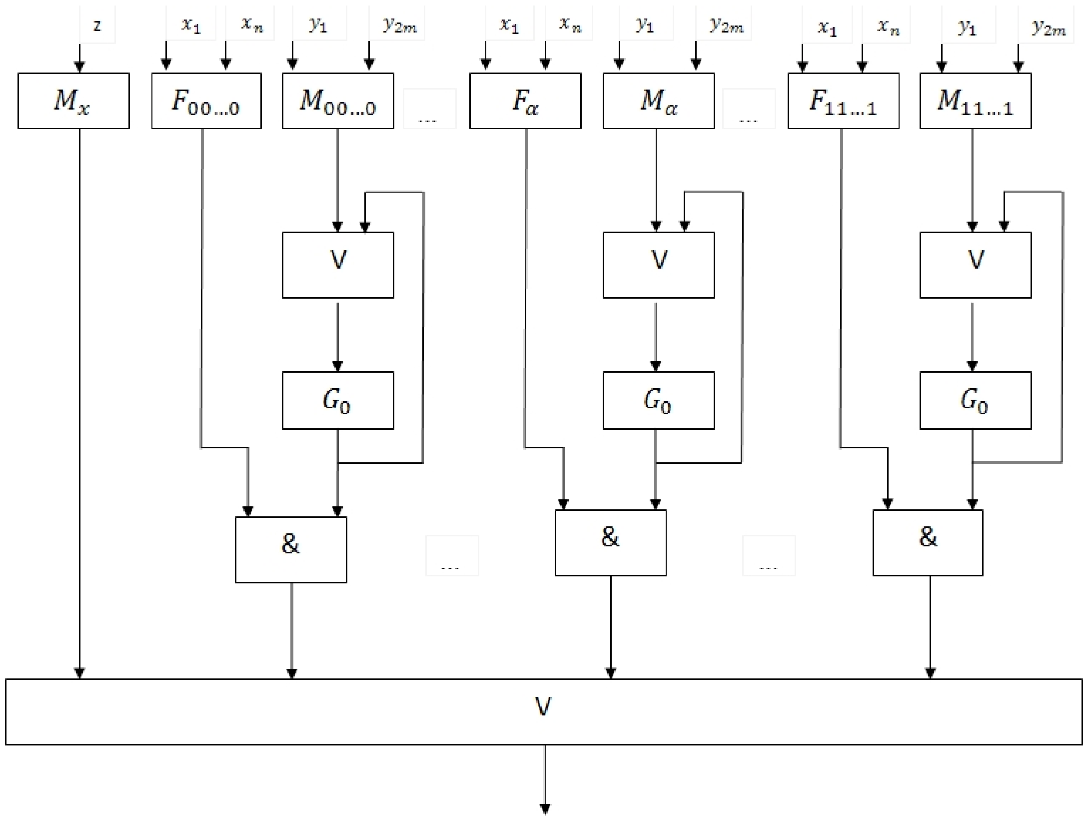
z
x_1
x_n
y_1
y_{2m}
x_1
x_n
y_1
y_{2m}
x_1
x_n
y_1
y_{2m}
M_x
$F_{00\ldots0}$
$M_{00\ldots0}$
…
F_α
M_α
…
$F_{11\ldots1}$
$M_{11\ldots1}$
V
V
V
G_0
G_0
G_0
&
…
&
…
&
V

Рис. 3.3.

лизуются в состояниях h. В первый момент реализуется z — тождественная функция а.-л. Во все остальные моменты реализуется функция а.-л., которая также реализуется в одном из состояний о.-.д функции f_α, которая принадлежит P_D. Следовательно, h также принадлежит P_D.

Покажем, что $f_{00..0},\ ..., f_{11..1} \in [h \cup R]$. Рассмотрим произвольную функцию f_α. Пусть в начальном состоянии f_α реализуется функция а.-л. $a(x_1,\ ..., x_n)$. Пусть $A(x_1,\ ..., x_n)$ — истинностная о.-.д функция, в состоянии которой реализуется a. Пусть о.-д. функции $\varphi_1(x),\ ..., \varphi_{2m}(x)$ определяются следующим образом: $\varphi_{2i-1}(x) = \varphi_{2i}(x) = x$, если i-й разряд набора α равен 0, и $\varphi_{2i-1}(x) = x, \varphi_{2i}(x) = \overline{x}$, если i-й разряд набора α равен 0, $i \in \{1,\ ..., m\}$. Очевидно, $A, h_j \in R$. Рассмотрим суперпозицию

$$h(x_1,\ ..., x_n, \varphi_1(x),\ ..., \varphi_{2m}(x), A(x_1,\ ..., x_n)).$$

Из определения функции h следует, что выход такой суперпозиции совпадает с выходом f_α в любой момент времени.

