Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
Московский Государственный Университет имени М.В. Ломоносова,
Механико-математический факультет Кафедра Математической
Теории Интеллектуальных Систем

На правах рукописи
УДК 517

Летуновский Алексей Александрович

Задача выразимости автоматных функций относительно расширенной суперпозиции

Специальность 01.01.09
«Дискретная математика»

Диссертация на соискание ученой степени
кандидата физико-математических наук

Научный руководитель:
д.ф.м.н, профессор
Бабин Д.Н.

город Москва – 2014 год

Оглавление

Введение

Общая характеристика работы

Актуальность темы исследования

Теория автоматов - раздел дискретной математики, возникший в середине 20-го века в связи с изучением свойств *конечных автоматов.* Конечный автомат можно охарактеризовать как устройство, имеющее входной и выходной канал, конечное число состояний и в каждый дискретный момент времени, получая на вход один из конечного множества входных сигналов, осуществляющее изменение своего состояния, а также выдающее на выход один из конечного множества выходных сигналов. Автомат фактически производит отображение входных последовательностей в выходные. Связанное с автоматом отображение называется *автоматной функцией.* Возможность получения новых автоматных функций за счет соединения автоматов приводит к алгебре автоматных функций.

Первой работой, давшей толчок к развитию теории автоматов, является работа Э. Поста 1941 года[1]. В ней была описана структура решетки замкнутых классов булевых функций. Булевы функции являются частным случаем автоматов - автоматами без памяти. Сами автоматы и их алгебры начали исследоваться в тридцатые годы предыдущего столетия, но особенно активно в период 50-х годов.

Возникшие для булевых функций, а также для функции k-значной логики, задачи о выразимости, полноте, базисах актуальны и для автоматных функций. Применим к ним и ап-

парат, используемый для решения этих задач. Под выразимостью здесь понимается возможность получения одной автоматной функций через другие автоматные функции. Частным случаем задачи выразимости является задача полноты, в которой проверяется возможность выразимости всех автоматных функций.

Теория автоматов наиболее тесно связана с *теорией алгоритмов* - наукой, возникшей в 30-х годах прошлого столетия в связи с возникновением предположений о невозможности алгоритмического разрешения многих математических проблем (в частности проблема соответствия Поста[2]).

Алгоритмические задачи в теории автоматов возникли в 1960-х годах в связи с проблемой разпознавания полноты: требуется найти алгоритм, позволяющий по любому заданному базису установить, является ли он полным или нет. Для некоторых классов автоматов эта задача была решена.

Э.Пост и С.В. Яблонский решили данную задачу для автоматов без памяти[1, 3], В.Б. Кудрявцев установил критерии полноты для функций с задержками[4], А.А. Летичевским были сформулированы условия полноты для базисов, содержащих автоматы Медведева и автоматы без памяти[5]. Вместе с тем В.Б. Кудрявцев показал континуальность множества предполных классов автоматных функций[6], а М.И. Кратко доказал алгоритмическую неразрешимость в общем случае проблемы распознавания полноты для конечных автоматов относительно операции суперпозиции и обратной связи[7]. В последней работе фактически была доказана алгоритмическая неразрешимость проблемы выразимости константных автоматов относительно операции суперпозиции.

В дальнейшем задача полноты для автоматных функции широко изучалась в различных вариациях. При этом применялись несколько подходов.

Первый подход связан с вариацией понятия равенства ав-

томатов. При этом использовались такие понятия равенства, как A-полнота (В.А. Буевич [8, 9]), Клини-полнота (J. Dassow [10]), ϵ-полнота (Строгалов А.С.[11]), полнота с учетом недостижимых состояний (Хабзун И.В.[12]), N - полнота (Бабин Д.Н.[13]). Все эти задачи оказались алгоритмически неразрешимыми.

Второй подход связан с изучением полноты в некоторых подклассах автоматов. В.Б. Кудрявцев для функций с задержками описал все предполные классы и нашел алгоритм распознавания полноты[4]. А.А. Часовских в классе линейных автоматов также описал все предполные классы и нашел алгоритм распознавания полноты конечных систем относительно операции композиции[14].

Третий подход связан с ограничениями на исследуемые системы автоматов. А.А. Летичевский нашел алгоритм решения задачи о полноте относительно композиции для конечных систем автоматных функций, выдающих свое состояние (автоматов Медведева) при наличии всех булевых функций[5]. В 1986 В.А. Буевич показал алгоритмическую разрешимость задачи A-полноты для систем, содержащих все булевы функции[9]. В 1992г. Д.Н. Бабин показал существование алгоритма распознавания полноты относительно суперпозиции и обратной связи для систем, содержащих все булевы функции[15]. Также Д.Н. Бабин осуществил классификацию добавок по свойству алгоритмической разрешимости полноты в случае наличия в системе данной добавки и показал, что добавок, обеспечивающих алгоритмическую разрешимость, конечное число[16].

В задаче суперпозиции автоматов без обратной связи задача полноты конечных систем не имеет смысла, т.к. любая конечная система относительно суперпозиции не является полной. Поэтому относительно суперпозиции разумно изучать полноту бесконечных систем. В этом направлении интересны работы Бабина Д.Н., который показал, что существуют полные

системы арности 2, а также показал, что система, состоящая из всех одноместных конечных автоматов, а также всех булевых функций, полна[17].

Вместе с тем, после работы М.И. Кратко[7] задача алгоритмической разрешимости для выразимости автоматов широко не изучалась. Основные работы по этой теме были посвящены алгебраической теории автоматов, которая развивалась за рубежом в 1970-х годах и связана в основном с работами К. Крона и Дж. Роудза. Теорема Крона-Роудза фактически утверждает, что любой автомат можно получить суперпозициями триггеров и автоматов, полугруппы которых являются простыми группами, содержащимися в полугруппе первоначального автомата[18].

Д.Н. Бабин в своей кандидатской работе ввел понятие вербального подавтомата и вербальной операции над автоматами. В терминах вербальных подавтоматов ему удалось получить необходимые условия полноты относительно суперпозиции и показать неполноту некоторых известных систем автоматов.

Д.Н. Бабин изучил функциональную систему конечных автоматов с операцией суперпозиции и взятия вербального подавтомата. Были получены критерии полноты и описаны предполные классы в этой функциональной системе. В работе показано, что для произвольных систем автоматов условие Крона-Роудза является, вообще говоря, лишь необходимым условием полноты относительно суперпозиции и превращается в достаточное условие полноты, если к операции суперпозиции добавить вербальную операцию.

С.В. Алешин показал, что в теореме Крона-Роудза при наличии в базисе константных автоматов может быть снято ограничение на специальный вид групповых автоматов в композиции. С.В. Алешин показал, что для любой простой группы G достаточно взять любой групповой автомат, группа которого имеет G в качестве делителя[19]. Тем не менее, вопрос алго-

ритмической неразрешимости задачи выразимости остался открытым.

Цель работы

Исследование задачи выразимости относительно суперпозиции для конечных систем автоматных функций. Найти дополнительные условия, при которых задача выразимости для конкретных известных автоматов алгоритмически разрешима. Исследование задачи выразимости относительно расширенной суперпозиции, т.е. выразимости через системы с конечной добавкой. Исследование задачи выразимости константных автоматов, линейных автоматов, автоматов с группой Z_n, групповых автоматов Медведева, произвольных групповых автоматов. Исследование задачи выразимости всех автоматов с n состояниями.

Научная новизна

Полученные в работе результаты для расширенной суперпозиции являются новыми. Среди них:

- Доказана алгоритмическая разрешимость выразимости константных автоматных функций.
  Приведен критерий выразимости и описано множество выразимых через конечную систему автоматных функций константных автоматных функций относительно операции суперпозиции для систем с фиксированной добавкой - штрих Шеффера и задержка.

- Доказана алгоритмическая разрешимость и приведен критерий выразимости линейных автоматных функций.

- Доказана алгоритмическая разрешимость и приведен критерий выразимости групповых автоматов Медведева.

- Доказана алгоритмическая разрешимость и приведен критерий выразимости групповых автоматов для систем с

фиксированной добавкой - штрих Шеффера и F_2 - универсальный автомат с 2-мя состояниями.

- Доказана алгоритмическая разрешимость и приведен критерий полноты в классе всех автоматов с не более, чем n состояниями для систем с фиксированной добавкой - штрих Шеффера и F_2 - универсальный автомат с 2-мя состояниями.

Основные методы исследования

Наряду с классическими методами и результатами теории автоматов, используются также алгебраические методы. Автором введено понятие цикловых индексов автоматов, которое является важным инструментом для исследования задачи выразимости для систем с фиксированными добавками.

Теоретическая и практическая значимость

Работа имеет теоретический характер. Полученные в ней результаты могут быть использованы в задачах синтеза автоматов.

Апробация результатов

Результаты диссертации неоднократно докладывались на научно-исследовательских семинарах: кафедральный семинар Теория автоматов кафедры Математической Теории Интеллектуальных Систем МГУ, Теория дискретных функций и приложения, Дискретный анализ.

Также результаты докладывались на следующих конференциях

- IX международная конференция "Интеллектуальные системы и компьютерные науки"
- X международная конференция "Интеллектуальные системы и компьютерные науки"
- XI Международный семинар "Дискретная математика и её приложения"

- XVII Международная конференция "Проблемы теоретической кибернетики"

Структура диссертации

Диссертация состоит из введения, трех глав, разбитых на параграфы, списка литературы и списка публикаций автора.

Публикации

Результаты диссертации опубликованы в 7 работах автора.

Краткое содержание работы

Введение Во введении изложена краткая история вопроса, показана актуальность рассматриваемых задач. Сформулированы цель работы и основные результаты.

Глава 1 посвящена введению основных понятий функциональной системы автоматных функций а также изучению алгоритмической разрешимости задачи выразимости относительно выразимости и A-выразимости для произвольных систем автоматов:

Определение Пусть $n, m \in \mathbf{N}$

$$f : (E_2^\infty)^n \to (E_2^\infty)^m$$

- *автоматная функция(a-функция),* если она задается рекуррентно соотношениями (1.1)

$$\begin{cases} q_1(1) = q0_1, \\ ... \\ q_s(1) = q0_s \\ q_1(t+1) = \phi_1(q_1(t), ..., q_s(t), a_1, ..., a_n), \\ ... \\ q_s(t+1) = \phi_s(q_1(t), ..., q_s(t), a_1, ..., a_n) \\ b_1(t) = \psi_1(q_1(t), ..., q_s(t), a_1, ..., a_n) \\ ... \\ b_m(t) = \psi_m(q_1(t), ..., q_s(t), a_1, ..., a_n) \end{cases}$$

Вектор $q = (q_1, ..., q_s)$ задает состояние a-функции f, $q0$ ее начальное состояние, буквы $a = (a_1 a_2 ... a_n)$ и $b = (b_1 ... b_m)$ называются входной и выходной буквами, а сверхслова $a(1)a(2)...$ и $b(1)b(2)...$ - входными и выходными сверхсловами, соответственно. Вектор-функции ϕ и ψ называются функциями переходов и выходной функцией, соответственно

Определение Шестерка

$$(E_2^n, E_2^s, E_2^m, \phi, \psi, q0)$$

- называется *автоматом, порождающим функцию f.*

Автомат называется автоматом Медведева, если $B = Q, \psi(a, q) = q$.

Класс всех автоматных функций обозначим через P.

В этом классе обычным образом вводится операции *суперпозиции.*

Пусть $M \subseteq P$, обозначим через $[M]$ - множество а-функций, получающихся из M с помощью операций суперпозиции.

Без ограничения общности можно считать, что выражающая система состоит из одной автоматной функции. Далее, если это не приводит к недоразумению, мы будем обозначать одной буквой автомат и его автоматную функцию.

Определение Пусть $M \in P$. Обозначим $< M >= [M \cup \{P_2, G_0\}]$, здесь G_0 - автомат "задержки"с нулевым начальным состоянием, P_2 множество всех булевых функций. Будем называть $< M >$ замыканием M относительно расширенной суперпозиции.

Определение Пусть $\tau \in N$, f - некоторая автоматная функция, обозначим через

$$f^\tau : (E_k^\tau)^n \to (E_k^\tau)$$

ограничение этой функции на множество слов длины τ. Скажем, что a - функции $f(x_1, ..., x_n)$ и $g(x_1, ..., x_n)$ - τ - равны, если $f^\tau = g^\tau$. Обозначим через $[M]_\tau$ - множество всех

a-функций, τ- равных получающимся из M с помощью суперпозиции, пусть

$$[M]_A = \bigcap_{\tau=1}^{\infty} [M]_\tau,$$

назовем $[M]_A$ - A- *замыканием* множества M.

Определение Автоматная функция k - называется *константной,*если для любого входного сверхслова $a(1)a(2)...$ ее выходное сверхслово - это одно и то же периодическое сверхслово

$$k(a(1)a(2)...) \equiv b(1)b(2)... = \beta$$

Используя результат Кратко М.И. в главе 1 были доказаны следующие теоремы:
Теорема (1.1) [7] Задача выразимости констант алгоритмически неразрешима.
Теорема (1.2) [8] Задача А-выразимости констант алгоритмически неразрешима.
Теорема (1.3) Задача пустоты множества выразимых констант алгоритмически неразрешима.
Теорема (1.4) Задача пустоты множества А - выразимых констант, алгоритмически неразрешима.
Теорема (1.5) Задача бесконечности множества выразимых констант, алгоритмически неразрешима.
Теорема (1.6) Задача бесконечности множества A - выразимых констант, алгоритмически неразрешима.

Также в главе 1 приведены достаточные условия конечности и бесконечности множества выразимых констант:

Для автоматной функции A определим последовательность подмножеств состояний:
$Q_0 = q_1, Q_1 = \{\phi(q_1, a)|a \in E_2^n\}, ..., Q_{i+1} = \{\phi(q_i, a)|q_i \in Q_i, a \in E_2^n\}$.

Это периодическая последовательность, пусть d - ее предпериод, а ρ_0 - период, $r = Q(A)$ - число состояний автомата A, тогда $\rho_0 < 2^r$, $d < 2^r$.

Для $i \neq j$ через $K_{ij} \subset K$ обозначим подмножество сверхслов $a(1)a(2)...$, у которых $a(i) = a(j)$. Скажем, что автоматная функция A сохраняет множество K_{ij}, если $A(K_{ij}) \subseteq K_{ij}$, в противном случае будем говорить, что автомат отличает моменты времени i и j.

Теорема (1.7) Пусть для некоторых $i, j < \rho(A)$, $s = j \cdot |Q(A)|$, A сохраняет множества $K_{i+t,i+j+t}, t = 0, .., s$,
тогда $|[A \cup P_2] \cap K| < \infty$.

Теорема (1.8) Пусть для всех $i, j < \rho(A)$, $i \neq j$, A отличает моменты времени i и j, тогда $|[A \cup P_2] \cap K| = \infty$ и $|[A \cup P_2]_A \cap K| = \infty$

В **Главе 2** вводится понятия:

Автономной назовём автоматную функцию с функцией переходов, несущественно зависящей от входа. Класс автономных автоматных функций обозначим через V. Заметим, что $K \subset V$.

Определение Пусть сверхслово β можно представить в виде $\beta = \gamma\alpha^\infty$. Выберем из всех таких представлений такое, что γ и α имеют наименьшую длину. Для выбранного представления назовем γ - наименьшим *предпериодом сверхслова* β, *а* α *наименьшим периодом сверхслова* β, *а слова вида* $\underbrace{\alpha\alpha...\alpha}_{n}$ *будем называть периодом сверхслова* β, *здесь* $n \in N$. *Обозначим* $|\alpha|$ *длину слова* α.

Для множества константных автоматных функций $K' \subseteq K$ обозначим через $\Theta(K')$- множество длин минимальных периодов сверхслов $\{\beta_{K_i} : K_i \in K'\}$.

В параграфе 1 главы 2 рассматриваются следующие задачи: по конечному множеству автоматов $M \subset P$ и $\beta \in K$ проверить, верно ли что

$$1)\beta \in < M >$$
$$2)|\ \Theta(< M > \cap K)\ | < \infty$$
$$3)\text{Описать множество } \Theta(< M > \cap K).$$

Также определяются *цикловые индексы* автомата через алгоритм их вычисления

Для некоторого автомата M и произвольного слова $\alpha \in A^*$ обозначим через $s_\alpha = \phi(q, \alpha)$ - подстановку на множестве состояний, задаваемую этим словом, π_α - разбиение множества состояний Q на классы отличимости $Q_1, ...Q_s$ этим словом. Состояния q_i и q_j принадлежат одному классу отличимости, если $\overline{\psi}(q_i, \alpha) = \overline{\psi}(q_j, \alpha)$.

Обозначим $e_\alpha = (s_\alpha, \pi_\alpha)$. Пусть $E_l = \{e_\alpha, |\alpha| = l\}$.

Рассмотрим последовательность $n_1, n_2, ..., n_k, ...$ натуральных чисел, связанную с автоматом M, где n_{i+1} получается из n_i следующим рекурсивным способом.

Пусть $c_i = \{\alpha_i\}$ - множество сверхслов с длиной периода $l|n_i$. Рассмотрим множество - $M(c_i)$ выходных сверхслов автомата M после подачи на него сверхслов из c_i . Очевидно, что $\Theta(M(c_i))$ - конечно. Тогда положим $n_{i+1} = HOK(\Theta(M(c_i)))$. n_i - максимальная длина периода констант, выразимых схемой глубины i, если не учитывать в схеме автоматы без памяти.

1. Вычисляем последовательность (n_i, E_i) до тех пор, пока не найдутся $j < i$, такие, что $E_{n_i} = E_{n_j}$.

2. Назовем $b = n_j$ - безусловным цикловым индексом автомата, $q = \frac{n_i}{n_j}$ - главным цикловым индексом автомата.

Теорема (2.2) Пусть M - автоматная функция, тогда $\Theta(< M > \cap K) = \cup_{i=1}^{\infty}\{t|bq^i\}$, где b,q - цикловые индексы автомата M.

Из теоремы 2.2 следует

Теорема (2.3) Пусть $M \in P$ и $\beta \in K$, тогда существует алгоритм, позволяющий проверить свойство $\beta \in < M >$.

и

Следствие (2.2) Пусть M - автоматная функция и v - автономная автоматная функция, тогда существует алгоритм, позволяющий проверить свойство $v \in < M >$

В параграфе 2 главы 2 приведены примеры вычисления цикловых индексов автомата, а также приведены оценки сложности их вычисления.

В параграфе 3 главы 2 введено понятие автомата Z_n

Определение Автоматом Z_n, $n \in N$ будем называть автомат Медведева вида
$(\{0,1\},\{1,...,n\},\{1,...,n\},\phi,\psi,1)$
$\phi(i,1) = i, \phi(i,0) = (i+1)\ mod\ n$
$\psi(i,0) = \psi(i,1) = i.$

Для выразимости данного автомата верны следующие теоремы:

Теорема (2.6) Пусть $M \in P$, тогда Z_n выразим через $< M >$ тогда и только тогда, когда n делит некоторую степень главного циклового индекса M.

Теорема (2.7) Пусть $M \in P$, тогда существует алгоритм, позволяющий проверить свойство выразимости Z_n через $< M >$.

В параграфе 4 главы 2 введено понятие линейного автомата:

Автомат $L = (E_2^k, Q, E_2^l, \phi, \psi, q0), Q \subset E_2^n$, называется *линейным,* если

$$\begin{cases} \phi(x,q) = Aq + Bx, \\ \psi(x,q) = Cq + Dx, \\ q_0 = (0,0,...,0), \end{cases}$$

где $A : E_2^n \to E_2^n, B : E_2^k \to E_2^n, C : E_2^n \to E_2^l, DB : E_2^k \to E_2^l$ - есть линейные операторы. Матрица A называется основной матрицей линейного автомата.

Доказаны следующие теоремы:

Теорема (2.8) Пусть $M \in P$, а L - линейный автомат, тогда

$$L \in < M > \Leftrightarrow \Theta(< L > \cap K) \subseteq \Theta(< M > \cap K)$$

.

Теорема (2.9) Задача выразимости линейных автоматов через произвольные автоматы относительно расширенной суперпозиции алгоритмически разрешима.

В **Главе 3** рассматривается применение алгебраических конструкций в задаче выразимости автоматов

Определение Пусть $M = (A, Q, B, \phi, \psi, q_0)$ - конечный автомат. Множество подстановок $\{\phi_a : Q \to Q | a \in A\}$, где $\phi_a(q) = \phi(q, a)$, порождает полугруппу подстановок S на множестве Q. Изоморфную S абстрактную полугруппу будем называть полугруппой автомата M и обозначать S_M.

