УДК 510.62

РАЗРЕШИМОСТЬ ТЕОРИЙ ОБОБЩЕНИЙ АВТОМАТНЫХ СИСТЕМ

Петров А.Е.
Кафедра информатики

Поступила в редакцию 24.05.2010, после переработки 05.06.2010.

В работе мы рассматриваем обобщение конечных автоматов путем добавления к их структуре бесконечной последовательности символов (оракула). Доказываем замкнутость класса языков, задаваемых такими автоматами, относительно пересечения, проекции и, в некоторых случаях, дополнения. Мы показываем, что этот класс шире класса регулярных языков. Предлагаем новый способ установления разрешимости теорий с помощью введённых объектов, приводим примеры таких теорий.

In this paper we extend finite automata by infinite sequence of symbols (oracle). We prove the class of languages which are recognized by these automata is closed under intersection, projection and under complement in some cases. We show this class is larger than regular languages. We present a new method to prove theory decidability using these automata. Also, we give examples of those theories.

Ключевые слова: конечный автомат, автоматная структура, релятивизация.
Keywords: finite automaton, automatic structure, relativisation.

Введение

Одним из важных свойств теорий является свойство разрешимости. Если можно предложить алгоритм, который проверяет по каждой замкнутой формуле принадлежит она теории или нет, то такая теория разрешима. Из таких алгоритмов известны, например, элиминация кванторов, проверка того, что каждое отношение системы можно распознать конечным автоматом и некоторые другие.

Элиминация кванторов — это процесс удаления кванторов из формулы, приводящий её к эквивалентной бескванторной. Теория плотного линейного порядка без концевых точек [3], арифметика Пресбургера [1] допускают элиминацию кванторов, однако теория линейного порядка — нет.

Одним из первых конечные автоматы для доказательства разрешимости теорий стал использовать Рабин М.О. [6]. Основной результат статьи, для которого использовался аппарат конечных автоматов, — разрешимость слабой теории второго порядка с двумя функциями следования. Это дало много других результатов разрешимости, которые просто следовали из главного, например: теория второго порядка счетных линейно упорядоченных множеств, теория первого порядка унарной функции со счетной областью определения — разрешимы.

Идеи Рабина М.О. о применении конечных автоматов для установления разрешимости были использованы в работе Блюменсата А., Гределя Е. [5]. Здесь вводится понятие автоматной системы. Так называется система, обладающая свойством:

> «по любому отношению системы $R(x_1, \ldots, x_n)$ можно эффективно построить конечный автомат, который по коду кортежа $(a_1, \ldots, a_n)$ (кортеж кодируется символами входного алфавита) сможет определить истинно R на $\bar{a}$ или ложно.»

В работе [5] также доказано, что если система является автоматной, то по любой формуле этой системы можно эффективно построить конечный автомат, который проверяет её истинность. По существу это следует из свойств замкнутости регулярных языков. Например, система $(\omega, <)$ является автоматной.

Мы предлагаем структуру конечного автомата с оракулом и доказываем с его помощью разрешимость некоторых теорий автоматных систем, обогащённых одноместным предикатом вида $U \subset \{2^x : x \in \omega\}$. Приводим пример неавтоматной системы, теория которой не допускает элиминацию кванторов, но которая разрешима.

Работа состоит из введения, четырех глав основной части, заключения и списка литературы. В главе 1 дается определение конечного автомата с оракулом, его работы, формулируется проблема остановки. Далее, здесь же мы определяем кодирование множеств в алфавитах таких автоматов, вводим понятие расширенно-автоматного отношения, расширенно-автоматной системы, языка, задаваемого формулой.

В следующей главе доказана теорема о детерминизации. Исследованы свойства замкнутости класса языков, задаваемых конечными автоматами с оракулами, — доказаны теоремы: о замкнутости относительно пересечения, проекции. Доказана теорема о том, что класс языков, задаваемых такими структурами, включает класс регулярных языков.

В главе 3 рассматривается вопрос о замкнутости относительно дополнения — даются примеры оракулов, которые допускают эффективное дополнение, что означает, что классы языков, задаваемых конечными автоматами с такими оракулами, замкнуты относительно всех теоретико-множественных операций.

Наконец, в заключительной главе сформулировано достаточное условие разрешимости теории расширенно-автоматной системы, приводятся примеры теорий, удовлетворяющих этому условию. Также дан пример неавтоматной системы, теория которой не допускает элиминацию кванторов, но которая удовлетворяет достаточному условию и, как сдедствие, её теория является разрешимой.

1. Определения

Заглавными латинскими буквами со знаком + вверху и, возможно, с индексами внизу мы будем обозначать конечные автоматы с оракулами. Например, M^+, M_1^+, NM^+, M_d^+, $M_\exists^+$.