Функцию h будем называть генератором для функций $f_{00..0},\ ..., f_{11..1}$.

Обозначим через S_n множество всех о.-д. функций из P_D, зависящих не более чем от n переменных и имеющих при этом не более n состояний. Количество таких функций конечно, поэтому для каждого множества S_n можно построить генератор h_n.

Рассмотрим бесконечную систему функций

$$N = R \bigcup_{i \geq 1} \{h_i\}.$$

Очевидно, система N полна. Предположим, из нее можно выделить базис. Функции из R обязательно должны присутствовать в базисе, поскольку все функции h_m пропускают значение переменной z в первый момент времени. Поскольку базис не может быть конечным, в нем присутствуют хотя бы две функции h_i, h_j такие, что j превосходит и количество переменных, и количество состояний функции h_i. Тогда, по построению, $h_i \in [R \cup h_j]$. Следовательно, функцию h_i можно исключить из базиса без потери свойства полноты. Следовательно, это не базис. Теорема доказана. $\square$

Для доказательства существования базиса этого нам понадобится обобщение F-свойства. Кодировать автоматы с помощью константных о.-д. функций уже не получится, поскольку они могут не принадлежать Р-множеству P_D. Поэтому в качестве ключа будем использовать о.-д. функции, зависящие от одной переменной.

Пусть $f(x_1, \dots, x_n), \varphi(x)$ — о.-д. функции из P_D. Рассмотрим о.-д. функцию $f'(x_1, \dots, x_n, y_1, y_2)$, которая реализуется представленной ниже схемой. Здесь символом ρ отмечена подсхема, реализующая истинностную о.-.д. функцию, в состояниях которой реализуется функция а.-л. $\rho(x_1, x_2) = x_1x_2 \vee \bar{x_1}\bar{x_2}$, символом & обозначена конъюнкция, а символом v функция $v(x_1, x_2, x_3) = x_1x_3 \vee x_2\bar{x_3}$, G_1 — единичная задержка, ϕ — о.-д. функция $\varphi(x)$.

Если на вход y_2 подавать значение $\varphi(y_1)$ в каждый момент времени, то на третий вход блока v всегда будет поступать 1, и на выходе системы будет реализовываться значение функции f. Если окажется, что значения последних двух входов не удовлетворяют условию $\varphi(y_1) = y_2$, на третий вход блока v будет поступать 0 и он начнет пропускать значение входа y_2.

Проверим, что функция f', построенная таким образом, принадлежит P_D. Действительно, если на третий вход блока v поступает значение 1, то на выход функции f' поступает значение f в этот момент времени. Функция а.-л., реализуемая в состоянии функции f, принадлежит D, поскольку $f \in P_D$. Если на третий вход блока v поступает значение 0, то на выход функции f' поступает значение φ в этот момент времени. Т.е., у функции f' достижимы только те состояния, в которых реализуются функции из D.

Будем говорить, что построенная таким образом функция f' кодирует f с помощью ключа φ и обозначать через $K(f, \varphi)$.

Замечание. *В некоторых случаях не обязательно иметь ключ, для того, чтобы "раскодировать"о.-д. функцию. Например, пусть f' кодирует некоторую о.-д. функ-*

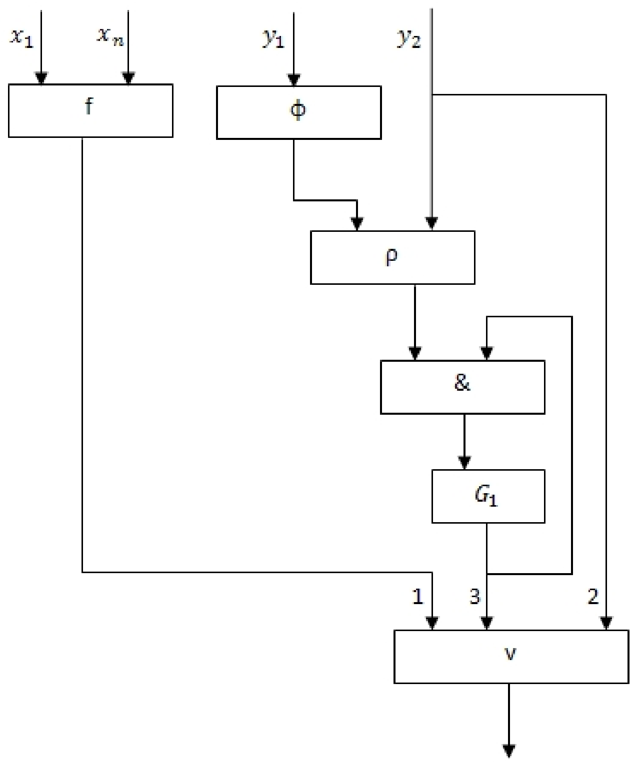

Рис. 3.4.