Определение Пусть S_1 и S - полугруппы. Скажем, что полугруппа S_1 делит полугруппу S, если в S найдется такая подполугруппа S_2, что S_1 является гомоморфным образом S_2. Будем обозначать этот факт через $S_1|S$. Множество всех делителей S обозначим через $Del(S)$

Определение Пусть G - множество всех конечных групп. Pr - множество всех простых конечных групп, S - конечная подполугруппа. Через $Pr(S)$ - обозначим множество всех простых групп - делителей полугруппы S. Пусть M - конечный автомат, через $Pr(M)$ обозначим множество простых групп - делителей полугруппы S_M.

Определение Пусть S - некоторая абстрактная полугруппа с единицей, $|S| = r$ и n - наименьшее целое такое, что $n \geq log_2 r$. Всякое отображение E_2^n на S будем называть кодированием. Если $\gamma : E_2^n \longrightarrow S$ - кодирование, то для всякого элемента $s \in S$ найдется набор $a = (a_1, ..., a_n) \in E_2^n$ такой, что $\gamma(a) = s$.

Зафиксируем такое кодирование γ и рассмотрим автомат $M = (E_2^n, S, E_2^n, \phi, \psi)$ с n входами и n выходами, множество

состояний которого совпадает с множестваом элементов полугруппы S, начальное состояние - единичный элемент $e \in S$, а функция переходов соответствует умножению в полугруппе S

$$\phi(s, a) = s * \gamma(a)$$

Функция выходов ψ определена следующим образом:

$$\phi(s, a) = \overline{\gamma^{-1}(s)},$$

где $\overline{\gamma^{-1}(s)}$ - произвольный набор из E_2^n такой, что $\gamma(\overline{\gamma^{-1}(s)}) = s$.

Будем называть построенный автомат *автоматом полугруппы* S, а автоматную функцию, реализуемую M, *специальной автоматной функцией полугруппы* S *и обозначать* $Sp(S)$.

Будем называть триггером (T) - автомат Медведева с 2-мя входами и 2-мя состояниями со следующей функцией переходов

$\phi(0, 00) = 0, \phi(1, 00) = 1$
$\phi(0, 01) = 0, \phi(1, 01) = 0$
$\phi(0, 10) = 1, \phi(1, 01) = 1$
$\phi(0, 11) = 0, \phi(1, 11) = 1$

Верны следующие теоремы:

Теорема Основная теорема о декомпозиции автоматов [18] (3.1) Пусть S - множество автоматных функций и M - множество специальных автоматных функций. Для того, чтобы $S \subseteq < M, T >$ необходимо и достаточно, чтобы $Del(S) \subseteq Del(M)$

С.В. Алешину[19] удалось избавиться от условия специальности, добавив в базис все константные автоматные функции.

Теорема (3.2) Пусть G - простая некоммутативная группа, M - произвольный групповой автомат, такой что S_M изоморфна G и $Sp(G)$ - специальная автоматная функция группы G. Тогда $Sp(G) \in < M, K >$

Теорема(3.3) *Пусть G - простая некоммутативная группа, M - произвольный групповой автомат, такой что группа S_M имеет G в качестве делителя. Тогда $Sp(G) \in < M, K >$*

В главе 3 доказана следующие теоремы:

Теорема (3.4) Пусть $M \in P$, G - произвольный групповой автомат Медведева, тогда проверка $G \in < M >$ алгоритмически разрешима.

Автоматную функцию F_2, задаваемую уравнениями

$$\begin{cases} q(1) = 0, \\ q(t+1) = q(\bar{t})a_1(t) \vee q(t)a_2(t), \\ b(t) = q(t), \end{cases}$$

назовём универсальной автоматной функцией с 2-мя состояниями.

Обозначим $< M >_{F_2} = [M \cup \{F_2, P_2\}]$.

Теорема (3.5) Пусть $M \in P$, G - произвольный групповой автомат, тогда $G \in < M >_{F_2}$ алгоритмически разрешима.

Теорема (3.6) Пусть $M \in P$, P^n - все автоматы с не более, чем n состояниями. Тогда задача $< M >_{F_2} \supseteq P^n$ является алгоритмически разрешимой.

Благодарность Автор выражает глубокую благодарность своему научному руководителю - доктору физико-математических наук, профессору Дмитрию Николаевичу Бабину за постановку задачи, постоянное внимание к работе и всестороннюю поддержку, а также всему коллективу кафедры Математической Теории Интеллектуальных Систем за ценные замечания и доброжелательную и творческую атмосферу.

Глава 1

Задача выразимости для произвольных систем автоматов

1.1 Задача выразимости константных автоматных функций

Через $\mathbf{N}$ обозначим множество натуральных чисел. Для $m, n \in \mathbf{N}$ будем обозначать через $m|n$ то, что m делит n.

Определение 1.1 Пусть $E_2 = \{0, 1\}$, $n \in \mathbf{N}$. Функции вида $g : E_2^n \to E_2$ называются *булевыми функциями,* их множество обозначается через P_2.

Пусть E_2^∞- множество всех сверхслов вида $a(1)a(2)...$, где $a(j) \in E_2$, $j = 1, 2, ...$

Определение 1.2 Пусть $n, m \in \mathbf{N}$

$$f : (E_2^\infty)^n \to (E_2^\infty)^m$$

- *автоматная функция(a-функция),* если она задается рекуррентно соотношениями (1.1)

$$\begin{cases} q_1(1) = q0_1, \\ ... \\ q_s(1) = q0_s \\ q_1(t+1) = \phi_1(q_1(t), ..., q_s(t), a_1, ..., a_n), \\ ... \\ q_s(t+1) = \phi_s(q_1(t), ..., q_s(t), a_1, ..., a_n) \\ b_1(t) = \psi_1(q_1(t), ..., q_s(t), a_1, ..., a_n) \\ ... \\ b_m(t) = \psi_m(q_1(t), ..., q_s(t), a_1, ..., a_n) \end{cases} \tag{1.1}$$

Вектор $q = (q_1, ..., q_s)$ задает состояние a-функции f, $q0$ ее начальное состояние, буквы $a = (a_1 a_2 ... a_n)$ и $b = (b_1 ... b_m)$ называются входной и выходной буквами, а сверхслова $a(1)a(2)...$ и $b(1)b(2)...$ - входными и выходными сверхсловами, соответственно. Вектор-функции ϕ и ψ называются функциями переходов и выходной функцией, соответственно

Определение 1.3 Шестерка

$$(E_2^n, E_2^s, E_2^m, \phi, \psi, q0)$$

- называется *автоматом, порождающим функцию* f.

Далее в тексте мы иногда будем использовать для автомата обозначение $(A, Q, B, \phi, \psi, q0)$, при этом предполагая что $A \subseteq E_2^n, Q \subseteq E_2^s, B \subseteq E_2^m$.

Автомат называется *автоматом Медведева,* если $B = Q, \psi(a, q) = q$.

Обычным образом доопределим функции ϕ и ψ на слова[20]:
$\phi(q, a(1)...a(t)) = \phi(\phi...\phi(q, a(1)), ..., a(t-1)), a(t))$,
$\psi(q, a(1), ..., a(t)) = \psi(\phi(q, a(1)), ..., a(t-1)), a(t))$
и определим рекурсивно функцию
$\overline{\psi}(q, a(1), ..., a(t)) = \overline{\psi}(q, a(1), ..., a(t-1))\psi(\phi(q, a(1)...a(t-1)), a(t))$.

Класс всех a-функций обозначим через $\mathbf{P}$.

В этом классе обычным образом введем операции *суперпозиции.*

Переменная x_i а-функции $f(x_1, ..., x_{i-1}, x_i, x_{i+1}, ..., x_n)$ называется *фиктивной* , если для любых слов одинаковой длины $\alpha_1, ..., \alpha_{i-1}, \alpha_i, \alpha_{i+1}, ..., \alpha_n, \alpha_i'$ из равенства $f(\alpha_1, ..., \alpha_{i-1}, \alpha_i, \alpha_{i+1}, ..., \alpha_n) = \beta$ следует равенство $f(\alpha_1, ..., \alpha_{i-1}, \alpha_i', \alpha_{i+1}, ..., \alpha_n) = \beta$.

Операция 1 Пусть x_{n+1} - переменная, не содержащаяся в множестве переменных $\{x_1, ..., x_n\}$. Будем говорить, что функция $f'(x_1, ..., x_n, x_{n+1})$ получена из функции $f(x_1, ..., x_n)$ *добавлением фиктивной переменной* x_{n+1}, если для любых слов $\alpha_1, ..., \alpha_n, \alpha_{n+1}$ имеем $f'(\alpha_1, ..., \alpha_n, \alpha_{n+1}) = f(\alpha_1, ..., \alpha_n)$.

Операция 2 Пусть x_i - фиктивная переменная а-функции $f(x_1, ..., x_{i-1}, x_i, x_{i+1}, ..., x_n)$. Будем говорить, что функция $f(x_1, ..., x_{i-1}, x_{i+1}, ..., x_n$ получена из функции f *изъятием фиктивной переменной* , если для любых слов $\alpha_1, ..., \alpha_{i-1}, \alpha_i, \alpha_{i+1}, ..., \alpha_n, \alpha$ имеет место $f'(\alpha_1, ..., \alpha_{i-1}, \alpha_{i+1}, ..., \alpha_n) = f(\alpha_1, ..., \alpha_{i-1}, \alpha, \alpha_{i+1}, ..., \alpha_n)$.

Операция 3 Будем говорить, что а-функция $h(x_1, ..., , x_i, ..., x_{j-1}, x_{j+1}, ..., x_n)$ получена из а-функции $f(x_1, ..., , x_i, ..., x_j, ..., x_n)$ *отождествлением переменных* x_i и x_j (в указанном порядке), если для любых $\alpha_1, ..., \alpha_n$ из $\{0,1\}^*$ имеет место $h(\alpha_1, ..., \alpha_i, ..., \alpha_{j-1}, \alpha_{j+1}, ..., \alpha_n) = f(\alpha_1, ..., \alpha_i, ..., \alpha_{j-1}, \alpha_i, \alpha_{j+1}, ..., \alpha_n)$.

Операция 4 Пусть $x_1', x_2', ..., x_n'$ - разные переменные. Функция $h(x_1', ..., x_n')$ получена из $f(x_1, ..., x_n)$ *переименованием переменных,* если для любого набора слов $\alpha_1, ..., \alpha_n$ имеет место $h(\alpha_1, ..., \alpha_n) = f(\alpha_1, ..., \alpha_n)$. Эти две функции задают одно и то же отображение $[\{0,1\}]^n \to \{0,1\}^*$ и отличаются лишь названиями переменных.

Операция 5 Пусть $f(x_1, ..., x_i, ..., x_n)$ и $h(x_1', ..., x_m')$ - две а-функции, при этом множества $\{x_1, ..., x_n\}$ и $\{x_1', ..., x_m'\}$ не пересекаются. Будем говорить, что функция $g(x_1, ..., x_{i-1}, x_{i+1}, ..., x_n, x_1', ..., x_m')$ получена из функций f и h

подстановкой функции h вместо переменной x_i в функцию f, если для всякого набора $\alpha_1, ..., \alpha_{i-1}, \alpha_{i+1}, ..., \alpha_n, \alpha_{n+1}, ..., \alpha_{n+m}$ слов из $\{0,1\}^*$ имеет место
$g(\alpha_1, ..., \alpha_{i-1}, \alpha_{i+1}, ..., \alpha_n, \alpha_{n+1}, ..., \alpha_{n+m}) =$
$f(\alpha_1, ..., \alpha_{i-1}, h(\alpha_{n+1}, ..., \alpha_{n+m}), \alpha_{i+1}, ..., \alpha_n)$.

Операции 1-5 называются операциями *суперпозиции.*

Пусть $M \subseteq P$, обозначим через $[M]$ - множество a-функций, получающихся из M с помощью операций суперпозиции. Рассматривая конечные системы автоматов, будем считать без ограничения общности, что M состоит из одного автомата, т.к. задачу выразимости для нескольких автоматов можно свести к задаче для одного автомата, являющегося их параллельным соединением.

Определение 1.4 Пусть $\tau \in N, f$ - некоторая автоматная функция, обозначим через

$$f^\tau : (E_k^\tau)^n \to (E_k^\tau)$$

ограничение этой функции на множество слов длины τ. Скажем, что a - функции $f(x_1, ..., x_n)$ и $g(x_1, ..., x_n)$ - τ - равны, если $f^\tau = g^\tau$. Обозначим через $[M]_\tau$ - множество всех a-функций, τ- равных получающимся из M с помощью суперпозиции, пусть

$$[M]_A = \bigcap_{\tau=1}^{\infty} [M]_\tau,$$

назовем $[M]_A$ - A- *замыканием* множества M.

Определение 1.5 Автоматная функция k - называется *константной,*если для любого входного сверхслова $a(1)a(2)...$ ее выходное сверхслово - это одно и то же периодическое сверхслово

$$k(a(1)a(2)...) \equiv b(1)b(2)... = \beta$$

Когда это не приводит к недоразумению, мы будем отождествлять константную автоматную функцию k с ее выходным сверхсловом и обозначать той же буквой. Класс всех константных автоматных функций обозначим через K.

На разных словах $\alpha(1)\alpha(2)...\alpha(s)$ и $\beta(1)\beta(2)...\beta(s)$ одинаковой длины s определим числовую функцию

$$t(\alpha, \beta) = min(i|(\alpha(i) \neq \beta(i))).$$

Можно считать, что эта функция естественным образом доопределена на разные сверхслова

$$t : (E_2^\infty)^2 \to N$$

Через $\alpha]_t$ - будем обозначать начало длины t слова α.

В этой главе мы рассмотрим следующие задачи: по конечному множеству автоматных функций M и $k \in K$ проверить верно ли что
1.$k \in [M]$ - задача выразимости константы
2.$k \in [M]_A$ - задача A-выразимости константы
3.$[M] \cap K = \emptyset$ - задача пустоты множества выразимых констант
4.$[M]_A \cap K = \emptyset$ - задача пустоты множества A-выразимых констант
5.$|[M] \cap K| = \infty$ - задача бесконечности множества выразимых констант
6.$|[M]_A \cap K| = \infty$ - задача бесконечности множества A-выразимых констант.

Теорема 1.1 [7] *Задача выразимости констант алгоритмически неразрешима.*

Теорема 1.2 [8] *Задача A-выразимости констант алгоритмически неразрешима.*

Теорема 1.3 *Задача пустоты множества выразимых констант алгоритмически неразрешима.*

Теорема 1.4 *Задача пустоты множества A - выразимых констант, алгоритмически неразрешима.*

Теорема 1.5 *Задача бесконечности множества выразимых констант, алгоритмически неразрешима.*

Теорема 1.6 *Задача бесконечности множества A - выразимых констант, алгоритмически неразрешима.*

Доказательства теорем 1.1-1.6.Для доказательства теорем используем некоторые конструкции из теории алгоритмов.

Однородная система продукций Поста - это тройка $T =< D, V, w >$, где $D = \{d_1, d_2, ..., d_k\}$ - конечный алфавит, $V : D \to D^*, R_i = V(d_i), w \geq 1$ - натуральное число. Будем говорить, что система продукций T - применима к слову

$$\xi = d_{i_1} d_{i_2} ... d_{i_k} \in D^*$$

при $l \geq w$, называть слово $\xi' \in D^*$ - результатом применения T к ξ и обозначать $\xi' = T(\xi)$, если

$$\xi' = d_{i_{w+1}} ... d_{i_l} R_{i_1}$$

Если $l < w$, то скажем, что система продукций T- неприменима к слову ξ.

Рассмотрим последовательность

$$\xi_1, \xi_2, ...,$$

такую, что $\xi_1 = \xi$, и $\xi_{i+1} = T(\xi_i), i = 1, 2...$ Если эта последовательность конечна, то будем говорить, что при применении к слову ξ система T останавливается через конечное число шагов. Для каждой однородной системы продукций Поста T

можно поставить вопрос о разрешимости "проблемы остановки": существует ли алгоритм, который по любому наперед заданному слову ξ устанавливает, конечно или бесконечно множество T - продукций слова ξ.

Лемма 1.1 [21]*Существует система однородных продукций Поста* $T =< D, V, w >$*, для которой не существует алгоритма, решающего проблему остановки.*

Обозначим Γ_0 - сверхслово, состоящее из одних нулей, Γ_1 - сверхслово, состоящее из одних единиц.

Сверхслово

$$\beta = \underbrace{0.....0}_{n(k+2)}\tilde{d}_i\tilde{d_{j_1}}...\tilde{d_{j_w}}\Gamma_0$$

начинающееся с серии нулей, длины кратной $k+2$, и слова $\tilde{d}_i$, и заканчивающееся сверхсловом из нулей, назовем *правильным* сверхсловом i-того типа. Обозначим множество правильных сверхслов i-го типа через M_i. Множество сверхслов вида

$$\underbrace{0.....0}_{n(k+2)}\tilde{d}_i\tilde{d_{j_1}}\tilde{d_{j_2}}...$$

обозначим через S_i. Для сверхслов $\gamma \notin M_i \cup S_i \cup \{\Gamma_0\}$ определим числовую функцию

$$c_i : E_2^\infty \to N, c_i(\gamma) = max\{t(\beta, \gamma), \beta \in M_i \cup S_i \cup \{\Gamma_0\}\}.$$

Обозначим через $L_i(\gamma) = \gamma]_{c(\gamma)-1} = \beta]_{c(\gamma)-1}$ начало того сверхслова $\beta \in M_i \cup S_i \cup \{\Gamma_0\}$, на котором этот максимум достигается.

Для доказательства теоремы 1.1 определим функции g_i. Для каждого правильного сверхслова i-го типа β определим функции g_i соотношениями а-г

а)$g_i(\beta) = \underbrace{0.....0}_{n(k+2)}\underbrace{0.....0}_{w(k+2)}\tilde{d_{j_w}}...\tilde{d_{j_l}}\tilde{R}_i\Gamma_0$ при $l \geq w-1$,

б)$g_i(\beta) = \Gamma_0$ при $l \leq w-1$
в)$g_i(\Gamma_0) = \Gamma_0$,
г)$g_i(\gamma) = g_i(L_i(\gamma))]_{c_i(\gamma)-1}\Gamma_1$ при $\gamma \notin M_i \cup S_i \cup \{\Gamma_0\}$

А-функции $g_i(x)$ определены корректно. Для слова $\xi \in D^*$ определим константную а-функцию

$$g_\xi(\alpha) = \tilde{\xi}\Gamma_0,\ \alpha \in \{0,1\}^\infty$$

Лемма 1.2 *А-функция* Γ_0 *выразима через* $\Sigma'_\xi = \{\Gamma_0, g_i(x), i = 1, ..., k, g_\xi(x)\}$ *тогда и только тогда, когда система продукций слова* ξ *конечна.*

Доказательство:

Достаточность:Пусть последовательность продукций обрывается на слове ξ_s, длина которого меньше w. В этом случае

$$\Gamma_0 = g_{i_s}(g_{i_{s-1}}(...g_\xi(x))),$$

где d_{i_j} - первая буква слова ξ_j. Константа Γ_0 выразима.

Необходимость Пусть в замыкании системы Σ_ξ есть константа Γ_0, тогда можно построить схему S над Σ_ξ, которая реализует Γ_0. Заметим, что множество $\{\alpha\Gamma_1 | \alpha \in E_2^*\}$ сохраняется автоматами $g_i(x)$, $i = 1, ..., k$, значит в схеме должна присутствовать g_ξ. Рассмотрим схему ниже последнего g_ξ. Идя вниз по схеме S, мы либо получим на выходе одного из элементов слово $\beta'\Gamma_1$, и тогда полученный автомат не является автоматом Γ_0, либо получим суперпозицию вида $\Gamma_0 = g_i(g_{i_l}(g_{i_{l-1}}(...g_\xi(x))))$, где $d_{i_1}, d_{i_2}, ..., d_{i_l}$ - первые буквы $\xi_{i_1}, \xi_{i_2}, ..., \xi_{i_l}, \xi_i$, что и говорит о конечности множества продукций Поста слова ξ. *Лемма 1.2 доказана.*

Теорема 1.1 непосредственно следует из лемм 1.2 и 1.1

Для доказательства теоремы 1.2 модифицируем функции $g_i(x)$, $i = 1, ..., k$, входящие в систему Σ_ξ. Рассмотрим функции $g'(x)$, отличающиеся от функций $g_i(x)$ условием б)

б')$g'(\beta) = \underbrace{0.....0}_{n(k+2)}\underbrace{0.....0}_{w(k+2)}\Gamma_1$, при $l < w-1$

Лемма 1.3 *Автоматная функция* Γ_0 *A-выразима через* $\Sigma'_\xi = \{g'_i(x), i = 1, ..., k, g_\xi\}$ *тогда и только тогда, когда множество* T_0 *продукций слова* ξ *бесконечно.*

Доказательство:

Достаточность:Пусть множество продукций слова ξ бесконечно и имеет вид

$$\xi_1 = d_{j_1}\gamma_1,\ \xi_2 = d_{j_2}\gamma_1,...,\xi_s = d_{j_s}\gamma_s,...$$

Тогда для любого s слово $\underbrace{0.....0}_{sw(k+2)}$ выразимо схемой

$$g'_{j_s}(g'_{j_{s-1}}(...(g'_{j_1}(g_{\xi(x)}))...))$$

, а значит и автомат Γ_0 - A-выразим.