Определение 1. Недетерминированным конечным автоматом с оракулом *мы будем называть семёрку:*

$$M^+ = \langle \Sigma, \Delta, Q, q_0, Q_f, \alpha, F \rangle,$$

где

- Σ — *входной алфавит символов,* $\Lambda \in \Sigma$, Λ — *пустой символ,*
- Δ — *входной алфавит символов,* $\Lambda \in \Delta$,
- Q — *конечное множество состояний,*
- q_0 — *начальное состояние,*
- Q_f — *множество заключительных состояний,* $Q_f \subseteq Q$,
- α — *бесконечная последовательность символов из* Δ (оракул),
- F — *правила перехода.* F *по каждому элементу множества* $Q \times \Sigma \times \Delta$ *дает один или более элементов множества* Q.

Если для любых $q \in Q, a \in \Sigma, b \in \Delta$ *существует в точности одно состояние* q_1 *такое, что* $(q, a, b \mapsto q_1) \in F$, *то* M^+ *будем называть* детерминированным.

Через $\alpha(i)$ обозначим i-ый символ последовательности α. В данной работе рассматриваем только рекурсивные оракулы, то есть $\alpha(i)$ — рекурсивная функция. Оракул, состоящий только из пустых символов, будем называть пустым оракулом и обозначать через $\alpha_\emptyset$.

Обозначим пустое слово через $\bar{e}$.

Введём понятие конфигурации M^+.

Определение 2 (конфигурация M^+)**.** *Пусть дан* $M^+ = \langle \Sigma, \Delta, Q, q_0, Q_f, \alpha, F \rangle$. *Тройку вида* $\langle q, \bar{w}, i \rangle$ *будем называть* конфигурацией M^+, *где*

- $q \in Q$ — *состояние,*
- $\bar{w} \in \Sigma^*$ — *входное слово, которое осталось прочитать,*
- i — *номер ячеек на первой и второй лентах (на второй ленте записан* α*), которые обозревает в данный момент головка автомата.*

$\langle q_0, \bar{w}, 0 \rangle$ — начальная конфигурация. $\langle q_f, \bar{e}, i \rangle$ — заключительная конфигурация, *где* $q_f \in Q_f$.

Опишем семантику конечного автомата с оракулом в терминах конфигураций.

Через $\langle q, \bar{w}, i \rangle \vdash^n_{M^+} \langle q_1, \bar{w}_1, i+n \rangle$ обозначим переход автомата

$$M^+ = \langle \Sigma, \Delta, Q, q_0, Q_f, \alpha, F \rangle$$

из конфигурации $\langle q, \bar{w}, i \rangle$ в конфигурацию $\langle q_1, \bar{w}_1, i+n \rangle$ за n шагов, точнее:

1. при $n = 0$: $\langle q, \bar{w}, i \rangle \vdash^0_{M^+} \langle q, \bar{w}, i \rangle$
2. при $n = 1$: $\langle q, \bar{w}, i \rangle \vdash^1_{M^+} \langle q_1, \bar{w}_1, i+1 \rangle$ тогда и только тогда, когда

(a) $\langle q, \bar{w}, i\rangle$ — не заключительная конфигурация,

(b) либо $\bar{w} = a\bar{w}_1$ и $(q, a, \alpha(i) \mapsto q_1) \in F$,
либо $\bar{w} = \bar{w}_1 = \bar{e}$ и $(q, \Lambda, \alpha(i) \mapsto q_1) \in F$,

3. при $m = n + 1$: $\langle q, \bar{w}, i\rangle \vdash^m_{M^+} \langle q_2, \bar{w}_2, i + m\rangle$ тогда и только тогда, когда $\langle q, \bar{w}, i\rangle \vdash^n_{M^+} \langle q_1, \bar{w}_1, i + n\rangle$ и $\langle q_1, \bar{w}_1, i + n\rangle \vdash^1_{M^+} \langle q_2, \bar{w}_2, i + m\rangle$ для некоторых $q_1, \bar{w}_1$.

Будем говорить, что конечный автомат с оракулом останавливается тогда и только тогда, когда он находится в заключительной конфигурации.

Работа M^+ — это последовательность конфигураций, первая из которых — начальная, а каждая следующая получается из предыдущей согласно правилам M^+. Если оракул рекурсивный, то работу автомата можно моделировать алгоритмически, то есть можно написать алгоритм, который по автомату и входному слову будет строить последовательность конфигураций.

Определение 3. Слово $\bar{w}$ воспринимается автоматом M^+ *тогда и только тогда, когда существует такое $n \geq 0$, что*

$$\langle q_0, \bar{w}, 0\rangle \vdash^n_{M^+} \langle q_f, \bar{e}, n\rangle,$$

где q_0 — начальное состояние, q_f — некоторое заключительное состояние. Языком, задаваемым автоматом M^+, *называется множество всех слов, которые им воспринимаются.*

Следствие 1. *Если автомат M^+ не воспринимает слово $\bar{w}$, то он не останавливается на $\bar{w}$.*

Так как конечный автомат с оракулом может работать после конца входного слова, то встает вопрос: остановится ли он когда-нибудь?