цию f, где в качестве ключа выступает тождественное отрицание. Для того, чтобы ее "раскодировать"достаточно подставить в последние два входа функции f' тождественные 0 и 1, при этом не обязательно иметь отрицание. Для того, чтобы "взломать"функцию, достаточно подавать на последние два входа значения, удовлетворяющие условию $\varphi(y_1) = y_2$.

Теорема 3.4. *Пусть порождающее множество D содержит тождественную функцию а.-л. и отрицание. Тогда в P_D существует базис.*

Доказательство. Для построения базиса рассмотрим систему $N = R \cup \{h_1, h_2...\}$, описанную в доказательстве предыдущей теоремы. Выделим из нее бесконечную подсистему $N' = R \cup \{h_{p_1}, h_{p_2}...\}$, где $p_1, p_2, ...$ — последовательность всех простых чисел, упорядоченная по возрастанию. Очевидно, N' также полна.

Пусть p — простое число. Обозначим через $g_p(x)$ такую о.-д. функцию, что $g_p(x(t)) = \overline{x(t)}$, если t кратно p и $g_p(x(t)) = x(t)$ в противном случае. Очевидно, g_p имеет p состояний, поэтому $g_p \in R \cup \{h_p\}$. Пусть H_n — множество всех периодических последовательностей, у которых длины периодов образуют множество чисел, представимых в виде $p_1^{s_1} p_2^{s_2} ... \, p_m^{s_m}$, где все p_j, $j = 1, \dots , m$ — простые числа, не превосходящие n.

Рассмотрим систему

$$N''_j = R \cup \{K(h_{p_1}, g_1), K(h_{p_2}, g_{p_1}), \dots , K(h_{p_j}, g_{p_{j-1}})...\},$$

которая также полна. Покажем, что она является базисом.

Никакую функцию из R нельзя исключить без потери свойства полноты, поскольку все функции, не принадлежащие R пропускают значение одной из входных переменных в первый момент времени.

Рассмотрим множество

$$N''_j = R \cup \{K(h_{p_1}, g_1), K(h_{p_2}, g_{p_1}), \dots , K(h_{p_j}, g_{p_{j-1}})\}.$$

По построению, оно сохраняет множество бесконечных последовательностей H_{p_j}. С другой стороны, любая функция $K(h_{p_{k+1}}, g_{p_k}), k > j$ также сохраняет H_{p_j}. Поэтому, $N'' \setminus K(h_{p_{j+1}}, g_{p_j})$ неполна для любого j. Следовательно, N'' является базисом.

$\square$

Список литературы

1. Kleene S. C. Introduction to Metamathematics, North-Holland, 1952.
2. Lo Czu-Kai. Precomplete classes defined by normal k-ary relations of functions preserving a partition // Acta. Sci. Natur. Univer. Jilinensis. — 1964. — V.3. — P. 39-50 (Chinese).
3. Moore E. F. Gedanken-experiments on Sequential Machines. Automata Studies, Annals of Mathematical Studies, 34, 129–153. Princeton University Press, Princeton, 1956.
4. Post E. The two-valued iterative systems of mathematical Logic. Princeton Univ. Press, Princeton, 1941.
5. Rosenberg J. La structure des fonctions de plusiers variables sur un ensemble fini. Comptes Rendus Acad. Sei. Paris, 1965 №260, c.3817-3819.
6. Turing A.M. Computing machinery and intelligence. Mind, 59, 433-460, 1950.
7. Автоматы, сборник статей. Под редакцией К.Э.Шеннона и Дж. Маккарти. Изд-во инностранной литературы, 1956.
8. Алешин С.В. Über ein Vollstänig klits kriterium für Automatenabildungen beruglich der Superposition // Rostoker Math. Kolloq. 1977. **5**. 119-132.
9. Бабин Д. Н. Разрешимый случай задачи о полноте автоматных функций. Москва, Дискретная математика, 1992. Т. 4, вып. 4. с. 41-56.
10. Бабин Д. Н. О классификации автоматных базисов Поста по разрешимости свойств полноты и А-полноты // Доклады Академии наук. №4. Т. 367. 1999. С. 439-441.
11. Буевич В.А. Об алгоритмической неразрешимости распознавания $A-$полноты для о.-д. функций. М.: Мат. заметки, 1972, вып. 6, с. 687-697.
12. Буевич В.А. Построение универсальной о.-д. функции от двух входных переменных // Проблемы кибернетики. М.: Наука, 1965, вып. 15, с. 241-245.