Необходимость Пусть автомат Γ_0 - A-выразим. Это значит, что $\forall\tau \geq 0$ слово $\underbrace{0.....0}_{\tau}$ - τ-выразимо некоторой схемой. Предположим, тем не менее, что множество продукций Поста слова ξ - конечно и имеет вид

$$\xi_0 = \xi, \xi_1, ..., \xi_s.\ \xi_0 = d_{j_0}\gamma_0,\ \xi_1 = d_{j_1}\gamma_1,...,\xi_s = d_{j_s}\gamma_s.$$

Рассмотрим сверхслово $\delta_l = \underbrace{0.....0}_{l}\Gamma_1 \notin M_i \cup S_i \cup \{\Gamma_0\}$, при l не кратном $k+2$. Имеем $c_i(\delta_l) = l+1$, значит $g'_i(\delta_l) = \delta_l$ при всех i. Если в схеме $S(x)$ нет элемента $g_\xi(x)$, то не может быть выполнено $S(x) \equiv \Gamma_0$, так как $S(\Gamma_0) = \Gamma_0$, $S(\delta_l) = \delta_l$.

Возьмем $\tau = w(s+1)(k+2)+k$. Без ограничения общности, рассмотрим схему ниже последнего $g_\xi(x)$. Если она построена согласно последовательности продукций Поста, то получится слово δ_l при $l < \tau$. Если схема автоматов не соответствует продукциям Поста, то для некоторых l и j будет

$$g'_j(\underbrace{0.....0}_{w(k+2)}\tilde{d}_l...\Gamma_0) = \delta_l,$$

где $l < \tau$ и не кратно $k+2$. Ниже стоящие функции сохраняют такое слово δ_l. Значит автомат Γ_0 - не τ выразим и мы получили противоречие *Лемма 1.3 доказана.*

Теорема 1.2 непосредственно следует из лемм 1.1 и 1.3

Для доказательства теоремы 1.3 определим множество слов вида

$$\overline{\beta} = \underbrace{0.....0}_{n} \tilde{d}_i ... \tilde{d_{j_w}} ... \tilde{d_{j_l}} \Gamma_0,$$

начинающихся с серии нулей и слова $\tilde{d}_i$, и заканчивающихся сверхсловом из нулей, обозначим через $\overline{M_i}$. Множество сверхслов вида

$$\underbrace{0.....0}_{n} \tilde{d}_i \tilde{d_{j_1}} \tilde{d_{j_2}} ...$$

обозначим через $\overline{S_i}$.

Определим функции $\overline{g_i}(x)$ следующими соотношениями
а) $\overline{g_i}(\overline{\beta}) = \underbrace{0.....0}_{n+w(k+2)} \tilde{d_{j_w}} ... \tilde{d_{j_l}} \tilde{R}_i \Gamma_0$, при $l \geq w-1$,
б)$\overline{g_i}(\overline{\beta}) = \Gamma_0$ при $l < w-1$,
в)$\overline{g_i}(\Gamma_0) = \Gamma_0$,
г)$\overline{g_i}(\gamma) = \overline{g_i}(L_i(\gamma))]_{c_i(\gamma)-1}\Gamma_1$, при $\gamma \notin \overline{M_i} \cup \overline{S_i} \cup \{\Gamma_0\}$
и функцию $\overline{g}_\xi(x)$
$\overline{g}_\xi(\Gamma_0) = \Gamma_0$, $\overline{g}_\xi(\alpha) = \Gamma_0]_{t(\Gamma_0,\alpha)-1}\tilde{\xi}\Gamma_0$ при $\alpha \neq \Gamma_0$.

Лемма 1.4 *Пусть* $\{\Sigma^\xi = \overline{g}_i(x), i = 1, ..., k, \overline{g}_\xi(x)\}$, *тогда множество выразимых относительно суперпозиции констант пусто тогда и только тогда, когда последовательность продукций слова* ξ *- бесконечна.*

Доказательство:

Достаточность: Пусть множество T - продукций слова ξ конечно. Это означает, что последовательность T - продукций $\xi = \xi_1, \xi_2, ..., \xi_s$ обрывается на слове ξ_s, длина которого меньше w. В этом случае

$$\Gamma_0 = \overline{g}_{i_s}(\overline{g}_{i_{s-1}}(...(\overline{g}_{\xi}(x))...)),$$

где d_{ij} - первая буква слова ξ_j. А значит константа Γ_0 - выразима.

Необходимость: Пусть последовательность продукций Поста слова ξ бесконечна и имеет вид $\xi_1, \xi_2, ..., \xi_s, ...$ и $d_{i_1}, d_{i_2}, ..., d_{i_s}, ...$ - последовательность первых букв слов ξ_i соответственно. Предположим, что некоторой схемой над Σ^{ξ} нам удалось реализовать константный автомат. Заметим, что это автомат Γ_0, т.к. для любого $g \in \Sigma^{\xi}$ выполнено $g(\Gamma_0) = \Gamma_0$.

Каждый из автоматов $\overline{g}_i(x), i = 1, ..., k$ сохраняет множество сверхслов, оканчивающихся на Γ_1, а также сверхслово Γ_0. Поэтому схемой без участия $\overline{g}_{\xi}(x)$ реализовать Γ_0 нельзя.

Пусть $W = E_2^{\infty} \backslash \Gamma_0$. Для некоторых индексов $i_1, i_2, ..., i_t$ рассмотрим формулы вида

$$\triangle(x) = \overline{g}_{i_1}(\overline{g}_{i_2}(...(\overline{g}_{i_t}(\overline{g}_{\xi}(x)...))))$$
$$\nabla(x) = \overline{g}_{i_1}(\overline{g}_{i_2}(...(\overline{g}_{i_t}(x)...)))$$

Заметим, что $\nabla(\Gamma_1) = 0...0\Gamma_1$. Заметим также, что для всякого $\alpha \neq \Gamma_0$ и всякой $\triangle$ выполнено $\triangle(\alpha) \neq \Gamma_0$. В самом деле: $\overline{g}_{\xi}(x)$ выдает константу $0...0\tilde{\xi}\Gamma_0$, правильная цепочка применений продукций даст

$$\overline{f}_{i_s}(\overline{f}_{i_{s-1}}(...(0...0\tilde{\xi}\Gamma_0)...)) = 0...0\tilde{\xi}\Gamma_0$$

а неправильная

$$\overline{f}_{i_s}(\overline{f}_{i_{s-1}}(...(0...0\tilde{\xi}\Gamma_0)...)) = 0...0\Gamma_1.$$

Всякая схема над Σ^{ξ} может быть представлена в виде

$$\triangle_p(...(\triangle_2(\triangle_1(x)))...) \text{ или } \triangle_p(...(\triangle_2(\nabla_1(x)))...)$$

В любом случае получаем, что $S(\Gamma_1) \neq \Gamma_0$. Таким образом, не существует схемы, реализующей Γ_0 *Лемма 1.4 доказана*

Теорема 1.3 непосредственно следует из лемм 1.1, 1.4.

Для доказательства теоремы 1.4 рассмотрим множество сверхслов β вида $\underbrace{0...0}_{n(k+2)}\ \tilde{d_i}\tilde{d_{j_1}}...\tilde{d_{j_w}}...\tilde{d_{j_l}}1\beta_t1\beta_{t+2}....$

А также автоматные функции $h_i(x)$, задаваемые соотношениями а-г

а)$h_i(\beta) = \underbrace{0...0}_{(n+w)(k+2)}\ \tilde{d_{j_w}}...\tilde{d_{j_l}}\tilde{R_i}1\beta_t1\beta_{t+2)}..,$

где $t = (n+l)w(k+2) + |\tilde{R_i}| + 1,\ l \geq w-1$

б)$h_i(\beta) = \underbrace{0...0}_{(n+w)(k+2)}\ 1\beta_t1\beta_{t+2}...,$

где $t = (n+l)w(k+2) + 1,\ l < w-1$

в)$h_i(\Gamma_0) = \Gamma_0,$

г)$h_i(\gamma) = h_i(P_i(\gamma))]_{c_i(\gamma)-1}1\gamma_t1\gamma t+2)..,\ t = c(\gamma)+1,$

при $\gamma \notin M_i \cup S_i \cup \{\Gamma_0\}$

А-функцию $h_\xi(x)$ определим так $h_\xi(\alpha) = \tilde{\xi}1\alpha_t1\alpha_{t+2}....$

Лемма 1.5 *Пусть* $\Sigma_0^\xi = \{h_i(x), i = 1, ..., k, h_\xi(x)\}$. *Тогда множество А-выразимых констант пусто тогда и только тогда, когда последовательность продукций Поста слова* ξ *конечна.*

Доказательство:

Достаточность:Пусть множество продукций слова ξ бесконечно и имеет вид $\xi_1 = d_{j_1}\gamma_1, \xi_2 = d_{j_2}\gamma_2, ..., \gamma_s = d_{j_s}\gamma_s....$
Тогда $\forall\tau \geq 0$ слово $\underbrace{00...0}_{\tau}$ выразимо схемой
$h_{j_s}(h_{j_{s-1}}(...(h_{j_1}(h_\xi(x))...))$, а значит и автомат Γ_0 - А-выразим и множество А-выразимых констант не пусто.

Необходимость: Пусть последовательность продукций слова ξ-конечна. Тогда любой автомат А-выразимый в схеме Σ с момента времени $\tau = sw(k+2)$, где s - длина последовательности продукций, существенно зависит от входа, а значит не константный.

Лемма 1.5 доказана.

Теорема 1.4 непосредственно следует из лемм 1.1, 1.5.

Для доказательства теоремы 1.5 определим функции $g_i(x\alpha), i = 1, ...k$ и $g_\xi(x\alpha), x \in E_2, \alpha \in E_2^\infty$ соотношениями а-г. Для правильного сверхслова i - го типа β
а)$g_i(x\beta) = x\underbrace{0.....0}\tilde{d_{j_w}}...\tilde{d_{j_l}}\tilde{R_i}\Gamma_0$ при $l \geq w - 1$,
б)$g_i(x\beta) = x\Gamma_0$ при $l < w - 1$,
в)$g_i(x\Gamma_0) = x\Gamma_0$
г)$g_i(x\gamma) = xg_i(L_i(\gamma))\Gamma_1$ при $\gamma \neq \beta$
$g_\xi(x\Gamma_0) = x\tilde{\xi}\Gamma_0, g_\xi(x\alpha) = x(\tilde{\xi}\Gamma_0]_{t(\Gamma_0,\alpha)-1}\Gamma_1,)$ при $\alpha \neq \Gamma_0$

Лемма 1.6 *Пусть* $\Sigma'_\xi = \{\Gamma_0, g_i(x), i = 1, ..., k, g_\xi(x)\}$ *тогда множество выразимых относительно суперпозиции констант бесконечно, тогда и только тогда, когда последовательность продукций слова* ξ*- бесконечна.*

Доказательство:

Достаточность:Пусть последовательность продукций слова ξ есть $\xi_1, \xi_2, ...,$ и она бесконечна, пусть d_{is} - первая буква слова ξ_s. Рассмотрим последовательность константных автоматов: $\alpha_1 = \Gamma_0, \alpha_2 = g_{i1}(\alpha_1), \alpha_3 = (g_{i2}(\alpha_2)), ..., \alpha_{j+1} = g_{ij}(\alpha_j), ...$ По построению функции g_i для всех s, j выполнено $\alpha_s \neq \alpha_j$, значит множество констант $\{\alpha_1, \alpha_2, ...\}$ - бесконечно.

Необходимость:Пусть последовательность продукций слова ξ - конечна и равна $\xi_1, \xi_2, ..., \xi_s$, и пусть d_{ij} - первая буква слова ξ_j. Заметим, что все автоматы системы Σ'_ξ, одноместные и все схемы, составленные из них имеют вид одной цепочки. Кроме Γ_0, все они имеют в начальном состоянии тождественную выходную функцию. Если в схеме нет автомата Γ_0, то схема имеет в начальном состоянии тождественную выходную функцию, а не константу. Такими схемами константных a - функций получить нельзя.

Если в схеме есть автомат Γ_0, но нет g_ξ, то можно считать, что он стоит в начале цепочки и других автоматов Γ_0 в схеме нет. Все автоматы g_i по построению таковы, что $g_i(\Gamma_0) = \Gamma_0$. Такими схемами можно получить лишь Γ_0.

Наконец, пусть в схеме есть автомат Γ_0 и автомат g_ξ. Можно считать, что Γ_0 стоит в начале цепочки, и других автоматов вида Γ_0 в схеме нет. Т.к. $g_i(\Gamma_0) = \Gamma_0$, то можно сразу считать, что выход Γ_0 непосредственно соединен со входом g_ξ. Схема

$$g_{is}(...(g_{i2}(g_\xi(\Gamma_0)))...)$$

последовательно преобразует константу Γ_0 следующим образом: если функции, стоящие ниже g_ξ, соответствует продукциям, то получается снова константа Γ_0. Если последовательность, стоящих ниже g_ξ функций такова, что g_j неправильно применяется к сверхслову, начинающемся с $\tilde{d}_i$ то имеем

$$g_j(x\underbrace{0.....0}_{nw(k+2)}\tilde{d}_i...\Gamma_0) = x\underbrace{00...0}_{l}\Gamma_1 = \delta_l, \delta_l \notin M_i \cup S_i \cup \{\Gamma_0\}$$

где l не кратно $k+2$ и не превосходят $sw(k+2)$. Множество слов, у которых с момента l встречаются лишь единицы сохраняются всеми автоматами из $\Sigma_\xi \backslash \Gamma_0$. Таким образом, мощность множества получаемых констант не превосходит $2^{sw(k+2)}$. *Лемма 1.6 доказана.*

Теорема 1.5 непосредственно следует из лемм 1.1,1.6.

Лемма 1.7 *Пусть $\Sigma'_\xi = \{\Gamma_0, g_i(x), i = 1, ..., k, g_\xi(x)\}$, тогда множество A-выразимых через Σ'_ξ констант конечно точно тогда, когда последовательность продукций слова ξ - конечна.*

Доказательство.Будем использовать конструкцию леммы 1.6. Из бесконечности выразимых через Σ_ξ констант прямо следует бесконечность A-выразимых через Σ_ξ констант. Заметим, что любой автомат, реализуемый схемами в Σ_ξ, начиная с момента $sw(k+2)$ выдает либо Γ_0, либо Γ_1. Значит,

A-выразимых констант не более, чем $2^{sw(k+2)}$. *Лемма доказана.*

Теорема 1.6 непосредственно следует из лемм 1.1,1.7.

1.2 Достаточные условия конечности и бесконечности множества выразимых констант

Хотя в общем случае задача выразимости константных автоматных функций является алгоритмически неразрешимой и более того неразрешимы также задача наличия в замыкании хотя бы одной константы и задача определения конечности количества констант в замыкании, удается в некоторых задачах получить необходимые и (или) достаточные условия для этих задач.

Для автоматной функции A определим последовательность подмножеств состояний:
$Q_0 = q_1, Q_1 = \{\phi(q_1, a)|a \in E_2^n\}, ..., Q_{i+1} = \{\phi(q_i, a)|q_i \in Q_i, a \in E_2^n\}$.
Это периодическая последовательность, пусть d - ее предпериод, а ρ_0 - период, $r = Q(A)$ - число состояний автомата A, тогда $\rho_0 < 2^r$, $d < 2^r$.

Для $i \neq j$ через $K_{ij} \subset K$ обозначим подмножество сверхслов $a(1)a(2)...$, у которых $a(i) = a(j)$. Скажем, что автоматная функция A сохраняет множество K_{ij}, если $A(K_{ij}) \subseteq K_{ij}$, в противном случае будем говорить, что автомат отличает моменты времени i и j.

Теорема 1.7 *Пусть для некоторых* $i, j < \rho(A)$, $s = j \cdot |Q(A)|$, *A сохраняет множества* $K_{i+t,i+j+t}, t = 0, .., s$,
тогда $|[A \cup P_2] \cap K| < \infty$.

Теорема 1.8 *Пусть для всех* $i, j < \rho(A)$, $i \neq j$, A *отличает моменты времени* i *и* j, *тогда* $|[A \cup P_2] \cap K| = \infty$ *и* $|[A \cup P_2]_A \cap K| = \infty$

Доказательство теорем 1.7, 1.8. Для автоматной функции A определим последовательность множеств сверхслов
$L_0 = \{\Gamma_0, \Gamma_1\}$,
$L_1(A) = P_2(L_0, A(L_0), ...$
$L_{i+1}(A) = P_2(L_i \cup A(L_i)), ...$
обозначим

$$L(A) = \bigcup_{i=0}^{\infty} L_i(R)$$

Здесь $L_i(A)$ - множество констант, получаемых схемами глубины i. $L(A)$ - множество констант, выразимых через $[A \cup P_2]$

Пусть для некоторых $i, j < \rho(A)$ множества $K_{i+t,i+j+t}, t = 0, ..., s$ сохраняются автоматом A. Очевидно, что $L_0 = \Gamma_0, \Gamma_1$ содержится в каждом из множеств K_{ij} и для всех $a \in L_0$ выполнено $\alpha(i) = \alpha(i + j), ..., \alpha(i + s) = \alpha(i + s + j)$. Сверхслова $\alpha \in L_0$ периодичны с периодом и предпериодом j.

Пусть все слова из $L_p(A)$ имеют период и предпериод j, покажем, что это свойство выполнено и для $L_{p+1}(A)$. Рассмотрим в $L_p(A)$ сверхслово $\alpha = a_1 a_1 ...$, где $|a_1| = j$. Подадим α на автомат A, находящийся в начальном состоянии, последовательность $q_1, q_2 = \phi(q_1, a_1), q_3 = \phi(q_2, a_1), ...$ содержит не более r различных состояний. Значит выходное сверхслово $A(\alpha)$ будет периодично с периодом и предпериодом в сумме не большим jr. По свойству сохранения множеств

$$K_{i+t,i+j+t}, t = 0...s,$$

$A(\alpha)$ будет периодично с периодом и предпериодом j на начальном куске длины jr, значит $A(\alpha)$ периодично с периодом j. Следовательно

$$L(A) = \bigcup_{i=0}^{\infty} L_i(A)$$

состоит из слов с периодом j и предпериодом j. Значит $L(A) = |[R \cup P_2] \cap K| < \infty$. Теорема 1.7 доказана.

Лемма 1.8 Пусть для всех $i \neq j, i, j < \tau$ моменты времени i и j отличимы A, тогда $L(A)]_\tau = E_2^\tau$.