Определение 4 (Проблема остановки для оракула)**.** *Зафиксируем оракул α в алфавите Δ.* Проблема остановки для оракула α*: по любому автомату $M^+ = \langle \Sigma, \Delta, Q, q_0, Q_f, \alpha, F\rangle$ и любому входному слову $\bar{w}$ эффективно определить — останавливается M^+ на $\bar{w}$ или нет.*

Определение 5 (Произведение последовательностей)**.** *Зафиксируем алфавит Σ. Пусть даны конечные последовательности $u_1, \ldots, u_n$ символов из Σ. $u_1 \otimes \cdots \otimes u_n$ — это слово в алфавите Σ^n:*

$$u_1 \otimes \cdots \otimes u_n = \begin{bmatrix} u_{11} \\ \vdots \\ u_{n1} \end{bmatrix} \cdots \begin{bmatrix} u_{1k} \\ \vdots \\ u_{nk} \end{bmatrix},$$

где u_{ij} — либо j-ый символ i-ой последовательности, либо символ Λ, если среди $u_1, \ldots, u_n$ есть более длинные последовательности, чем u_i.

Для бесконечных последовательностей произведение определяется аналогично.

вход	$\cdots$	0	$\cdots$	0	$\cdots$	0	$\cdots$	1	$\Lambda\ \cdots\ \Lambda$
оракул	$\cdots$	0	$\cdots$	1	$\cdots$	0	$\cdots$	1	$\cdots\cdots\cdots$

$\underbrace{\qquad\qquad\qquad}_{\log_2 u_i}$

$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{\log_2 u_{i+1}}$

Рис. 1: Подмножество степеней двойки — расширенно-автоматное отношение

Неформально это определение можно понимать как записывание последовательности u_{i+1} под последовательностью u_i, а j-ый символ такой последовательности — «многоэтажный» символ, состоящий из j-ых символов каждой последовательности.

Будем считать, что для любого оракула α верно следующее: $\alpha \otimes \alpha = \alpha$, $\alpha \otimes \alpha_\emptyset = \alpha$. Это означает, что «присоединение» самого себя или пустого оракула не добавляет никакой информации, которую можно было бы использовать при распознавании входа.

Определение 6 (Кодирующая функция)**.** *Зафиксируем алфавит Σ и множество A.* Кодирующей функцией *назовём взаимно однозначное отображение $\sigma : A \longleftrightarrow \Sigma^*$. Будем считать, что $\sigma(a_1, \ldots, a_n) = \sigma(a_1) \otimes \cdots \otimes \sigma(a_n)$.*

Определение 7 (Расширенно-автоматное отношение)**.** *Пусть дан алфавит Σ. Отношение $R^n(x_1, \ldots, x_n)$ над некоторым множеством A будем называть* расширенно-автоматным *для кодирующей функции $\sigma : A \longleftrightarrow \Sigma^*$, если существует автомат M^+ такой, что:*

$$L(M^+) = \{\bar{w} \in \Sigma^* : \sigma^{-1}(\bar{w}) \in R^n\}.$$

Пример 1. *Всякое подмножество степеней двойки $U \subset \{2^x : x \in \omega\}$ — расширенно-автоматное отношение.*

Возьмём оракул α в алфавите $\{0, 1, \Lambda\}$ такой, что единицы стоят в точности под номерами степеней элементов из U. Тогда нетрудно написать программу для конечного автомата с оракулом α, который будет распознавать множество U: элемент $n \in \omega$ должен быть степенью двойки и единица двоичной записи n в обратном порядке должна «стоять» над единицей оракула (рис. 1).

В [5] введено понятие автоматной системы. Мы введём понятие расширенно-автоматной системы.

Определение 8 (Расширенно-автоматная система)**.** *Зафиксируем алфавит Σ. Пусть дана алгебраическая система $\Omega = (A, R_1^{r_1}, \ldots, R_n^{r_n})$. Система Ω называется* расширенно-автоматной, *если существует кодирующая функция $\sigma : A \longleftrightarrow \Sigma^*$, для которой каждое отношение $R_i^{r_i}, 1 \le i \le n$ является расширенно-автоматным.*

Пример 2. *Алгебраическая система $\Omega = (\omega, R_1, \ldots, R_n)$, где каждое отношение $R_i, 1 \le i \le n$ — подмножество степеней двойки, является расширенно-автоматной системой.*

Для дальнейших рассуждений нам понадобится определение языка, задаваемого формулой.