13. Буевич В. А. О т-полноте в классе автоматных отображений. Москва, ДАН СССР, т. 252. №5. 1980.
14. Буевич В. А. Условия А-полноты для конечных автоматов, ч.1, ч.2. Издательство МГУ, 1986, 1987 г.г.
15. Буевич В. А. Вариант доказательства критерия полноты для функций k-значной логики, Дискретная математика, 1996, 8, выпуск 4.
16. Буевич В.А. Критерий полноты систем, содержащих все одноместные ограниченно-детерминированные функции, Дискретная математика, 2000, 12, выпуск 4.
17. Жук Д.Н. О классификации автоматных базисов Поста по разрешимости свойств А-полноты для дефинитных автоматов. *Дискретная математика*, **22**:2 (2010), 80-95.
18. Кратко М.И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов. М.: ДАН СССР, 1964, т.155, №1.
19. Кудрявцев В.Б. О мощности множеств предполных классов некоторых функциональных систем, связанных с автоматами. М.: ДАН СССР, 1963, т.151, №3.
20. Кудрявцев В.Б. О мощности множеств предполных множеств некоторой функциональной системы, связанной с автоматами // Проблемы кибернетики. Вып. 13 М.: Физматгис, 1965. 45-74.
21. Кудрявцев В.Б. Функциональные системы. М. Изд-во МГУ, 1982.
22. Кудрявцев В.Б., Алешин С.В., Подколзин А.С. Введение в теорию автоматов. М.: Наука, 1985.
23. Кузнецов А. В. О проблемах тождества и функциональной полноты для алгебраических систем. Труды третьего всесоюзного математического съезда. Т. 2. Москва. Изд. АН СССР, 1956, с.145-146.
24. Кузнецов А.В. Математика в СССР за 40 лет. М., 1959, т.1, §13, с.102-115.

25. Кузнецов А. В. Структуры с замыканием и критерии функциональной полноты. Успехи математических наук. Т. 16, №2, 1961, с.201-202.

26. Летичевский А. А. Условия полноты в классе автоматов Мура. В кн.: Материалы научных семинаров по теоретическим и прикладным вопросам кибернетики, вып. 2, Киев, 1963.

27. Мальцев А.И. Алгоритмы и рекурсивные функции. М.: Наука, 1965.

28. Мальцев А.И. Итеративные алгебры Поста. Новосибирск, изд-во СО АН СССР, 1976.

29. Марченков С.С. О классах Слупецкого для детерминированных функций *Дискретная математика*, **10**:2 (1998).

30. Угольников А.Б. Классы Поста. Изд-во ЦПИ при мех.-мат. ф-те МГУ, 2008.

31. Часовских А. А. О полноте в классе линейных автоматов. Математические вопросы кибернетики. Вып. 3. 1995, с. 140-166.

32. Яблонский С.В. Функциональные построения в к-значной логике. Труды Матем. института им. В.А. Стеклова(1958) 51, 5-142.

33. Яблонский С.В. Введение в дискретную математику. Наука, Москва, 1986.

34. Яблонский С.В., Гаврилов Г.П., Кудрявцев В.Б. Функции алгебры логики и классы Поста. М.: Наука, 1966.

35. Янов Ю.И., Мучник А.А. О существовании k-значных замкнутых классов, не имеющих конечного базиса. М.: ДАН СССР, 1959, т.127, №1.

Публикации автора по теме диссертации

36. Родин А. А. О континуальности множества специальных предполных классов во множестве автоматных отображений. *Интеллектуальные системы.* (2012) **16**, 329-334.

37. Родин А. А. О некоторых свойствах $P-$множеств ограниченно-детерминированных функций. *Вестник Московского университета. Сер. 1, Математика. Механика.* 2013. №1. С. 51-53.

38. Родин А. А. Критерий полноты некоторых систем, содержащих P-множества о.-д. функций. *Дискретная математика*, **25**:1 (2013), 76-89.

39. Родин А. А. Базисы в $P-$множествах. *Интеллектуальные системы.* (2013) **17**, 380-392.

40. Родин А. А. О предполных классах во множестве автоматных отображений // Современные проблемы математики и их приложений. Материалы конференции, посвященной 70-летию академика В. А. Садовничего. – М.: Изд-во МГУ, 2009 – С.372.

41. Родин А. А. О существовании алгоритмов для распознавания полноты систем о.-д. функций из множества N_D // Материалы X Международного семинара Дискретная математика и ее приложения –М.: Изд-во МГУ, 2010 – С.421.

42. Родин А. А. Критерий полноты некоторых бесконечных систем во множестве автоматных отображений // Материалы X международной конференции «Интеллектуальные системы и компьютерные науки»(2011, Москва).

43. Родин А. А. Эффективный критерий А-выразимости для систем, содержащих P-множества // Тезисы докладов международной конференции студентов, аспирантов и молодых ученых «Ломоносов-2012» (2012, Москва).