Лемма 1.9 *Пусть для всех $i \neq j, i, j < \rho(A)$ автомат отличает моменты времени i и j, тогда автомат отличает моменты времени i и j для всех $i \neq j$*

Доказательство теоремы 1.8 следует из лемм 1.8,1.9
В самом деле: По лемме 1.9 имеем, что все моменты $i \neq j$ отличимы, а по лемме 1.8 - для любого τ выполнено $L(A)]_\tau = E_2^\tau$. Значит $|[R \cup P_2] \cap K| = \infty$ и $|[R \cup P_2] \cap K|_A = \infty$
Доказательство леммы 1.8 Доказательство проведём по индукции
1) При $\tau = 2$ у нас есть константы $00, 11$. Так как первые два момента времени отличимы, то мы можем получить некоторую константу $ab..., a \neq b$. Её с помощью $h(x) \in P_2$ такой, что $h(a) = c, h(b) = d$ можно преобразовать в константу $cd...$ при всех c и d, а значит на начале длины 2 есть все константы длины 2 или $L(A)]_2 = E_2^2$
2)Покажем, что если $L(A)]_\tau$, то выполнено $L(A)]_{\tau+1} = E_2^{\tau+1}$.
У нас есть все константы до длины τ и $\tau+1$-й момент времени отличим от всех предыдущих t-х при всех $t \leq \tau$. Покажем, что $|L(A)]_{\tau+1}| > 2^\tau$. В самом деле, если это не так, то продолжение $x_{\tau+1}$ константы $x_1x_2...x_\tau$ на $\tau + 1$ момент функционально зависит от её значений в предыдущие τ моментов, и если функция $h(x_1, x_2, ..., x_\tau) = x_{\tau+1}$, такая что для любых двух наборов $y_1y_2...y_\tau, z_1z_2...z_\tau \in E_k^\tau$ и любой функции $W(y, z) \in P_2$ будет выполнено 1.2.

$$h(W(y_1, z_1), W(y_2, z_2), ..., W(y_\tau, z_\tau)) = W(h(y_1, y_2, ..., y_\tau), h(z_1, z_2, ..., z_\tau)) \quad (1.2)$$

При $W \equiv 0$ получаем, что $h(0,0,...,0) = 0$, при $W \equiv p$ получаем, что $h(p,p,...,p) = p$. Предположим, что $h(x_1,x_2,...,x_\tau) = x_{\tau+1}$ существенно зависит от x_1, тогда найдутся наборы $(a,c_2,...,c_\tau),(b,c_2,...,c_\tau)$, такие что

$$h(a,c_1,...,c_\tau) = c \neq d = h(b,c_2,...,c_\tau).$$

Для функции

$$W_0(x,y) = \begin{cases} 1, x = y \\ 0, x \neq y \end{cases}$$

соотношение 1.2 даст
$h(1,0,..,.0) = h(W_0(a,b),W_0(c_2,c_2),...,W_0(c_\tau,c_\tau)) =$
$= W_0(h(a,c_2,...,c_\tau),h(b,c_2,...,c_\tau)) = W_0(c,d) = 1.$
Если предположить, что $h(x_1,x_2,...,x_\tau) = x_{\tau+1}$ зависит существенно от двух переменных, то получим, без ограничения общности

$$h(1,0,...,0) = 1, h(0,1,0,...,0) = 1$$

Если далее взять $W_1(x,y) = max(x,y), W_2(x,y) = x + y$, то получим противоречивые равенства:
$h(1,1,0,...,0) = h(W_1(1,0),W_1(0,1),W_1(0,0),...,W_1(0,0) =$
$= W_1(h(1,0,...,0),h(0,1,0,...,0)) == W_1(1,1) = 1$
$h(1,1,0,...,0) = h(W_2(1,0),W_2(0,1),W_2(0,0),...,W_2(0,0)) =$
$= W_2(h(1,0,...,0),h(0,1,0,...,0)) = W_2(1,1) = 0$

Следовательно $h(x_1,x_2,...,x_\tau) = x_{\tau+1}$ функция одного переменного, сохраняющая все константы, то есть $h(x_1,x_2,...,x_\tau) = x_i$ при некотором i, что означает неотличимость моментов времени i и $\tau+1$ и противоречит условию леммы. Значит $|L(A)]_{\tau+1}| > 2^\tau$ и найдутся наборы $(c_1,c_2,...,c_\tau,c),(c_1,c_2,...,c_\tau,d) \in L(A)]_{\tau+1}$ из которых с помощью функции W_0 можно получить набор $(0,0,...,1)$ длины $\tau+1$, складывая который с другими наборами получим все наборы длины $\tau+1$. $L(A)]_{\tau+1} = E_2^{\tau+1}$. Лемма 1.8 доказана.

Доказательство леммы 1.9.

Пусть моменты времени i и j отличимы, значит, найдутся входные слова $\alpha, \beta, |\alpha| = i, |\beta| = j - 1$ и входная буква a, такие что

$$q_i = \phi(q_1, \alpha), q_j = \phi(q_1, \alpha\beta), \psi(q_i, a) \neq \psi(q_j, a), q_i \in Q_i, q_j \in Q_j$$

По построению $\rho = \rho(A)$ для $d_0 < i < j < \rho$ имеем $Q_i = Q_{i+\rho}, Q_j = Q_{j+\rho}$, Можно считать, что $|\alpha| = i + l\rho, |\beta| = j + l\rho$, откуда следует что моменты времени $i + l_1\rho$ и $j + l_2\rho$ при $i < j$ отличимы. Лемма 1.9 доказана.

Глава 2

Задача выразимости для расширенной суперпозиции. Цикловые индексы автомата.

2.1 Разрешимость задачи выразимости констант для расширенной суперпозиции.

Определение 2.1 *Автоматную функцию G_0, задаваемую уравнениями*

$$\begin{cases} q(1) = 0, \\ q(t+1) = a(t), \\ b(t) = q(t), \end{cases}$$

назовём автоматной функцией нулевой задержки.

Определение 2.2 *Пусть $M \in P$. Обозначим $< M >= [M \cup \{P_2, G_0\}]$ и будем называть замыканием M относительно расширенной суперпозиции*

Автономной назовём автоматную функцию с функцией переходов, несущественно зависящей от входа. Класс автономных автоматных функций обозначим через V. Заметим, что $K \subset V$.

Определение 2.3 *Пусть сверхслово β можно представить в виде $\beta = \gamma\alpha^{\infty}$. Выберем из всех таких представлений такое, что γ и α имеют наименьшую длину. Для выбранного представления назовем γ - наименьшим предпериодом сверхслова β, а α наименьшим периодом сверхслова β, а слова вида $\underbrace{\alpha\alpha...\alpha}_{n}$ будем называть периодом сверхслова β, здесь $n \in N$. Обозначим $|\alpha|$ длину слова α.*

Для множества константных автоматных функций $K' \subseteq K$ обозначим через $\Theta(K')$- множество длин минимальных периодов сверхслов $\{\beta_{K_i} : K_i \in K'\}$.

Мы будем рассматривать следующие задачи: по конечному множеству автоматов $M \subset P$ и $\beta \in K$ проверить, верно ли что

$$1)\beta \in < M >$$
$$2)|\ \Theta(< M > \cap K)\ | < \infty$$

Также опишем множество $\Theta(< M > \cap K)$.

Замечание 2.1 *Для множеств автоматных функций, содержащих фиксированную добавку из задержки и всех булевых функций, получаем что мощность множества выразимых констант всегда равна бесконечности (за счет увеличения предпериода функцией задержки), поэтому для второй задачи мы рассматриваем мощность множества минимальных периодов.*

Лемма 2.1 *Пусть $K_1, K_2 \in K$, причем $|K_2| \mid |K_1|$. Тогда $K_2 \in < K_1 >$*

Лемма 2.1 показывает, что имея в замыкании хотя бы одну константу периода l, мы можем выразить любую константу периода делящего l.

Имеют место

Замечание 2.2 *Пусть* $|\Theta(< M > \cap K)| < \infty$, *тогда* $\Theta(< M > \cap K) = \{l \in N : l | max(\Theta(< M > \cap K))\}$

Замечание 2.3 *Пусть* $K_1, K_2 \in K$. *Тогда* $max(\Theta(< \{K_1\} \cup \{K_2\} >)) = HOK(max(\Theta(K_1)), max(\Theta(K_2)))$.

Фактически конечное $K' \subset K$ имеет множеством периодов делители одного числа $l = max(\Theta(K'))$. Тем самым всякое конечное множество константных функций таково, что $< K' >=< \{\beta_l\} >$, где β_l - константа периода l.

Имеет место

Теорема 2.1 [20] *Автоматная функция* M *с числом состояний* n, *преобразует периодическое сверхслово* $\alpha \in A^*$ *с наименьшей длиной периода* τ *в периодическое сверхслово с наименьшей длиной периода вида* θm, *где* θ - *делитель числа* τ, $m \in \{1, ..., n\}$

Данная теорема называется теоремой об удлинении периода констант автоматом. Из неё следует, что множество длин периодов констант, выразимых автоматом, имеет вид $2^{l_1}3^{l_2}...p_i^{l_{i-1}}$, где p_i - простые числа, $p_i \leq |Q|$, а l_i - натуральные числа.

Для некоторого автомата M и произвольного слова $\alpha \in A^*$ обозначим через $s_\alpha = \phi(q, \alpha)$ - подстановку на множестве состояний, задаваемую этим словом, π_α - разбиение множества состояний Q на классы отличимости $Q_1, ...Q_s$ этим словом. Состояния q_i и q_j принадлежат одному классу отличимости, если $\overline{\psi}(q_i, \alpha) = \overline{\psi}(q_j, \alpha)$.

Обозначим $e_\alpha = (s_\alpha, \pi_\alpha)$. Пусть $E_l = \{e_\alpha, |\alpha| = l\}$.

Рассмотрим последовательность $n_1, n_2, ..., n_k, ...$ натуральных чисел, связанную с автоматом M, где n_{i+1} получается из n_i следующим рекурсивным способом.

Пусть $c_i = \{\alpha_i\}$ - множество сверхслов с длиной периода $l|n_i$. Рассмотрим множество - $M(c_i)$ выходных сверхслов автомата M после подачи на него сверхслов из c_i . Очевидно, что

$\Theta(M(c_i))$ - конечно. Тогда положим $n_{i+1} = HOK(\Theta(M(c_i)))$. Из замечаний 2.2,2.3 следует, что n_i - максимальная длина периода констант, выразимых схемой глубины i, если не учитывать в схеме автоматы без памяти.

По построению $n_i | n_{i+1}$. Далее мы докажем, что $m_i = \frac{n_{i+1}}{n_i}$ - периодическая последовательность.

Лемма 2.2 *Пусть для некоторых* l, m $E_l = E_m$, *тогда для любого* $k \in N$ $E_{lk} = E_{mk}$.

Доказательство: Без ограничения общности покажем, что $E_{lk} \subseteq E_{mk}$. Для этого покажем, что $\forall \alpha, |\alpha| = lk$ $\exists \alpha_1, |\alpha_1| = mk$, т.ч. $e_\alpha = e_{\alpha_1}$. Пусть $\alpha = \beta_1 ... \beta_k$, где $|\beta_i| = l$. Тогда $s_\alpha = s_{\beta_1} * ... * s_{\beta_k}$, а π_α будет получаться сначала как разбиение, задаваемое β_1, затем как измельчение этого разбиения разбиением, задаваемым словом $\beta_1\beta_2$ и т.д. Для $\forall e_{\beta_i} \in E_l$ $\exists e_{\gamma_i} \in E_m$, т.ч. $e_{\beta_i} = e_{\gamma_i}$. Рассмотрим слово $\alpha_1 = \gamma_1 ... \gamma_k$. Для него выполнено $e_\alpha = e_{\alpha_1}$. Действительно $s_{\alpha 1} = s_{\gamma 1} * ... * s_{\gamma k}$, а π_{α_1} будет получаться сначала как разбиение, задаваемое γ_1, затем как измельчение этого разбиения разбиением $\gamma_1\gamma_2$ и т.д.

Таким образом $E_{lk} \subseteq E_{mk}$, обратное включение доказывается аналогично. Лемма 2.2 доказана.

Лемма 2.3 m_i - *периодична*

Доказательство: Пусть нашлись n_i, n_j, такие, что $E_{n_i} = E_{n_j}$. Из построения m_i следует, что m_i - это фактически длина максимального удлинения, получаемого при подаче слов длины n_i на автомат M и затем взятия НОК этих удлинений. Очевидно, что множество удлинений однозначно задается множеством E_{n_i}. Таким образом $m_i = m_j$ и из леммы 2.2 следует, что $E_{n_{i+1}} = E_{n_{j+1}}$, а таким образом $m_{i+1} = m_{j+1}$ и лемма 2.3 доказана.

Теперь определим *цикловые индексы* автомата через алгоритм их вычисления

1. Вычисляем последовательность (n_i, E_i) до тех пор, пока не найдутся $j < i$, такие, что $E_{n_i} = E_{n_j}$.

2. Назовем $b = n_j$ - безусловным цикловым индексом автомата, $q = \frac{n_i}{n_j}$ - главным цикловым индексом автомата.

Теорема 2.2 *Пусть M - автоматная функция, тогда*

$$\Theta(< M > \cap K) = \bigcup_{i=1}^{\infty} \{t | bq^i\}, \tag{2.1}$$

где b,q - цикловые индексы автомата M.

Доказательство: Пусть константа β содержится в замыкании нашего множества. Рассмотрим схему, выражающую данную константу. Пусть глубина этой схемы равна L. Тогда по построению последовательности n_i и из леммы об удлинении периодов констант следует что $\Theta(\beta)|n_L$.

Рассмотрим произвольную константу периода bq^i. По леммам 2.2, 2.1, а также по построению чисел b, q данная константа выразима схемой подходящей глубины.

Теорема 2.2 доказана

Из теоремы 2.2 следует

Теорема 2.3 *Пусть $M \in P$ и $\beta \in K$, тогда существует алгоритм, позволяющий проверить свойство $\beta \in < M >$*

Следствие 2.1 *Пусть M - автоматная функция, тогда существует алгоритм, позволяющий проверить свойство $|\ \Theta(< M > \cap K)\ | < \infty$*

Доказательство:Если главный цикловый индекс больше 1, то выразимо бесконечное число констант. Если равен 1, то конечное.

Следствие 2.2 *Пусть M - автоматная функция и v - автономная автоматная функция, тогда существует алгоритм, позволяющий проверить свойство $v \in < M >$*

Доказательство:

Определение 2.4 *Длина периода автономного автомата - длина периода его функции переходов.*

Лемма 2.4 *Пусть v_l - некоторый приведенный автономный автомат с минимальной длиной периода l, k_l - константный автомат с минимальной длиной периода l, тогда для произвольного автомата M выполнено*

$k_l \in < M > \Leftrightarrow v_l \in < M >$

Доказательство: Для доказательства достаточности построим явно автомат v_l через k_l, булевы функции и задержки. Пусть в разных состояниях $q_1, ..., q_n$автоматной функции v_l реализуются разные булевы функции $\psi_1, ..., \psi_n$, причем $\psi_1, .., \psi_l$ повторяются в периоде. По лемме 2.1 выразимы константные автоматные функции

$K_1 = (\underbrace{10..0}_{l})^\infty$, $K_2 = (\underbrace{01..0}_{l})^\infty ..., K_l = (\underbrace{00..1}_{l})^\infty$.

Тогда v_l выразима формулой

$$v_l = \vee(\wedge(K_1, \psi_1), \wedge(K_2, \psi_2), ..., \wedge(K_m, \psi_m)),$$

где $\vee$ - дизьюнкция, а $\wedge$ - коньюнкция, .

Для доказательства необходимости применим метод доказательства от противного. Без ограничения общности будем считать, что автомат v_l имеет один вход. Докажем, что возможно получить схему, на выходе которой будет реализовываться константа периода l. Пусть это невозможно. Рассмотрим параллельное соединение двух автоматов v_l. На вход первого подадим 0^∞, на вход второго 1^∞.На выходе получим последовательность пар (x, y), где $x, y \in \{0, 1\}$. Пусть эта последовательность имеет период, меньший, чем l, без ограничения общности $l/2$. Тогда $\psi_1 = \psi_{l/2+1}, \psi_2 = \psi_{l/2+2} ..., \psi_{l/2} = \psi_l$, а это противоречит приведенности автомата v_l. Лемма доказана

Следствие 2.2 следует из теоремы 2.2 и из леммы 2.4.

Непосредственно из определения цикловых индексов индексов следует необходимое условие выразимости

Теорема 2.4 (Необходимое условие выразимости) *Пусть* R_1, R_2- *конечные множества автоматов и* $R_2 \in [R_1]$. b_1, q_1, b_2, q_2 - *цикловые индексы* R_1 *и* R_2 *соответственно. Тогда*

$$\bigcup_{i=1}^{\infty}\{t|b_2q_2^i\} \subseteq \bigcup_{i=1}^{\infty}\{t|b_1q_1^i\}$$

и

$$\Theta(< R_2 > \cap K) \subseteq \Theta(< R_1 > \cap K)$$

.

Заметим, что Необходимое условие выразимости не является достаточным. Контрпримером является пример 3 из параграфа 2 главы 2 "Цикловые индексы автомата"

2.2 Цикловые индексы автомата

Из описанного в предыдущей главе алгоритма описания множества периодов выразимых констант, а также теоремы 2.2 следует, что для произвольного автомата M существуют натуральные $b_M, q_M \in \mathbf{N}$, такие что

$$\Theta(< M > \cap K) = \{t : t|b_Mq_M^i, i = 0, 1, ..\}.$$

Определение 2.5 *Число* q_M *назовем главным цикловым индексом автомата* M, b_M - *частным цикловым индексом автомата* M.

Из описания алгоритма, вычисляющего цикловые индексы следует, что b_M и q_M вычислимы по M за конечное время. Заметим, что q_M^2, q_M^3,..., q_M^t,... также являются главными

цикловыми индексами, а bq_M^2, bq_M^3,..., bq_M^t также удовлетворяют (2.1). Минимальные b_M и q_M, удовлетворяющие уравнению (2.1) назовем минимальными цикловыми индексами автомата M.

Пусть некоторые цикловые индексы автомата M имеют вид $b_M = p_1^{i_1} p_2^{i_2} ... p_s^{i_s}$, $q_M = p_1^{j_1} p_2^{j_2} ... p_s^{j_s}$ и $HOD(b_M, q_M) = p_1^{k_1} p_2^{k_2} ... p_s^{k_s}$ и $k_1 > 0, ..., k_t > 0, k_{t+1} = 0 ... k_s = 0$. Тогда минимальные цикловые индексы будут следующими $b_M^{min} = p_{t+1}^{i_{t+1}} ... p_s^{i_s}$, $q_M^{min} = p_1 p_2 ... p_t$

Приведем несколько примеров вычисления цикловых индексов автоматов, а также оценим сложность вычисления цикловых индексов при росте числа состояний автомата.

Пример 1 Автомат Z_3

Рассмотрим автомат, изображенный на рисунке 2.1

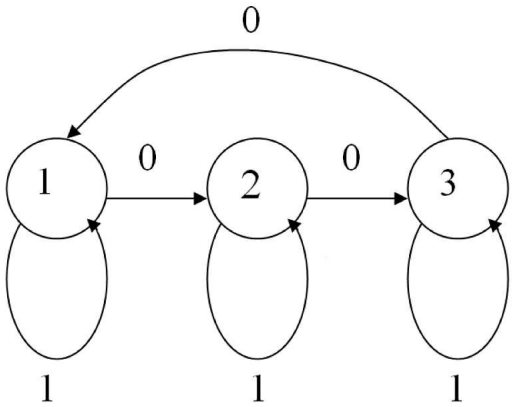

Рис. 2.1:

Будем действовать согласно алгоритму A.

1. Рассмотрим слова длины 1 - $\{0, 1\}$. Им соответствуют следующие пары (подстановка, разбиение) - E_1

$0 - ((123), (\{1\}, \{2\}, \{3\}))$

$1 - ((i), (\{1\}, \{2\}, \{3\}))$, где e - тождественная подстановка.

2.Т.к. подстановка (123) имеет порядок 3 и дает полное разбиение, на 2-м шаге мы получим все слова длины 3 и соответствующие им пары (подстановка, разбиение) - E_3
$000 - ((i), (\{1\}, \{2\}, \{3\}))$
$001 - ((132), (\{1\}, \{2\}, \{3\}))$
$010 - ((132), (\{1\}, \{2\}, \{3\}))$
$011 - ((123), (\{1\}, \{2\}, \{3\}))$
$100 - ((132), (\{1\}, \{2\}, \{3\}))$
$101 - ((123), (\{1\}, \{2\}, \{3\}))$
$110 - ((123), (\{1\}, \{2\}, \{3\}))$
$111 - ((i), (\{1\}, \{2\}, \{3\}))$

3. Согласно алгоритму на 3-м шаге мы должны были бы рассмотреть подстановки, задаваемые словами длины 9. Однако это было бы проблематично в рамках данной работы, т.к. таких слов 512. Поэтому заметим лишь, что новых подстановок по сравнению со словами длины 3 они не дадут.

Согласно алгоритму получаем $E_3 = E_9$, поэтому все множество констант может быть описано формулой

$$\Theta(< Z_3 > \cap K) = \{t : t|3^i, i = 0, 1, ..\}.$$

Для данного автомата главный цикловый индекс q равен 3, частный цикловый индекс b равен 1.

Пример 2 Рассмотрим автомат B, изображенный на рисунке 2.2

Аналогично первому примеру рассмотрим последовательность множеств E_i
1.E_1
$0 - ((12), (\{1\}, \{2, 3\}))$
$1 - ((23), (\{2\}, \{1, 3\}))$
2.E_2

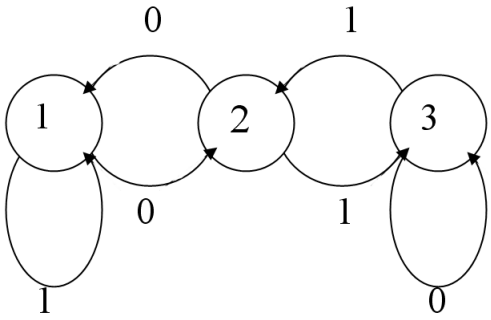

Рис. 2.2:

$00 - ((i), (\{1\}, \{2\}, \{3\}))$
$01 - ((132), (\{1\}, \{2, 3\}))$
$10 - ((123), (\{2\}, \{1, 3\}))$
$11 - ((i), (\{1\}, \{2\}, \{3\}))$
3.E_6. Рассмотрим всевозможные слова длины 6 - это всевозможные комбинации слов длины 2 по 3. Обозначим перестановки, задаваемые $01 - t_1$, $10 - t_2$. Получим возможные варианты
$iii = i$,
$iit_n = it_ne = t_nii = t_n$,
$it_nt_m = t_nit_m = t_nt_mi = i, n \neq m$,
$et_nt_n = t_net_n = t_nt_ne = t_m, n \neq m$,
$t_nt_nt_m = t_nt_mt_n = t_mt_nt_n = t_n, n \neq m$,
$t_nt_nt_n = i$.

Получаем, что множество подстановок, задаваемых словами длины 6, совпадает с множеством подстановок, задаваемых словами длины 2. Т.к. разбиения, полученного на длине 2, уже было достаточно для того, чтобы отличить состояния автомата, то его же будет и достаточно для слов длины 6. Поэтому можно считать, что $E_6 = E_2$, и все множество констант может быть описано формулой

$$\Theta(< B > \cap K) = \{t : t|2 * 3^i, i = 0, 1, ..\}.$$

Для данного автомата главный цикловый индекс q равен 3, частный цикловый индекс b равен 2.

Пример 3. Пусть $M_1 = Z_{30}$ по аналогии с примером 1, а $M_2 = A_5$ - автомат, изображенный на рис 2.3.

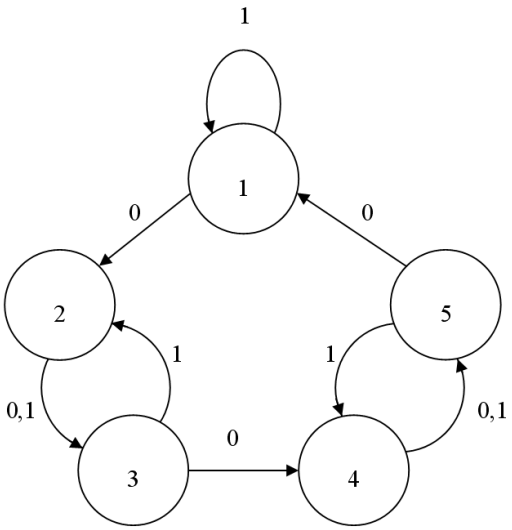

Рис. 2.3:

M_1 и M_2 удовлетворяют условию теоремы 2.4, т.к. $b_{M_1} = b_{M_2} = 1$, $q_{M_1} = q_{M_2} = 30$, однако M_2 не выразим через M_1.

Как и для любого алгоритма представляет интерес сложность его реализации и возможность за обозримое время на вычислительной машине решить задачу выразимости констант.

Теорема 2.5 *Сложность алгоритма, решающего задачу выразимости для констант асимптотически не больше, чем* 2^{n^n}*, где* n *- число состояний автомата.*

Доказательство: Для завершения алгоритма, решающего задачу выразимости для констант, необходимо выполнение

условия совпадения двух подмножеств множества пар (подстановка, разбиение) $E_n = E_m$. Оценим, сколько всего таких пар существует для фиксированного числа состояний автомата.

Число подстановок(S_n) - это число наборов из n элементов, где на каждом месте может стоять любой из n элементов. Всего их n^n.

Число разбиений множества(Π_n) - это известное *число Белла*[22]

$$|\Pi_n| = B_n = \sum_{k=0}^{n} \frac{1}{k!} \sum_{j=0}^{k} (-1)^{(k-j)} \binom{k}{j} j^n$$

.

Для числа Белла известна оценка[23]

$$B_n < \left(\frac{0.792n}{ln(n+1)} \right)^n$$

Используя эти 2 формулы получаем

$$E_n \ll n^n$$

Или для количества подмножеств E_n.

$$2^{E_n} \ll 2^{n^n},$$

что и требовалось доказать.

Данный алгоритм, конечно, очень медленный и на практике используется его упрощение, позволяющее значительно сократить сложность поиска цикловых индексов.

Упрощение алгоритма Построим алгоритм сначала для автомата Медведева. Пусть b и q - цикловые индексы автомата M с n состояниями. По построению $q = p_1 p_2 ... p_s$, где p_i - простые числа, меньшие n. Тогда для любого p_i выполнено *условие(*)* - существуют $N_i, b_i \in N$ и слова $|\alpha_i| = b^{N_0}$, $|e_{p_i}| = b^{N_0}$, такие что α_i порождает в автомате A цикл длины b_i на некотором множестве состояний, причем $p_i | b_i$ и $b_i < n$, а e_{p_i} на том

же множестве состояний ведёт себя как тождественная подстановка. Причем период сверхслова $A(\alpha_i)$ делит p_i, если A стартует с одного из отмеченного множества состояний.

Непосредственной проверкой можно проверить, что приведенные условия выполнены тогда и только тогда когда b и q - цикловые индексы автомата. И таким образом мы можем перебрать все $p_i < n$ и определить, какие из них могут быть делителями главного циклового индекса автомата и каковы длины слов, на которых это проявляется.

Итак, пусть p_i - простое число, такое что $p_i < n$. Тогда нам нужно перебрать все $b_i : p_i | b_i < n$ и все подмножества множества состояний мощности b_i и построить множества слов, удовлетворяющих условию(*). Наша цель состоит в том, чтобы найти такую длину слов из A^*, начиная с которой для слов большей длины новых циклов не будет.

Запишем условия, накладываемые на слова α_i и e_i.
1.α_i - $\exists(q_0, q_1, ..., q_{b_i}) : \phi(q_0, \alpha_i) = q_1, \phi(q_1, \alpha_i) = q_2, ..., \phi(q_{b_i}, \alpha_i) = q_0$.
2.e_i - $\phi(q_0, e_i) = q_0, \phi(q_1, e_i) = q_1, ..., \phi(q_{b_i}, e_i) = q_{b_i}$
3.Период сверхслова $A(\alpha_i)$ равен b_i периодам сверхслова α_i

Для описания множества циклов автомата построим следующий граф. Пусть $|Q| = n$, $A = \{0, 1\}$. Начальной вершиной графа будет вектор $(1, 2, ..., n)$. Вершинами вектора $(q_1, ..., q_n)$, где $q_i \in \{1...n\}$. Из вершины $(q_1, ..., q_n)$ выходит 2 ребра в вершины $(\phi(q_1, 0), ..., \phi(q_n, 0))$ и $(\phi(q_1, 1), ..., \phi(q_n, 1))$.

Для описания всевозможных циклов в автомате M нужно провести следующую процедуру.
1. Рассматриваем все пути, ведущие из корня - считаем его начальной вершиной. Отмечаем все вершины, в которых на некотором упорядоченном подмножестве состояний $(q_1, ..., q_i)$ произошла перестановка $(q_i, ..., q_{i-1})$ или сохранение $(q_1, ..., q_i)$. Считаем эти вершины финальными.
2. С помощью регулярного выражения описываем всевозмож-

ные слова, на которых есть перестановки и сохранения.
3.Переписываем данное выражение, заменяя слова на длины слов, а перестановки на их порядок.
4. Для описания множества выразимых констант теперь достаточно описать полученное регулярное выражение, имея ввиду, что изначально у нас в распоряжении только константа периода 1.

Пример 4

Рассмотрим автомат (рис 2.4)

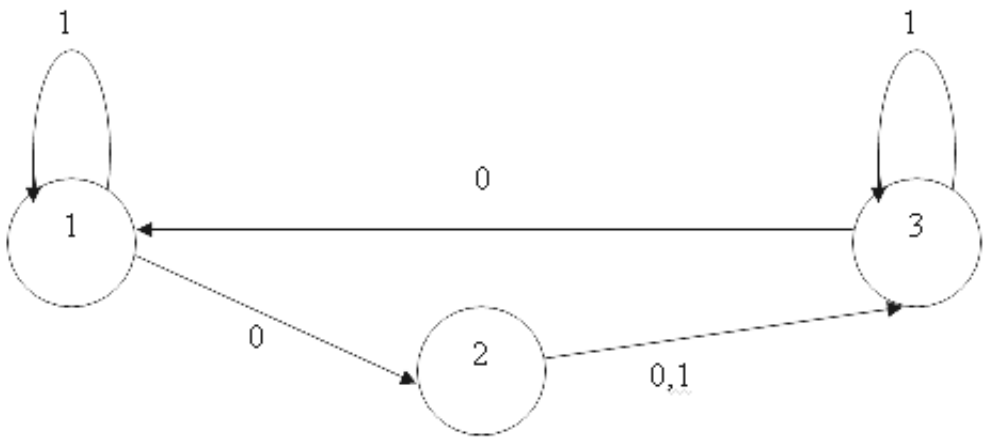

Рис. 2.4:

Для данного автомата построим граф, описанный выше (рисунок 2.5).

Теперь опишем все слова, дающие циклы в нашем автомате
Циклы
1.Цикл длины 3 дают состояния 2 и 4, соответствующие им константы 0 и 00.
2. Цикл длины 2 дают состояния 6 (слово 10) и 22 (слово 001010) - на (12), 5 (слово 01) и 11 (слово 101) на (13), 18

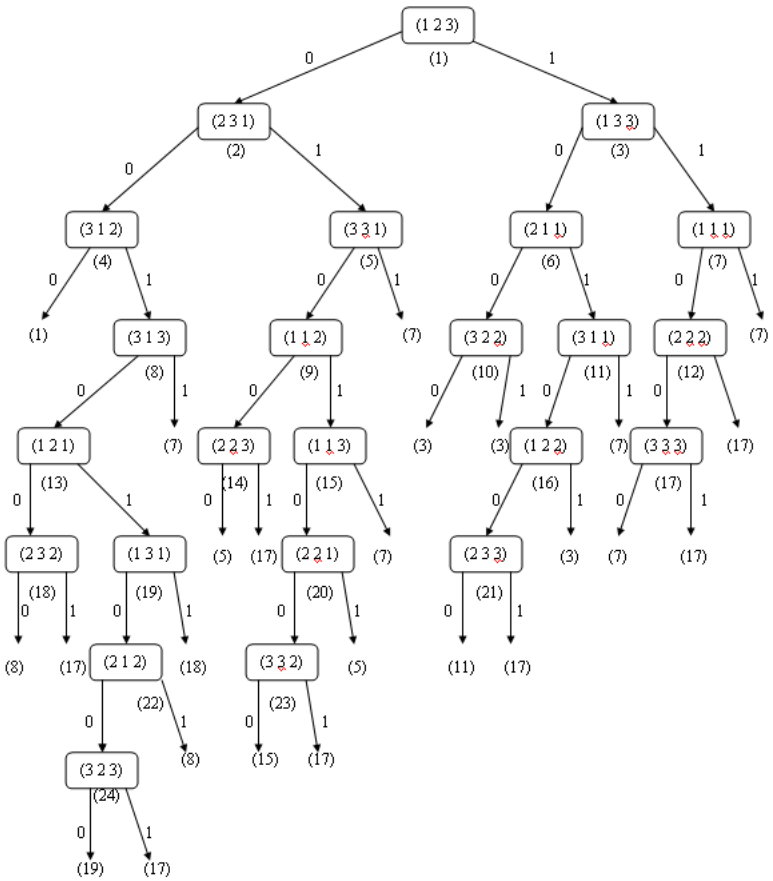

Рис. 2.5:

(слово 00100) и 23 (слово 010100) на (23)

Тождественные подстановки

1. Тождественную подстановку длины 3 дает состояние 1 на слове (000)

2. Тождественную подстановку длины 2 дают состояния 16 (слово 1010) и 13 (слово 0010) на (12), 3 (слово 1) и 15 (слово 0101) на (13), 14 (слово 0100) и 24 (слово 0010100). А также состояние 1 и слово 000 на всех трех.

Исходя из этого циклы длины 3 дает только слова длины 1. Циклы длины 2 дают слова вида $2+4n, 2+n, 5+4n, 6+4n, 5+$

$7n, 6 + 7n$ или что то же самое $2 + n$. Таким образом 2 будет главным цкиловым индексом этого автомата, т.к. удлинение в 2 раза есть на любых длинах, начиная с 2. 3 будет частным цикловым индексом этого автомата.

В общем случае (не автомата Медведева), вместе с вектором состояний в вершинах графа необходимо отмечать разбиение, задаваемое входным словом. Т.к. при наращивании слова разбиение не убывает, всего максимальное количество состояний данного графа увеличивается в n раз.

2.3 Задача выразимости автомата Z_n

Определение 2.6 *Автоматом* Z_n, $n \in N$ *будем называть автомат Медведева вида*
$(\{0,1\}, \{1,...,n\}, \{1,...,n\}, \phi, \psi, 1)$
$\phi(i,1) = i, \phi(i,0) = (i+1)\ mod\ n$
$\psi(i,0) = \psi(i,1) = i.$

Его диаграмма показана на рис 2.6

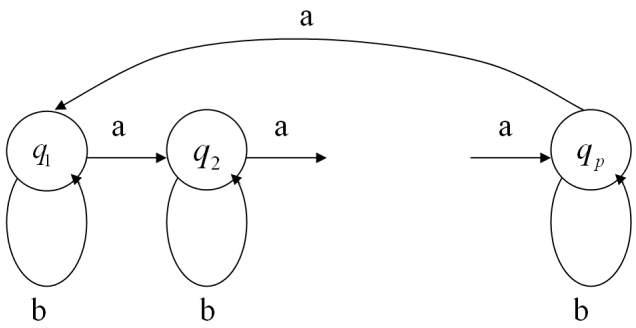

Рис. 2.6:

Определение 2.7 [17] *Пусть* f *и* g *- автоматы с одинаковым числом входов и одинаковым числом выходов. Скажем,*

что автоматная функция g копирует автоматную функцию f, если найдутся такие натуральные n, j, k $(n \leq j)$, что для любого $l = 0, 1, 2, ...$ и любой входной последовательности достаточной длины значение автоматной функции g в момент $j + kl$ совпадает со значением автоматной функции f в момент $n + kl$, т.е. $f(n + kl) = g(j + kl)$.

Лемма 2.5 [17] *(Лемма о копировании) Пусть g - автоматная функция Медведева и g копирует f с параметрами n, j, l, тогда $f \in [g \cup \{G_0, P_k, (\underbrace{1...0}_{l})^{\infty}\}]$*

Теорема 2.6 *Пусть $M \in P$, тогда Z_n выразим через $< M >$ тогда и только тогда, когда n делит некоторую степень главного циклового индекса M.*

Теорема 2.7 *Пусть $M \in P$, тогда существует алгоритм, позволяющий проверить свойство выразимости Z_n через $< M >$.*

Доказательство теорем.

Доказательство теоремы 2.6:
Необходимость: Пусть $Z_n \in \langle M \rangle$, тогда

$$\Theta(M) \supseteq \Theta(Z_n) = \{n^i, i = 0, 1, ..\},$$

т.к. очевидно $\Theta(Z_n) = \{n^i, i = 0, 1, ..\}$, но тогда $n | q_M^i$ для некоторого i.

Достаточность: Докажем сначала, что выразим автомат Z_{q_M}, так как Автомат Z_n выразим как суперпозиция Z_{q_M} и функции $h(q) = q \ mod \ n$.

Для доказательства выразимости Z_{q_M} построим схему из автоматов $\langle M \rangle$, которая "копировала"бы автомат Z_{q_M}. Для постороения этой схемы воспользуемся алгоритмом построения

цикловых индексов, а также несколькими вспомогательными функциями.

По построению b_M и q_M существует слово α длины b_M и схема Σ из $\langle M \rangle$ такие, что период $\beta = \Sigma(\alpha)$ равен $b_M q_M$. Из этого следует, что α задает на состояниях схемы Σ подстановку $s_1 \to s_2, s_2 \to s_3 ..., s_{q_M} \to s_1$, при этом состояние s_1 является достижимым в схеме. Без ограничения общности будем считать, что s_1 - начальное состояние.

$\breve{\alpha} = \underbrace{\alpha\alpha...\alpha}_{q_M}$ является словом, попарно отличающим состояния $(s_1, s_2, ..., s_{q_M})$. Действительно, пусть это не так и состояния s_i и s_j неотличимы словом $\breve{\alpha}$, тогда период β равен $b_M(j-i)$, что неверно. Таким образом $\breve{\alpha} = \underbrace{\alpha\alpha...\alpha}_{q_M}$ - слово, задающее единичную подстановку на $s_1, ..., s_{q_M}$ и отличающее все эти состояния.

Из алгоритма построения цикловых индексов следует, что $E_{b_M} = E_{b_M * q_M}$. А значит для любого слова α длины b_M существует слово β длины $b_M * q_M$, такое, что $\phi_\alpha = \phi_\beta$ для M, причём α^∞ и β^∞ выразимы через $< M >$.

Рассмотрим слова $\bar{\alpha} = \underbrace{\breve{\alpha}\breve{\alpha}...\breve{\alpha}}_{q_M}$ и $\bar{\beta} = \underbrace{\breve{\alpha}\breve{\alpha}...\breve{\alpha}}_{q_M - 1}\beta$. Заметим, что слова $\bar{\alpha}$ и $\bar{\beta}$ задают соответственно единичную подстановку и циклическую подстановку порядка q_M на состояниях $s_1, s_2, ..., s_{q_M}$, при этом состояния попарно отличимы словами $\bar{\alpha}$ и $\bar{\beta}$. Заметим также, что $|\bar{\alpha}| = |\bar{\beta}| = b_M * q_M^2$.

Обозначим i - единичную подстановку на состояниях автомата Z_{q_M} (она задается 1), t - подстановку $(q_2, q_3, ..., q_n, q_1)$ (она задается 0). Обозначим $\bar{0} = \underbrace{11...1}_{b_M q_M^2}$, $\bar{1} = \underbrace{11...1}_{b_M q_M^2 - 1}\ 0$. Заметим, что $\bar{0}$ задает подстановку i, $\bar{1}$ - подстановку t.

Теперь построим несколько вспомогательных функций, позволяющих отобразить входные слова в алфавите $\{0, 1\}$ в нужные нам входные слова в алфавите $\bar{\alpha}, \bar{\beta}$.

Пусть γ - произвольное слово длины $b_M * q_M^3$. На состояниях автомата Z_{q_M} слово γ задаёт одну из q_M подстановок - $(i, t, t^2, ..., t^{q_M-1})$. Пусть γ задает подстановку t^i. Тогда $\overline{f(\gamma)} = \underbrace{\bar{1}\bar{1}...\bar{1}}_{i}\underbrace{\bar{0}\bar{0}...\bar{0}}_{q_M-i}$. Заметим, что $\overline{f(\gamma)}$ задает ту же подстановку, что и γ на состояниях Z_{q_M}.

g - функция к-значной логики, такая что $g(\bar{0}) = \bar{\alpha}$,$g(\bar{1}) = \bar{\beta}$.

G_0^i - задержка на i тактов, в первые i тактов выдающая 0.

$G_{\breve{\alpha}}^i$ - задержка на i тактов, в первые i тактов выдающая $\breve{\alpha}$.

Обозначим через S - автомат с $b_M q_M^3$ входами - переключатель входов. В первые $b_M q_M^3$ тактов времени он выдаёт по циклу буквы слова $\breve{\alpha}$, а после по циклу с периодом $b_M q_M^3$ передает i-й вход на выход.

Несложно понять, что автомат S может быть получен суперпозицией счетчиков по модулю $b_M q_M^3$, булевых функций и задержек.

H - функция k-значной логики, которая по выходу автомата Σ после подачи слова $\breve{\alpha}$ определяет состояние автомата Σ после подачи слова $\breve{\alpha}$, А затем по состоянию и входному слову длины $b_M(q_M^3 - q_M)$ определяет состояние автомата Σ через $b_M(q_M^3 - q_M)$ тактов времени, а затем осуществляет отображение $s_1 \to q_1, s_2 \to q_2, , s_{q_M} \to q_{q_M}$.

Рассмотрим следующую схему Σ_K (рис.2.7)и докажем, что автоматная функция, реализуемая этой схемой, копирует автоматную функцию Z_{q_M}.

Рассмотрим $j = 0, n = 2q_M b_M, k = q_M^3 b_M$ и докажем, что схема Σ_K копирует автомат A_{q_M} с параметрами j, n, k. Для этого рассмотрим произвольное входное слово $\gamma = \gamma_1\gamma_2...\gamma_{q_M^3 b_M} r$ длины $q_M^3 b_M r$ для некоторого r. Докажем, что выход автомата Σ_K в момент времени $q_M^3 b_M r + 2q_M b_M$ совпадает с выходом автомата Z_{q_M} в момент времени $q_M^3 b_M r$ при подаче на оба автомата слова γ.

Докажем это утверждение по индукции

1.В момент времени 0 выход автомата Z_{q_M} q_1. В момент времени $2q_M b_M$ автомат Σ находится в состоянии s_1, т.к. на его вход поступает входное слово $\breve{\alpha}$, а $\phi_\Sigma(s_1, \breve{\alpha}) = s_1$. $H(s_1, \underbrace{\breve{\alpha}, ..., \breve{\alpha}}_{b_M(q_M^3 - q_M)}) =$ q_1, т.к. функция H по выходу функции Σ после подачи слова $\breve{\alpha}$ определяет, что автомат Σ находится в состоянии s_1 и по определению функции H, на выходе у неё q_1.

2.Пусть утверждение выполнено для $n = r$, докажем, что оно выполнено для $n = r + 1$.

Пусть в момент времени $b_M q_M^3 r$ автомат Z_{q_M} находится в состоянии q_i, докажем, что тогда автомат Σ в момент времени $b_M q_M^3 (r + 1)$ находится в состоянии s_i. Действительно, по построению функций f, g и S суммарное входное воздействие на автомат Z_{q_M} за $b_M q_M^3$ тактов времени равно входному воздействию на автомат Σ, только применительно к состояниям $s_1, ..., s_{q_M}$. Плюс изначальная задержка на $b_M q_M^3$ тактов.

Пусть по входному слову длины $b_M q_M^3$ автомат Σ из состояния q_i переходит в состояние q_j, тогда функция H, фактически моделирующая работу функции переходов автомата Σ в момент времени $b_M q_M^3 (r+1) + 2 b_M q_M$ выдает q_j и копирование доказано.

Из копирования и из леммы 2.5 следует теорема 2.6. Теорема 2.6 доказана

Теорема 2.7 следует из теоремы 2.6 и определения цикловых индексов.

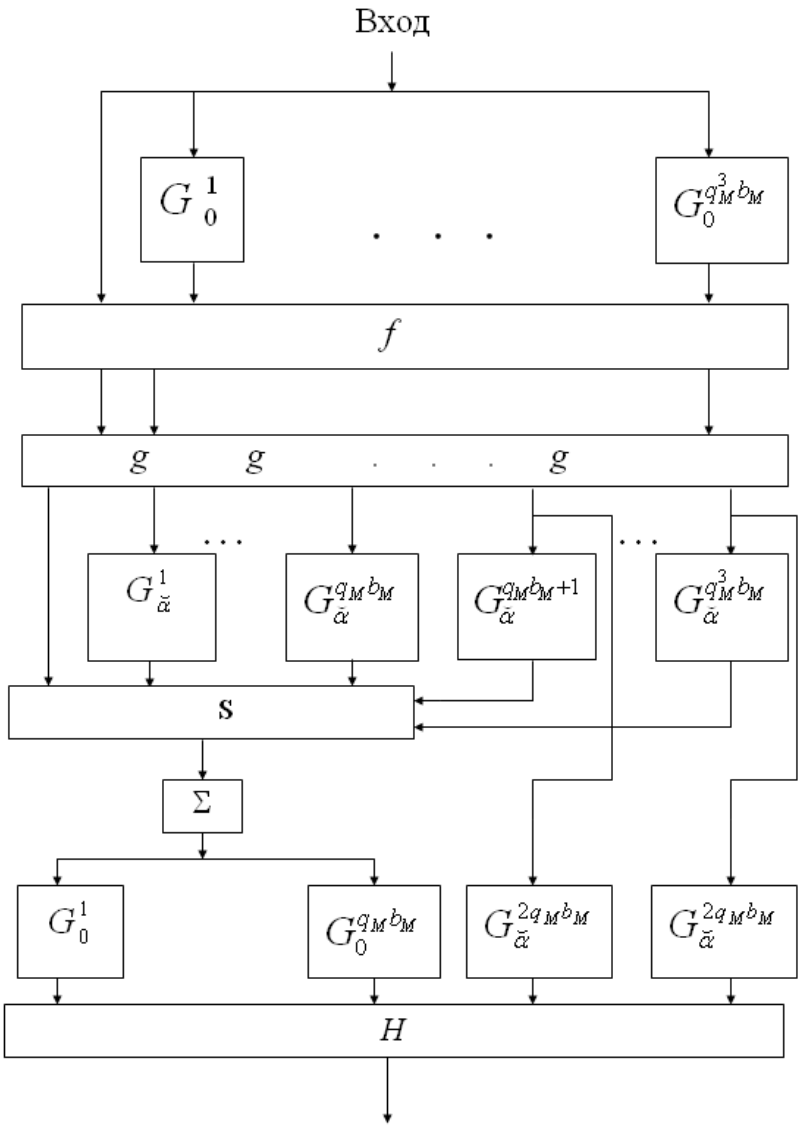
Вход
G_0^1
$G_0^{q_M^3 b_M}$
f
g g g
$G_{\tilde{\alpha}}^1$
$G_{\tilde{\alpha}}^{q_M b_M}$
$G_{\tilde{\alpha}}^{q_M b_M+1}$
$G_{\tilde{\alpha}}^{q_M^3 b_M}$
S
Σ
G_0^1
$G_0^{q_M b_M}$
$G_{\tilde{\alpha}}^{2q_M b_M}$
$G_{\tilde{\alpha}}^{2q_M b_M}$
H

Рис. 2.7:

2.4 Задача выразимости линейных автоматов

Автомат $L = (E_2^k, Q, E_2^l, \phi, \psi, q0), Q \subset E_2^n$, называется *линейным,* если

$$\begin{cases} \phi(x,q) = Aq + Bx, \\ \psi(x,q) = Cq + Dx, \\ q_0 = (0,0,...,0), \end{cases}$$

где $A : E_2^n \to E_2^n, B : E_2^k \to E_2^n, C : E_2^n \to E_2^l, DB : E_2^k \to E_2^l$ - есть линейные операторы. Матрица A называется основной матрицей линейного автомата.

Теорема 2.8 *Пусть $M \in P$, а L - линейный автомат, тогда*

$$L \in < M > \Leftrightarrow \Theta(< L > \cap K) \subseteq \Theta(< M > \cap K)$$

.

Теорема 2.9 *Задача выразимости линейных автоматов через произвольные автоматы относительно расширенной суперпозиции алгоритмически разрешима.*

Основные леммы и доказательство теорем

Лемма 2.6 [25] *Групповой линейный автомат выразим через групповой автономный автомат, Z_2 и задержку.*

Доказательство:
Пусть L - линейный групповой автомат

$$L = (E_2^k, S, E_2^l, \phi_1, \psi_1, 0), S \subset E_2^n,$$

$$\begin{cases} q' = \phi_1(x, s) = As + Bx, \\ y = \psi_1(x, s) = Cs + Dx, \\ s_0 = (0, 0, ..., 0), \end{cases}$$

где $A : E_2^n \to E_2^n, B : E_2^k \to E_2^k$ - линейные операторы. Так как L - групповой автомат, то $det(A) \neq 0$[26]. Найдется такое натуральное число t, что $A^t = I$, где I - тождественный линейный оператор и для всех $t' < t$ $A^t \neq I$. Возьмем автомат

$$G = (E_2^k, \{I, A, A^2, ..., A^{t-1}\} \times Q), E_2^l, \phi_2, \psi_2, (I, 0)).$$

Для $(Q, q) \in \{I, A, A^2, ..., A^t\} \times Q, x \in Q, u \in E_2^l$

$$\begin{cases} (Q, q)' = \phi_2(x, (Q, q)) = (Aq, q + (AQ)^{-1}Bx), \\ u = \psi_2(x, (Q, q)) = \phi_1(x, Qq) \\ q_0 = (0, 0, ..., 0), \end{cases}$$

Покажем, что автоматы L и G - эквивалентны. Пусть на входы автоматов L и G подана последовательность $x_1, x_2, ..., x_m$. Соответствующая ей последовательность состояний автомата L пусть $0, q_2, q_3, ..., q_m$, последовательность состояний автомата G $(I, 0), (Q_2, q_2), (Q_3, q_3), ..., (Q_m, q_m)$, выходная последовательность автомата L $y_1, y_2, ..., y_m$, выходная последовательность автомата G $u_1, u_2, ..., u_m$.

Покажем,что последовательности состояний автоматов L и G связаны следующим соотношением:

$$Q_i q_i = s_i, i = 1, 2, ...m.$$

Применим индукцию по длине входной последовательности. Первый шаг $I0 = 0$. Пусть $Q_i q_i = s_i$, из уравнений автомата L следует $Q_{i+1} = AQ_i, q_{i+1} = q_i + (AQ_i)^{-1}Bx_i$, тогда $Q_{i+1}q_{i+1} = AQ_i(q_i + (AQ_i)^{-1}Bx_i) = AQ_i q_i + Bx_i = As_i + Bx_i$. Из уравнений автомата G следует $s_{i+1} = As_i + Bx_i$, значит

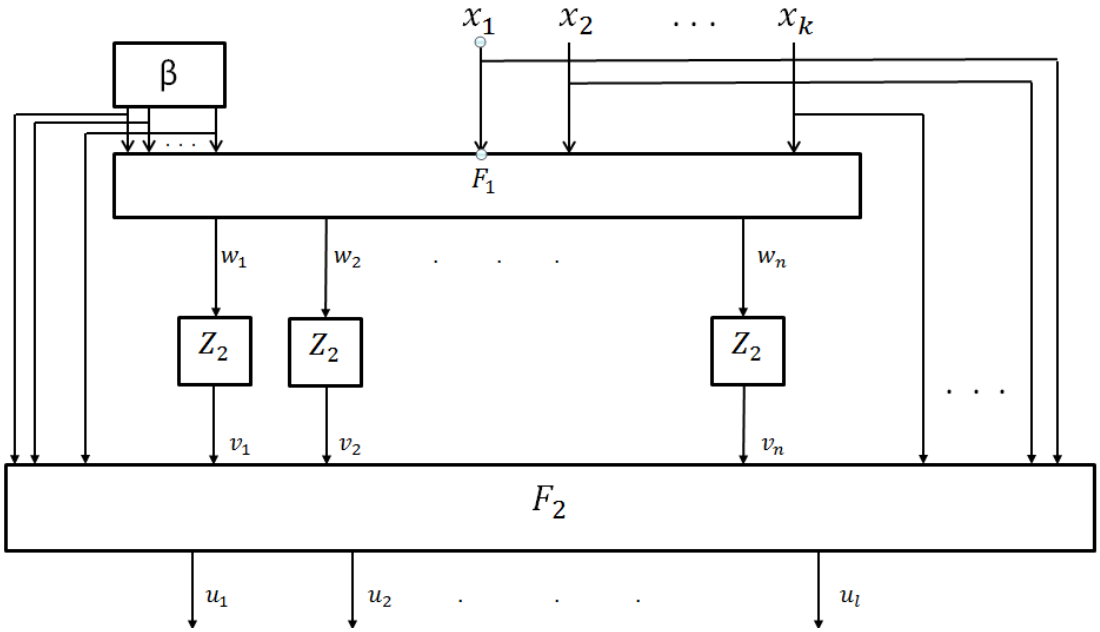

Рис. 2.8:

$Q_{i+1}q_{i+1} = s_{i+1}$. Теперь покажем, что выходные последовательности автоматов L и G одинаковы. В самом деле

$$y_1 = \phi_q(x_1, 0), u_1 = \phi_2(x_1, (I, 0)) = \phi_1(x_1, I0) = y_1,$$
$$y_2 = \phi_q(x_2, s_2), u_2 = \phi_2(x_2, (Q_2, q_2)) = \phi_1(x_2, Q_2q_2) = y_2,$$
$$y_m = \phi_q(x_m, s_m), u_m = \phi_2(x_m, (Q_m, q_m)) = \phi_1(x_m, Q_mq_m) = y_m$$

Таким образом, на произвольной входной последовательности автоматы L и G дают одинаковые выходные последовательности, значит, L и G эквивалентны. Автомат G можно представить в виде схемы, изображенной на рис 2.8.

Здесь β - автономный автомат $\beta = (\{I, A, ..., A^t\}, E_2^r, \gamma_1, \delta_1, I)$, где r - наименьшее натуральное число такое, что $t \leq 2^r$. Для $Q, Q' \in \{I, A, ..., A^t\}, z \in E_2^r$ $Q' = \gamma_1(Q) = AQ, z = \delta_1(Q)$. Функция δ_1 на A^i принимает значение $\delta_1(A^i) = a_1a_2...a_r$, где $a_1a_2...a_r$ - двоичная запись числа i.

$F_1 \in P_2$. $F_1 : E_2^r \times E_2^k \to E_2^n$, если $a_1a_2...a_r$ - двоичная запись числа i, а $x \in E_2^k$, то $F_1(a_1a_2...a_r, x) = (AA^i)^{-1}Bx$.

$F_2 \in P_2$. $F_2 : E_2^r \times E_2^n \times E_2^k \to E_2^l$. $F_1(a_1a_2...a_r, v, x) = \phi_1(x, A^i, v)$.

Лемма 2.7 [25] *Произвольный линейный автомат выразим через групповой линейный автомат и задержку.*

Доказательство:

Пусть $L = (E_2^k, Q, E_2^l, \phi, \psi, q_0), Q \subset E_2^n, q_0 = 00...0$ - линейный автомат и его уравнения

$$\begin{cases} q_1 = \phi(x, q) = Aq + Bx, \\ y_1 = \psi(x, q) = Cq + Dx \end{cases}$$

Можно выбрать такую систему координат в E_2^n, что в ней основная матрица A имеет клеточный вид[26]

$$\begin{pmatrix} A_1 & 0 & ... & 0 \\ 0 & A_2 & ... & 0 \\ . & . & . & . \\ 0 & 0 & ... & A_t \end{pmatrix} \tag{2.2}$$

,

где либо $detA_i \neq 0$, либо $A_i = \begin{pmatrix} 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 1 & ... & 0 \\ . & . & . & . & . \\ 0 & 0 & . & . & 1 \\ 0 & 0 & . & . & 0 \end{pmatrix}, i = 1, 2, ...t.$

Если r_i - порядок квадратной матрицы A_i и $q_i \in E_2^r, i = 1, 2, ..., t$, то уравнения автомата L можно записать в следующем виде:

$$\begin{cases} q_1' = A_1q_1 + B_1x, \\ q_2' = A_2q_2 + B_2x, \\ ... \\ q_t' = A_tq_t + B_tx, \\ y = \psi(x, q_1, q_2, ..., q_t) \end{cases}$$

откуда видно, что автомат L изображается схемой, изображенной на рисунке 2.9, где $T_i = (E_2^k, Q_i, E_2^{r_i}, \phi_i, \psi_i, q_0^{(i)})$, $Q_i \in E_2^{r_i}, q_0^{(i)} = 00...0$,

$$\begin{cases} q_i' = A_i q_i + B_i x, \\ u_i = \psi(x, q_i), \end{cases} i = 1, 2, ...t$$

$F \in P_2$. $F : E_2^{r_1} \times E_2^{r_1} \times ... \times E_2^{r_t} \times E_2^k \to E_2^l$. $F(u_1, u_2, ..., u_t, x) = \psi(x, u_1, u_2, ..., u_t)$. Если $detA_i \neq 0$, то автомат T_i - групповой.

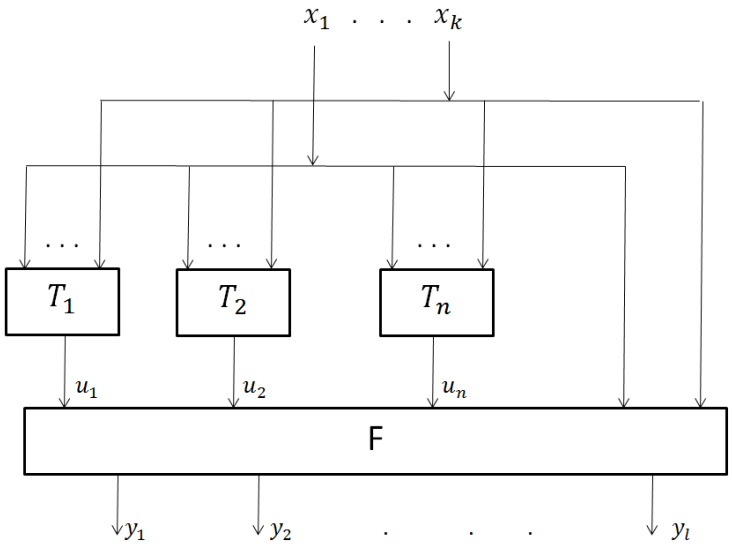

Рис. 2.9:

Пусть $A_j = \underbrace{\begin{pmatrix} 0 & 1 & ... & 0 \\ . & . & ... & . \\ 0 & 0 & ... & 1 \\ 0 & 0 & ... & 0 \end{pmatrix}}_{r_j}$

Уравнения автомата T_j можно записать в виде

$$\begin{cases} q_1 = q_2 + B_j^{(1)} x \\ q_2 = q_3 + B_j^{(2)} x \\ \dots \\ q_{r_j - 1} = q_{r_j} + B_j^{(r_j - 1)} x \\ q_{r_j} = B_j^{(r_j)} x \\ u_j = (q_1, q_2, \dots q_{r_j}) \end{cases}$$

откуда видно, что автомат T_j может быть реализован схемой, изображенной на рисунке 2.10. $B_j \in P_2$. $B_j : E_2^k \to E_2^{r_j}$.

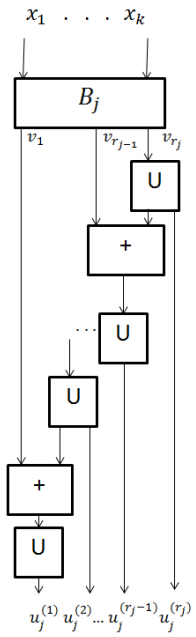

Рис. 2.10:

$B_j(x) = (B_j^{(1)} x, B_j^{(2)} x, ..., B_j^{(r_j)} x)$. G_0 - автомат задержка. $\oplus$ - двоичное сложение. Лемма доказана.

Лемма 2.8 *Пусть частный цикловый индекс линейного автономного автомата L равен b, K_b - все константные автоматы с длиной периода b, тогда если главный цикловый индекс равен 2, то:*

1.$L \in < K_b, Z_2 >$,
2.$K_b \in < L >$,
3.$Z_2 \in < L >$. *Если главный цикловый индекс равен 1, то* $L \in < K_b >$

Доказательство:Из лемм 2.6, 2.7 следует, что главный цикловый индекс линейного автомата всегда либо 1 либо 2, т.к. линейный автомат выразим через константы, Z_2, задержки и булевы функции.

Рассмотрим представление линейного автомата в виде (2.2) и соответствующую схему 2.9.

Если ни один из автоматов T_i не является групповым, то для выразимости этого автомата достаточно булевых функций и задержек. Его главный цикловый индекс в этом случае равен 1.

Пусть хотя бы один из автоматов T_i - групповой. Если все групповые автоматы автономные, то в соответствующих схемах 2.8 булева функция F_2 не зависит от входов $v_1, v_2, ..., v_n$ и такие автоматы выразимы через автомат β.

Теперь предположим, что хотя бы один групповой автомат не автономный. Обозначим его T_1 и переставим его на первый вход в схеме 2.9. Функция F при этом существенно зависит от 1-го входа. Докажем тогда, что главный цикловый индекс автомата L не может быть равен 1. Действительно, пусть частный цикловый индекс автомата L равен b, а главный цикловый индекс равен 1. Тогда все константы периода 1 переходят после подачи на автомат L в константы периодов делителей b. Пусть автомат L задается уравнениями

$$\begin{cases} q(t+1) = Aq(t) + Bx(t) \\ y(t) = Cq(t) + Dx(t) \end{cases}$$

, тогда, взяв в качестве константы периода 1 нулевое сверхслово, получим $Cq = CA^b q$ для любого q.

Докажем теперь, что $A^b q \sim q$. Т.к. $CA^i q = CA^{b+i} q$, то $C(A^i q + A^{i-1} B\alpha_1 + ... + B\alpha_i) = C(A^{b+i} q + A^{i-1} B\alpha_1 + ... + B\alpha_i)$ для любых q и $\alpha_1\alpha_1...\alpha_i$ и состояние $A^b q \sim q$. По условию $Cq = C(A^b q + A^{b-1} B\alpha_1 + ... + B\alpha_b)$, а значит $C(A^{b-1} B\alpha_1 + ... + B\alpha_b) = 0$ для всех слов длины b. Значит автомат по всем словам длины b переходит в начальное состояние. Такой автомат не является групповым. Получили противоречие.

Для доказательства утверждения 1 заметим, что в леммах 2.6, 2.7 мы построили линейный автомат из задержек, булевых функций, Z_2 и константы периода t такого, что $A_G^t = I$, где A_G - невырожденная часть в разложении (2.2). Ранее в доказательстве мы показали, что если частный цикловый индекс автомата равен b, причем $b|t$, то состояния q и $A^b q$ - неотличимы. А значит групповой автомат можно заменить на эквивалентный такой, что $A_G'^b = I$, а значит и константу можно заменить на частный цикловый индекс.

Доказательство теоремы 2.8:Пусть $L \in M$, тогда возможны 3 случая.
1.$L \in < \emptyset >$
2.$L \in < K_b >$. Тогда L выразим тогда и только тогда когда выразимы все константы периода b.
3.$L \in < K_b, Z_2 >$. Тогда L вырадим тогда и только тогда, когда выразимы все константы периода b и Z_2. А Z_2 выразим тогда и только тогда, когда главный цикловый индекс M делится на 2, а значит тогда и только тогда, когда выразимы все константы периода степени 2.
Теорема доказана.

Таким образом для линейных автоматов необходимое условие выразимости 2.4 является также и достаточным. Теорема 2.9 непосредственно следует из теоремы 2.8

Глава 3

Применение алгебраических конструкций в задаче выразимости автоматов относительно расширенной суперпозиции и F_2 суперпозиции.

В данной главе рассматривается применение алгебраических конструкций в задаче выразимости автоматов. Доказана алгоритмическая разрешимость выразимости групповых автоматов Медведева через расширенную суперпозицию. Также рассматривается задача выразимости относительно F_2 суперпозиции. Для неё показана алгоритмическая разрешимость задачи выразимости произвольных групповых автоматов. Также решена задача N - полноты относительно F_2 суперпозиции.

Определение 3.1 *Пусть* $M = (A, Q, B, \phi, \psi, q_0)$ *- конечный автомат. Множество подстановок* $\{\phi_a : Q \to Q | a \in A\}$, *где* $\phi_a(q) = \phi(q, a)$, *порождает полугруппу подстановок* S *на множестве* Q. *Изоморфную* S *абстрактную полугруппу будем называть полугруппой автомата* M *и обозначать* S_M.

Например, группа автомата Z_n есть циклическая группа порядка n - $Z/(n)$.

Определение 3.2 *Пусть S_1 и S - полугруппы. Скажем, что полугруппа S_1 делит полугруппу S, если в S найдется такая подполугруппа S_2, что S_1 является гомоморфным образом S_2. Будем обозначать этот факт через $S_1|S$. Множество всех делителей S обозначим через $Del(S)$*

Определение 3.3 *Пусть G - множество всех конечных групп. Pr - множество всех простых конечных групп, S - конечная подполугруппа. Через $Pr(S)$ - обозначим множество всех простых групп - делителей полугруппы S. Пусть M - конечный автомат, через $Pr(M)$ обозначим множество простых групп - делителей полугруппы S_M.*

Определение 3.4 [19] *Пусть S - некоторая абстрактная полугруппа с единицей, $|S| = r$ и n - наименьшее целое такое, что $n \geq log_2 r$. Всякое отображение E_2^n на S будем называть кодированием. Если $\gamma : E_2^n \longrightarrow S$ - кодирование, то для всякого элемента $s \in S$ найдется набор $a = (a_1, ..., a_n) \in E_2^n$ такой, что $\gamma(a) = s$.*

Зафиксируем такое кодирование γ и рассмотрим автомат $M = (E_2^n, S, E_2^n, \phi, \psi)$ с n входами и n выходами, множество состояний которого совпадает с множестваом элементов полугруппы S, начальное состояние - единичный элемент $e \in S$, а функция переходов соответствует умножению в полугруппе S

$$\phi(s, a) = s * \gamma(a)$$

Функция выходов ψ определена следующим образом:

$$\psi(s, a) = \overline{\gamma^{-1}(s)},$$

где $\overline{\gamma^{-1}(s)}$ *- произвольный набор из* E_2^n *такой, что* $\gamma(\overline{\gamma^{-1}(s)}) = s$.

Будем называть построенный автомат автоматом полугруппы S*, а автоматную функцию, реализуемую* M*, специальной автоматной функцией полугруппы* S *и обозначать* $Sp(S)$.

Такое название правомерно, т.к. справедлива следующая лемма об изоморфизме

Лемма 3.1 *Любые две специальные автоматные функции полугруппы* S *изоморфны.*

Будем называть триггером (T) - автомат Медведева с 2-мя входами и 2-мя состояниями со следующей функцией переходов

$\phi(0, 00) = 0, \phi(1, 00) = 1$
$\phi(0, 01) = 0, \phi(1, 01) = 0$
$\phi(0, 10) = 1, \phi(1, 01) = 1$
$\phi(0, 11) = 0, \phi(1, 11) = 1$
Верна следующая теорема

Теорема 3.1 [18] *Пусть* N *- множество автоматных функций и* M *- множество специальных автоматных функций. Для того, чтобы* $N \subseteq < M, T >$ *необходимо и достаточно, чтобы* $Del(N) \subseteq Del(M)$

С.В. Алешину удалось избавиться от условия специальности, добавив в базис все константные автоматные функции.

Теорема 3.2 [19] *Пусть* G *- простая некоммутативная группа,* M *- произвольный групповой автомат, такой что* S_M *изоморфна* G *и* $Sp(G)$ *- специальная автоматная функция группы* G*. Тогда* $Sp(G) \in < M, K >$

Теорема 3.3 [19] *Пусть G - простая некоммутативная группа, M - произвольный групповой автомат, такой что группа S_M имеет G в качестве делителя. Тогда $Sp(G) \in < M, K >$*

Теорема 3.4 *Пусть $M \in P$, G - произвольный групповой автомат Медведева, тогда проверка $G \in < M >$ алгоритмически разрешима.*

Автоматную функцию F_2, задаваемую уравнениями

$$\begin{cases} q(1) = 0, \\ q(t+1) = q(\bar{t})a_1(t) \vee q(t)a_2(t), \\ b(t) = q(t), \end{cases}$$

назовём универсальной автоматной функцией с 2-мя состояниями.

Обозначим $< M >_{F_2} = [M \cup \{F_2, P_2\}]$.

Теорема 3.5 *Пусть $M \in P$, G - произвольный групповой автомат, тогда $G \in < M >_{F_2}$ алгоритмически разрешима .*

Теорема 3.6 *Пусть $M \in P$, P^n - все автоматы с не более, чем n состояниями. Тогда задача $< M >_{F_2} \supseteq P^n$ является алгоритмически разрешимой.*

Позже в тексте мы сформулируем условия выразимости, аналогичные теоремам 3.1, 3.2, 3.3

Основные леммы и доказательства теорем

Воспользуемся обозначениями из параграфа 2.1. Пусть $\alpha \in A^*$. Обозначим $e_\alpha = (\phi_\alpha, \pi_\alpha)$. Для $A' \in A^*$ обозначим $E_{A'} = \{e_\alpha : \alpha \in A'\}$.

Определение 3.5 *Будем говорить, что автоматы* $M_1 = (A_1, Q_1, B_1, \phi_1, \psi_1)$, $M_2 = (A_2, Q_2, B_2, \phi_2, \psi_2)$ *подобны*$(M_1 \approx M_2)$, *если* $Q_1 = Q_2$ *и* $E_{A_1} = E_{A_2}$.

Утверждение 3.1 *Пусть автоматы* M_1 *и* M_2 *подобны, тогда* $M_1 \in < M_2 >$ *и* $M_2 \in < M_1 >$.

Пусть $t \in \mathbf{N}$, обозначим $M^t{=}(A^t, Q, B^t, \overline{\phi}, \overline{\psi}, q0)$ - автомат M на словах длины t.

Пусть b, q - цикловые индексы автомата M. Т.к. всего существует конечное число попарно не подобных автоматов с фиксированным числом состояний, то в последовательности M^b, M^{bq}, M^{bq^2},... найдется конечное число попарно не подобных автоматов. Значит для некоторых $l_0 < l_1$ $M^{bq^{l_0}} \approx M^{bq^{l_1}}$. Без ограничения общности в этой главе будем считать частным цикловым индексом автомата M число bq^{l_0}, а главным цикловым индексом число $q^{l_1 - l_0}$.

Лемма 3.2 *Пусть* b, q *- цикловые индексы автомата Медведева* M,
$q > 1$ *тогда* $M^{bq} \in < M >$.

Доказательство : Для доказательства леммы введем некоторые обозначения и приведем схему, копирующую автомат M^{bq} согласно определению 2.5.

$f(x_1, ..., x_{(bq)^2})$ - булева функция с $(bq)^2$ входами и bq выходами, такая что $f(\bar{x}) = \bar{y}$ тогда и только тогда, когда $e(\bar{x}) = e(\bar{y})$, причем $y_1 = x_1$. Такое $\bar{y}$ всегда найдется по построению цикловых индексов

w, w_1 - автоматные функции с bq входами и 1 выходом, такие что $w(t) = x_i$ при $t = i \ mod \ n_1$, $w_1(t) = x_i$ при $t = i \ mod \ n_1 + 1$

w^{-1} - автоматная функция с bq входами и $(bq)^2$ выходами, такая что $w^{-1}(t) = \overline{x(t - n_1 + 1)x(t - n_1 + 2)...x(t)}$ при $t = 0 \ mod \ n_1$, $w^{-1}(t) = 0$ иначе.

$S(x_1, x_2)$ - автоматная функция, такая что при $t = 1, ..., n_1$ $S(x_1, x_2) = x_1$, а при $t > n_1$ $S(x_1, x_2) = x_2$.

Рассмотрим схему (рис. 3.1) и докажем, что она копирует автомат M^{bq}.

Действительно, пусть $a(0)a(1)a(2)...$ - произвольная входная последовательность автомата M^{bq}, $q(0)q(1)...$ и $b(0)b(1)b(2)...$ - соответствующие последовательность состояний и выходная последовательность. Посмотрим, как преобразует эту входную последовательность построенная схема. Обозначим $a(t) = \overline{a_1(t)a_2(t)...a_{bq}(t)}$. $q'(0)q'(1)...$, $b'(0)b'(1)...$ - последовательность состояний и выходная последовательность автомата M в схеме. В моменты времени $0...bq - 1$ на вход автомата M последовательно попадают $a_1(0), a_2(0), ..., a_{bq}(0)$. Таким образом $q'(bq) = q(1), b'(i) = b_i(0), i = 1..bq$. По построению функций f, w^{-1}, w_1

$q'(2bq) = \phi(q'(bq), w_1(f(w^-1(a(1)a(2)...a(bq)))))) =$

$= \phi(q'(bq), w_1(f(\overline{a(1)a(2)...a(bq)}))) =$

$= \phi(q'(bq), f(\overline{a(1)a(2)...a(bq)}) =$

$= \phi(q(1), a(1)a(2)...a(bq)) = q(bq)$. Т.к. автомат M^{bq} автомат Медведева, любые 2 состояния автомата M, достижимые словами длины кратной bq, отличимы любым словом длины bq. Таким образом данная схема копирует автомат, подобный автомату M^{bq} с параметрами $bq, bq, 1$, а значит по лемме о копировании и утверждению 1 $M^{bq} \in < M >$. Лемма доказана.

Определение 3.6 *Пусть* $M = (A, Q, B, \phi, \psi, q_0)$, $M' = (A', Q', B', \phi', \psi', q'_0)$. M' - *называется n-подавтоматом*

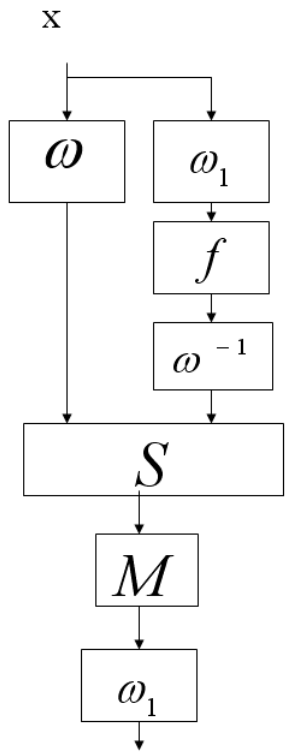

Рис. 3.1:

M, если $\exists n$, т.ч. $A' \subseteq A^n, Q' \subseteq Q, B' \subseteq B^n$ и $\phi(A', Q') \subseteq Q'$.

Прямо из леммы 3.2 следует

Утверждение 3.2 *Пусть b, q - цикловые индексы автомата Медведева M, M' - bq - подавтомат M , тогда $M' \in < M >$*

Определение 3.7 *Пусть $M = (A, Q, B, \phi, \psi, q_0)$,*
$M' = (A', Q', B', \phi', \psi', q_0')$ - автоматы. Скажем, что автомат M' является гомоморфным образом автомата M, если найдутся такие отображения "на" $\chi : Q \to Q'$, $\eta : A \to A'$, $\varpi : B \to B'$, что диаграммы, изображенные ниже, коммутативны.

$$\begin{array}{ccccc} A_1 & \times & Q_1 & \xrightarrow{\phi} & Q_1 \\ \eta\downarrow & & \chi\downarrow & & \chi\downarrow \\ A_2 & \times & Q_2 & \xrightarrow{\phi'} & Q_2 \end{array} \qquad \begin{array}{ccccc} A_1 & \times & Q_1 & \xrightarrow{\psi} & B_1 \\ \eta\downarrow & & \chi\downarrow & & \varpi\downarrow \\ A_2 & \times & Q_2, & \xrightarrow{\psi'} & B_2 \end{array}$$

Несложно показать, что

Утверждение 3.3 *Пусть автомат M' является гомоморфным образом автомата M, тогда $M' \in < M >$.*

Определение 3.8 *Будем говорить, что $M''|M$, если $\exists n$, $\exists$ M' - n - подавтомат M, т.ч. M'' - является гомоморфным образом M'.*

Определение 3.9 *Будем называть простым автоматом, автомат Медведева с простой группой.*

Лемма 3.3 *Пусть $M = (A, Q, Q, \phi, \phi, q_0)$ - групповой не константный автомат Медведева, b, q - его цикловые индексы. Тогда $q > 1$.*

Доказательство: Докажем утверждение от противного. Предположим, что $q = 1$. Тогда для всех слов $\gamma \in A^b$ период сверхслова $M(\gamma^\infty)$ равен b. Значит, что $\phi(q_0, \gamma) = q_0$. Т.к. автомат групповой, то для любого $a \in A$ отображение $\phi(q, a)$: $Q \to Q$ - взаимно-однозначное, а значит $|\phi(Q, a)| \geq |Q|$. Т.к. для любого слова длины b отображение $|\phi(q_0, \gamma)| = 1$, то для любого $a \in A$ $|\phi(q_0, a)| = 1$, а значит автомат M - константный, что противоречит условию леммы. Лемма доказана.

Лемма 3.4 *Пусть M - некоммутативный групповой автомат Медведева, S_M - группа автомата M, M' - автомат группы S_M. Тогда $M' \in < M >$, $M \in < M' >$.*

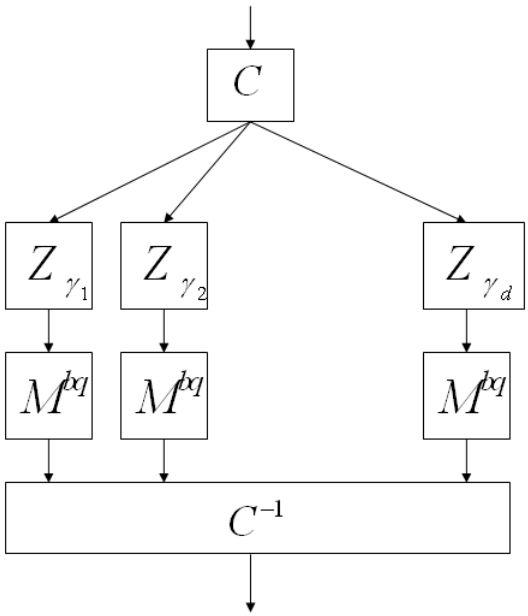

Рис. 3.2:

Доказательство:В [19] показано, что существует r, такое что любой элемент группы S_M может быть представлен словом длины r. По лемме 3.3 $q > 1$ и в качестве r можно взять $bq > r$достаточно большой цикловый индекс автомата M. По лемме 3.2 $M^{bq} \in < M >$. Построим теперь по автомату M^{bq} автомат M'.

Т.к. автомат M^{bq} групповой и содержит всю группу S_M, любое состояние автомата M^{bq} достижимо словом длины bq. Обозначим γ_i - слово, переводящее начальное состояние автомата M^{bq} в состояние q_i.

Пусть d - число состояний автомата M. Рассмотрим схему, изображенную на рисунке 3.2.

Здесь $C : S_M \to E_2^{bq}$ - функция кодирования, отображающая элементы группы S_M в слова во входном алфавите M^{bq}. Z_{γ_i} - задержка, выдающая в первые bq моментов времени γ_i. $C^{-1} : Q^d \to S_M$ - функция обратного кодирования отобража-

ющая текущий вектор состояний M^{bq} в элемент группы S_M. Построенный автомат является автоматом группы S_M, что и требовалось доказать. Аналогично доказывается включение $M \in < M' >$.

Аналогично лемме 3.4 верна

Лемма 3.5 *Пусть M - групповой автомат Медведева и известно, что $Z/(n)|S_M$. Тогда $n|q(M)$.*

Доказательство Рассмотрим подстановки на множестве состояний автомата M, соответствующие словам длины t - S_t. Последовательность S_t является периодической с некоторого момента. Действительно, множество подстановок ограничено множеством подмножеств всех подстановок и найдутся индексы i и j, такие что $S_i = S_j$. Отсюда, очевидно следует, что $S_{i+1} = S_{j+1}$ а следовательно и периодичность. Обозначим период последовательности S_t через m.

Докажем, что $m|b$. Действительно по построению цикловых индексов $E_b = E_{bq} \Rightarrow m|b(q-1)$.

С другой стороны заметим, что единица в группе S_M может соответствовать только словам длины, кратной m. Действительно, пусть это не так и существует слово длины $k < m$, задающее единицу в группе S_M. Тогда последовательность $S_t, S_{t+k}, S_{t+2k}, ...$ является последовательностью вложенных множеств. Т.к. она возрастает и ограничена, то с какого-то момента она стабилизируется, но тогда $m|k$, что неверно. Но мы знаем, что взяв слово длины b q раз мы получим слово, соответствующее единице. Таким образом существуют единицы длины bq. Таким образом $m|bq$.

Из последних двух утверждений следует, что $m|b$. Отсюда очевидно, что $S_{qb} = S_{2qb} = S_{3qb} = ... = S_{lqb} = S_{bq^2}$ для $\forall l$.

Из леммы 3.8 и из строения группы Z_n очевидно, что $\exists l$ и слова α, β $(l(\alpha) = l(\beta) = l)$, такие, что α задает на некотором множестве состояний $q_1, ..., q_n$ автомата M единичную

подстановку, а β на этом же множестве состояний циклическую перестановку. Но в этом случае то же самое верно и для всех длин, кратных l, в том числе и bql, а значит и для bq^*. Таким образом мы показали, что в множестве P_{bq^*} всегда есть циклическая подстановка ранга n, а отсюда следует утверждение леммы. Лемма доказана.

Лемма 3.6 *Пусть C_p и B_p приведенные автоматы, C_p не является безусловным, причём $S_{C_p} = S_{B_p} = Z_p$. Тогда $\langle C_p \rangle \supseteq \langle B_p \rangle$.*

Лемма 3.7 *Пусть G - групповой автомат Медведева, $M \in P$, тогда $G \in < M > \Leftrightarrow$ все простые автоматы, делящие G принадлежат $< M >$.*

Доказательство: *Необходимость* Пусть автомат $G \in < M >$, докажем, что для произвольного простого Pr, такого, что $Pr | G$ $Pr \in < G > \subseteq < M >$. Если автомат Pr - коммутативный, то разделяются 2 случая: автомат Pr - константный и автомат Pr - автомат Z_n. Оба случая рассмотрены в главе 2 - параграф 2.1 и параграф 2.3 соответственно.

Пусть теперь группа автомата Pr - некоммутативна.

По условию делимости $\exists n$, и существует n-подавтомат G, такой что Pr является гомоморфным образом этого подавтомата. Как обычно b и q - цикловые индексы автомата G. Докажем, что в качестве n можно взять $n = bq$, тогда утверждение леммы будет следовать из утверждения 3.2 и утверждения 3.3.

Для доказательства этого рассмотрим последовательность степеней автомата G - G, G^2, G^3,...,G^i,... По определению подобия автоматов, найдутся такие ρ и ρ_0, что для любого $j \geq \rho_0$ $G^j \approx G^{j+\rho}$. Более того несложно показать, что для любого $j < \rho_0$ G^j - $(j + \rho)$ - подавтомат G.

Покажем, что $\rho | bq$. Для этого покажем, что bq также является периодом последовательности G^i. Действительно взяв

любое слово α длины bq q раз подряд, мы получим тождественную подстановку на некотором множестве состояний автомата G i_α, а значит такая же тождественная подстановка α' есть и на длине bq. Значит $\forall\alpha$ $e_{\alpha\alpha'} = e_\alpha$ и $E_{bq} \subseteq E_{2bq}$. Продолжая далее аналогичные рассуждения, получим цепочку $E_{bq} \subseteq E_{2bq} \subseteq ... \subseteq E_{bq^2}$. Но мы знаем, что $E_{bq} = E_{bq^2}$ и таким образом $E_{bq} = E_{2bq} = ... = E_{bq^2}$ и bq - период последовательности G^i.

Теперь вернемся к доказательству леммы. Как мы только что показали, $\exists i$, что $Pr|G^{bq+i}$. Рассмотрим автомат $G^{bq(bq+i)}$. Используя то же самое отображение, что и при делении G^{bq+i} мы получим некоторый подавтомат Pr, т.к. Pr - простой автомат, то либо это Pr либо константный автомат с одним состоянием. Второй случай невозможен, т.к. это противоречит некоммутативности Pr. Таким образом $Pr|G^{bq(bq+i)} \approx G^{bq}$ и лемма доказана.

Достаточность Для группового автомата Медведева G уже показано, что его выразимость эквивалентна выразимости автомата G^{bq}. Таким образом достаточно доказать выразимость автомата G^{bq}. Простые автоматы, делящие G делятся на константные и не константные. Покажем, что нет константных автоматов, делящих G^{bq}. Действительно, пусть это так и автомат G^{bq} делится на константу периода l, тогда автомат G^{bql} не подобен автомату G^{bq}, что противоречит тому, что $G^{bq} \approx G^{2bq}$.

Таким образом все простые автоматы, делящие G^bq - не константные. Теперь, пользуясь леммой 3.4, теоремой 2.6 и леммой 3.6, заметим, что из простых автоматов выразимы специальные автоматы соответствующих групп, а значит и выразим автомат G^{bq}. Лемма доказана.

Лемма 3.8 *Пусть $M = (A, Q, B, \phi, \psi, q_0)$ - произвольный автомат Медведева, (X, S) - простая подгруппа S полугруппы S_M с системой образующих $X = (s_1, ..., s_k)$. Пусть $\alpha_1, ..., \alpha_k$ -*

множество слов в алфавите A, таких, что $\phi(q, \alpha_i) = s_i(q), i = 1, ..., k$. Тогда в группе S существует система образующих $X' = (s'_1, ..., s'_k)$, и множество слов в алфавите A - $\alpha'_1, ..., \alpha'_k$, такие что $\phi(q, \alpha'_i) = s'_i(q), i = 1, ..., k$ и $l(\alpha'_1) = ... = l(\alpha'_k)$.

Доказательство Пусть $l_1 = l(\alpha_1), .., l_m = l(\alpha_m))$. Обозначим $d = NOD(l_1, .., l_m)$ Пусть $(e_1, ..)$ - множество слов в алфавите A, таких что $\phi(q, e_i) = q, i = 1, ...$ Обозначим $l(e_i) = d_i$. Обозначим $d_e = NOD(\{d_i\})$. Очевидно, что $d_e = Cd$ для некоторого C. Возможно 2 случая
1.$C > 1$
2.$C = 1$

1.Пусть $C > 1$. Рассмотрим множество элементов группы S, соответствующее словам длины кратной Cd в алфавите A. Несложно показать, что это нормальная подгруппа группы S, что возможно только если это единица.

Таким образом для любого элемента группы S имеем $s^C = e$. Причем $s^i \neq e$ для $i < C$ Рассмотрим новые образующие группы S $X' = (s'_1, ..., s'_k)$ такие, что $s'_1(q) = \phi(q, \underbrace{s_1...s_1}_{l_2...l_m}),...,s'_k(q) = \phi(q, \underbrace{s_k...s_k}_{l_1...l_{k-1}})$. Очевидно, что $\{s_i, s_i^2, ..., s_i^{C-1}\} = \{s'_i, s_i'^2, ..., s_i'^{C-1}\}$. Поэтому X' образующие группы S, удовлетворяющие условиям леммы.

2. Пусть $C = 1$. Тогда найдутся 2 слова в алфавите A (e_1, e_2), такие что $\phi(q, e_1) = \phi(q, e_2) = q$ и $l(e_1) - l(e_2) = d$. Добавляя e_1 и e_2 к образующим мы можем выровнять длины образующих элементов при этом не меняя значений соответствующих элементов группы.

Лемма доказана.

Лемма 3.9 *Пусть Pr - простой автомат Медведева, M - произвольный автомат, тогда $Pr \in < M > \Leftrightarrow Pr|M^{bq}$.*

Доказательство: Необходимость:Доказательство аналогично доказательству необходимости в лемме 3.7 с той лишь разницей, что теперь автомат M не автомат Медведева. Но т.к. автомат Pr - автомат Медведева и $Pr|M^{bq}$, то найдется M' - bq подавтомат автомата M, такой что $Pr|M'$ и $M' \in < M >$ по лемме 3.2.

ДостаточностьИз теоремы 3.1 и того факта, что $Pr \in < M >$ следует что $S_P r|S_M$. Определение делимости для полугрупп следующее $S_1|S$, если в S найдётся подполугруппа S_2, такая что S_1 является гомоморфным образом S_2.

Вообще говоря из делимости полугрупп не следует делимость соответствующих автоматов. Для доказательства делимости автоматов в случае простого некоммутативного автомата Медведева нам понадобится лемма 3.8.

Из леммы 3.8 и того факта, что $Pr|M$ следует, что существует n - подавтомат M' и отображения "на" $\chi : Q_{M'} \to Q_P r$, $\eta : A_{M'} \to A_P$, что диаграмма, изображенная ниже, коммутативна

$$\begin{array}{ccccc} A_{M'} & \times & Q_{M'} & \xrightarrow{\phi} & Q_{M'} \\ \eta \downarrow & & \chi \downarrow & & \chi \downarrow \\ A_P & \times & Q_P & \xrightarrow{\phi'} & Q_P \end{array}$$

Для доказательства делимости осталось показать, что существует отображение "на" $\varpi : B_{A'} \to B'$, что диаграмма, изображенная ниже, коммутативна

$$\begin{array}{ccccc} A_{M'} & \times & Q_{M'} & \xrightarrow{\psi} & B_{M'} \\ \eta \downarrow & & \chi \downarrow & & \varpi \downarrow \\ A_P & \times & Q_P, & \xrightarrow{\psi'} & B_P \end{array}$$

Рассмотрим схему, выражающую автомат Pr, состоящую из автомата M, булевых функций и задержек. Без ограничения общности будем считать, что схема, выражающая Pr являет-

ся суперпозицией 2х автоматов M_1 - верхнего и M_2 - нижнего. По теореме 3.1 либо M_1 либо M_2 имеет гомоморфизм по переходам на автомат Pr.

Рассмотрим всевозможные случаи. 1.Автомат M_1 состоит из задержек и булевых функций и не имеет гомоморфизма по переходам на Pr. Тогда M_2 имеет гомоморфизм на Pr по переходам, а т.к. выход всей схемы совпадает с выходом Pr, то существует гомоморфизм и по выходам на Pr.

Пусть автомат M_1 не является автоматом из задержек и булевых функций. Т.к. вся схема имеет гомоморфизм по переходам на Pr, то такой гомомрфизм имеет и M_1, т.к. состояние схемы это пара - (состояние M_1, состояние M_2). Пусть M_2 имеет также гомоморфизм на Pr. Для дальнейшего доказательства нам понадобится

Лемма 3.10 *Пусть автомат M имеет гомоморфизм по переходам на простой групповой автомат Pr, тогда существует M' - групповой приведенный подавтомат M, такой что M' также имеет гомоморфизм на Pr.*

Доказательство Рассмотрим максимальное подмножество множества состояний Q' автомата M такое, что $\forall \alpha \in A\, \phi(\alpha, Q') = Q'$. Очевидно выбранное подмножество будет групповым подавтоматом автомата M. Докажем, что этот подавтомат будет иметь гомоморфизм на P. Понятно, что свойство коммутативности по переходам при выделении подавтомата исходного автомата сохраняется. Значит нужно доказать, что для любого состояния автомата Pr найдется прообраз в автомате M'. Пусть это не так и существует $p \in Q_P$, т.ч. любое $q \in Q_M$ - прообраз p, q не принадлежит Q'. В этом случае $Q_p \subseteq Q_M$ - прообраз p при гомоморфизме "склеивается"с некоторым другим прообразом при подаче подходящего слова. Т.к. это выполнено в автомате M, то будет выполнено и в автомате Pr, что невозможно, т.к. автомат Pr - групповой. Лемма доказана.

Лемма 3.10 позволяет без ограничения общности считать автомат M_1 групповым. Рассмотрим множество слов над входным алфавитом автомата Pr, которое переводит начальное состояние автомата M_1 в себя. Это множество слов образует нормальную подгруппу в группе автомата Pr. Т.к. Pr - автомат с простой группой, эта нормальная подгруппа является либо всей группой Pr либо единичной подгруппой. В первом случае на выбранном множестве слов автомат M_2 работает синхронно с автоматом Pr, а следовательно имеет гомоморфизм и по выходам на Pr. Во втором случае рассмотрим множество слов, переводящих выбранное состояние в некоторое другое состояние в автомате M_1. Данное множество слов будет образовывать некоторый смежный класс в группе Pr по единичной подгруппе, а таким образом все множество слов будет образовывать всю группу Pr. Значит автомат M_1 в точности автомат Pr. Т.к. автомат M_1 групповой, приведенный и имеет гомоморфизм по переходам на Pr, то он имеет гомоморфизм и по выходам на Pr.

Пусть теперь M_1 имеет гомоморфизм по переходам на Pr, а M_2 не имеет такого гомоморфизма. Выделим в автомате M_1 групповой подавтомат стандартным образом. Осуществим процедуру приведения неотличимых состояний автомата M_1. Если автомат M_1 все еще имеет гомоморфизм на автомат Pr, то из того, что автомат M_1 групповой, приведенный и имеет гомоморфизм по переходам на автомат Pr следует, что он имеет гомоморфизм и по выходам на автомат Pr. Если же автомат M_1 после приведения не имеет гомоморфизма по переходам на Pr, то мы пришли к противоречию, т.к. получили из 2х автоматов, не имеющих гомоморфизм по переходам на Pr схемой автомат Pr, что невозможно.

Таким образом либо Pr делит M_1 либо Pr делит M_2. Продолжая данную процедуру вглубь схемы, получим на каком-то уровне, Pr делит M, т.к. очевидно Pr не делит штрих Шеф-

фера и задержку.

Лемма доказана.

Леммы 3.7 и лемма 3.9 дают нам критерий выразимости группового автомата Медведева аналогичный теоремам 3.1, 3.2, 3.3 и таким образом теорема 3.4 доказана.

Определение 3.10 *Пусть* $M = (A, Q, B, \phi, \psi, q_0) \in P_a$ *- произвольный автомат. Назовем слово* $\alpha \in A^*$ *- единым тестом для автомата* M*, если*
$\forall q_1, q_2 \in Q\ \bar{\psi}(q_1, \alpha) \neq \bar{\psi}(q_2, \alpha)$.

Определение 3.11 *Пусть* $= (A, Q, B, \phi, \psi, q_0)$ *- произвольный автомат. Будем говорить, что* $M' = (A, Q, Q, \phi, \psi', q_0)$ *- автомат Медведева автомата* M*, если* $\psi'(a, q) = q$.

Лемма 3.11 *Пусть* $M = (A, Q, B, \phi, \psi, q_0) \in P_a$ *- произвольный приведенный групповой автомат. Тогда* $\exists k \in \boldsymbol{N}$ *такое что для любого* $\alpha \in A^{2^k}$ *существует* $\alpha' \in A^{2^k}$ *- такое, что:*
1. $\phi(\alpha, q) = \phi(\alpha', q)$ *для любого* q*;*
2. α' *- единый тест для автомата* M.

Доказательство:Т.к. у автомата M все состояния отличимы, для любой пары состояний q_i, q_j найдется слово α_{ij}, такое что $\psi(q_i, \alpha_{ij}) \neq \psi(q_j, \alpha_{ij})$.

Обозначим через α_{ij}^{-1} слово в алфавите A такое, что слово $\phi(\alpha_{ij}\alpha_{ij}^{-1}, q) = q$ для любого q. Тогда слово $\beta = \alpha_{12}\alpha_{12}^{-1}\alpha_{13}\alpha_{13}^{-1}...\alpha_{d-1d}\alpha_{d-1d}^{-1}$, $|Q| = d$ будет отличать любую пару состояний автомата M и задавать единичную подстановку на множестве состояний. Тогда произвольное слово вида $\beta\hat{\beta}$, такое что $|\beta\hat{\beta}| = 2^k$ также будет отличать все состояния автомата M.

Докажем теперь, что для произвольных α и β ($|\alpha| = 2^k$, $|\beta| = l < 2^k$), существует β' ($|\beta'| = 2^k - l$) такое что α и $\beta\beta'$ порождают одинаковые подстановки на множестве состояний автомата M.

Рассмотрим последовательность подмножеств подстановок на множестве состояний

$$G_1 = \{\pi_a, a \in A\},$$
$$G_2 = \{\pi_{ab}, a, b \in A\},$$
$$...$$
$$G_k = \{\pi_{a_1 a_2 ... a_k}, a_i \in A\},$$
$$...$$

Эта последовательность, начиная с некоторого t, периодическая, то есть

$\Gamma = \{G_t, G_{t+1}, ..., G_{t+s}, G_t ...\}$.

Т.к. слово β есть единичная подстановка, то очевидно $s|l$. Значит для слова α найдется слово β' длины $2^k - l$, задающее ту же подстановку. Оно очевидно удовлетворяет условиям леммы. Лемма доказана.

Лемма 3.12 *Пусть $M \in P$ - произвольный групповой автомат. M' - его автомат Медведева. Тогда*
1. $M' \in < M >_{F_2}$;
2. $M \in < M' >_{F_2}$.

Доказательство:Доказательство пункта 2 элементарно, достаточно "навесить"на выход автомата Медведева функции выходов, реализуемые в состояниях автомата M и соединить с ними вход автомата M'.

Для доказательства пункта 2 воспользуемся леммой 3.7 и покажем, что все простые автоматы, делящие M', выразимы через M.

Из леммы 3.2 и леммы 3.11 несложно показать, что подавтомат Медведева автомата M^{2^k} для достаточно большого k выразим через $< M >$, поэтому достаточно показать, что простые автоматы выразимы через M^{2^k} для достаточно большого k.

Простые автоматы делятся на 3 типа
а)Коммутативные константные автоматы;
б)Коммутативные не константные автоматы;
в)Некоммутативные автоматы с простыми группами.

Пусть константный автомат K_s делит автомат M'. Возможны 2 случая - s делит 2^k и s не делит 2^k. В первом случае очевидно константный автомат выразим. Во втором случае автомат K_s не является делителем автомата M'^l для $s|l$, но т.к. s не делит 2^k, а автоматы Медведева M^{2^k} и M'^{2^k} совпадают по лемме 3.11, то $K_s|M^{2^k}$ и по лемме 3.9 автомат K_s выразим через M^{2^k}.

Пункты б и в непосредственно следуют из леммы 3.9, а также из того факта, что если не константный простой автомат делит автомат Медведева, то он делит и все степени этого автомата. Т.к. автоматы M'^{2^k} и M^{2^k} подобны, то простые автоматы, делящие M'^{2^k}, делят и автомат M^{2^k}. Лемма доказана.

Теорема 3.5 следует из теоремы 3.4 и леммы 3.12.

Теорема 3.6 следует из теоремы 3.4 и того факта, что $< M >_{F_2} \supseteq P_a^n$ тогда и только тогда, когда через $< M >_{F_2}$ выразимы все простые автоматы с не более, чем n состояниями.

Литература

[1] Post E. Two-Valued 1.erative Systems of Mathematical Logic. Princeton Univ. Press, Princeton, 1941

[2] Post E. A variant of recursively unsolvable problem, Bull. Amer. Math. Soc 52, 1946

[3] Яблонский С.В. Функциональные построения в k-значной логике, Труды математического института им. В.А. Стеклова, АН СССР, 1958, Т.51, стр. 5-142

[4] Кудрявцев В.Б. Теорема полноты для одного класса автоматов без обратных связей. Проблемы кибернетики, 1962 год №8, стр. 91-115

[5] Летичевский А.А. Условия полноты для конечных автоматов, Вычислительная математика и математическая физика, №4, 1961 год, стр. 702-710.

[6] Кудрявцев В.Б. О мощностях множеств предполных классов некоторых функциональных систем, связанных с автоматами, ДАН СССР т.151,N3,1963, с.493-496.

[7] Кратко М.И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов, ДАН СССР, 1964, т.155, N 1, с.35–37.

[8] Буевич В.А. Об алгоритмической неразрешимости распознавания А-полноты для ограниченно-

детерминированных функций, Математические заметки, вып.6, 1972, стр. 687-697

[9] Буевич В.А. Условия А-полноты для автоматов, М., изд. МГУ, 1986

[10] Dassow J., Ein modifizierter Vollstandigkeitsbegriff in einer Algebra von Automatenabbildungen, Dissertation Doktor B, Rostock, Universitet,1978.

[11] Строгалов А.С., Метрические свойства о.д.-функций, Межвузовский сборник трудов, N 56, МЭИ, 1985, стр. 80-84

[12] Хазбун И.В., Об условиях полноты и выразимости в точной алгебре автоматов, Логико-алгебраические конструкции, Тверь 1984, стр. 35-41.

[13] Бабин Д.Н. О суперпозициях о.д.-функций ограниченного веса, Логико-алгебраические конструкции, Тверь 1984, стр. 21-27

[14] Часовских А.А., О полноте в классе линейных автоматов, Математическме вопросы кибернетики, 1995, N3, стр. 140–166.

[15] Бабин Д.Н., Разрешимый случай задачи о полноте автоматных функций, Дискретная математика, том 4, 1992, выпуск 4, стр. 41-56, Наука, Москва

[16] Бабин Д.Н., О классификации автоматных базисов Поста по разрешимости свойств полноты и А-полноты, ДОКЛАДЫ АКАДЕМИИ НАУК, N 4, Т.367, 1999 стр. 439-441

[17] Бабин Д.Н., О полноте двухместных о.д.-функций относительно суперпозции, Дискретная математика, том 1, 1989, выпуск 4, стр. 86-91

[18] Арбиб М, Алгебраическая теория автоматов языков и полугрупп, "Статистика М.,1975

[19] Алешин С.В., Об одном следствии теоремы Крона-Роудза, Дискретная математика, том 11, вып.4, 1999 год, стр. 101-109

[20] Кудрявцев В.Б., Алешин С.В., Подколзин А.С., Введение в теорию автоматов, Наука, М., 1985.

[21] Мальцев А.И., Алгоритмы и рекурсивные функции, М.Наука, 1965

[22] Яблонский С.В., Введение в дискретную математику, М.Наука, 1986

[23] Berend, D.; Tassa, T., "Improved bounds on Bell numbers and on moments of sums of random variables". Probability and Mathematical Statistics 30 (2), 2010 185–205.

[24] Каргаполов, Мерзляков, Основы теории групп 3е изд, Наука, М.,

[25] Бабин Д.Н., Задача выразимости в некоторых классах автоматов, Комбинаторно-алгебраические методы в прикладной математике, 1982 год, стр. 21-45

[26] Гилл А., Линейные последовательностные машины. Анализ, синтез и применение. Перевод с английского А.С. Бернштейна, Издательство Наука, 1974.

[27] Кудрявцев В. Б., Гаврилов Г. П., Яблонский С. В. Функции алгебры логики и классы Поста. Наука, Москва, 1966.

Публикации автора по теме диссертации

[1] А.А. Летуновский. О выразимости константных автоматов. Интеллектуальные системы, 9(1-4):457–469, 2005.

[2] А.А. Летуновский. О выразимости константных автоматов суперпозициями. Интеллектуальные системы, 13(1-4):397–406, 2009.
[3] А.А. Летуновский. О выразимости суперпозициями автоматов с разрешимыми группами. Интеллектуальные системы, 14(1-4):379–393, 2010.
[4] А.А. Летуновский. О задаче выразимости автоматов относительно суперпозиции для систем с фиксированной добавкой. Интеллектуальные системы, 15(1-4):401–412, 2011.
[5] А.А. Летуновский. О задаче выразимости автоматов относительно суперпозиции для систем с фиксированной добавкой. Интеллектуальные системы в производстве, (1):36–50, 2012.
[6] А.А. Летуновский. О выразимости суперпозициями групповых автоматов Медведева. Интеллектуальные системы, 17(1-4):179–181, 2013.
[7] А.А. Летуновский. Цикловые индексы автомата. Дискретная математика, 25(4):24–29, 2013.