Определение 9 (Язык, задаваемый формулой)**.** *Дана система Ω, носителем которой является множество A, алфавит Σ, кодирующая функция $\sigma : A \longleftrightarrow \Sigma^*$, формула $\phi(x_1, \ldots, x_n)$ в системе Ω.*

Тогда множество слов $L_\phi = \{\bar{w} \in \Sigma^* : \phi(\sigma^{-1}(\bar{w}))$ истинна в системе $\Omega\}$ будем называть языком, задаваемым формулой *ϕ.*

Другими словами, язык, задаваемый формулой — это множество закодированных в некотором алфавите кортежей, на которых истинна формула.

2. Основные свойства конечных автоматов с оракулами

Класс регулярных языков замкнут относительно теоретико-множественных операций, проекции. Для каждого недетерминированного конечного автомата можно эффективно построить детерминированный, задающий тот же язык, что и исходный.

Исследуем свойства замкнутости класса языков, задаваемых конечными автоматами с оракулами.

Теорема 1 (О детерминизации)**.** *Для каждого недетерминированного автомата $M^+ = \langle \Sigma, \Delta, Q, q_0, Q_f, \alpha, F \rangle$ можно эффективно построить детерминированный автомат M_d^+ с оракулом α такой, что $L(M^+) = L(M_d^+)$.*

Доказательство. Построим автомат M_d^+:

$$M_d^+ = \langle \Sigma, \Delta, P(Q), q_0, \{Q' | Q' \in P(Q) \text{ и } Q' \cap Q_f \neq \emptyset\}, \alpha, F' \rangle.$$

Правила F' — множество правил вида: $Q, a, b \mapsto \bigcup\limits_{q \in Q} \{F(q, a, b)\}$, где $Q \in P(Q)$, $P(Q)$ — множество всех подмножеств Q.

Доказательство того, что $L(M^+) = L(M_d^+)$ аналогично доказательству в теории конечных автоматов. □

Теорема 2 (Замкнутость относительно пересечения)**.** *Пусть даны два детерминированных автомата $M_1^+ = \langle \Sigma, \Delta_1, Q_1, q_0^1, Q_f^1, \alpha_1, F_1 \rangle$ и $M_2^+ = \langle \Sigma, \Delta_2, Q_2, q_0^2, Q_f^2, \alpha_2, F_2 \rangle$, задающие языки $L(M_1^+)$ и $L(M_2^+)$ соответственно. Тогда можно эффективно построить детерминированный конечный автомат с оракулом $\alpha_1 \otimes \alpha_2$, задающий $L(M_1^+) \cap L(M_2^+)$.*

Доказательство. Построим автомат M_3^+:

$$M_3^+ = \langle \Sigma, \Delta_1 \times \Delta_2, Q_1 \times Q_2, \langle q_0^1, q_0^2 \rangle, Q_f^1 \times Q_f^2, \alpha_1 \otimes \alpha_2, F \rangle.$$

Правила F — множество правил вида: $\langle q_1, q_2 \rangle, a,\ \langle b_1, b_2 \rangle \mapsto \langle F_1(q_1, a, b_1), F_2(q_2, a, b_2) \rangle$, где $q_i \in Q_i$, b_i — некоторый символ последовательности α_i, $i \in \{1, 2\}$.

Доказательство того, что $L(M_3^+) = L(M_1^+) \cap L(M_2^+)$ аналогично доказательству в теории конечных автоматов. □

Определение 10 (Проекция)**.**

1. *Пусть дан символ* $W = \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}$. Проекцией символа W *по* i*-му аргументу назовём символ:*
$$\tau_i(W) = \begin{bmatrix} w_1 \\ \vdots \\ w_{i-1} \\ w_{i+1} \\ \vdots \\ w_n \end{bmatrix}.$$

2. Проекция слова $\bar{W} = W_1 \cdots W_n$ *— это слово* $\tau_i(\bar{W}) = \tau_i(W_1) \cdots \tau_i(W_n)$.

3. Проекцией языка L *назовём язык* $\tau_i(L) = \{\tau_i(\bar{W}) : \bar{W} \in L\}$.

Теорема 3 (Замкнутость относительно проекции)**.** *Пусть дан детерминированный автомат* $M^+ = \langle \Sigma^k, \Delta, Q, q_0, Q_f, \alpha, F \rangle$. *Пусть* $L(M^+)$ *— язык, задаваемый этим автоматом. Тогда можно эффективно построить детерминированный автомат* $M^+_\exists$ *с тем же оракулом, задающий язык* $L(M^+_\exists) = \tau_i(L(M^+))$.

Доказательство. Построим сначала недетерминированный автомат $N^+_\exists$ по M^+:
$$N^+_\exists = \langle \Sigma^{k-1}, \Delta, Q, q_0, Q_f, \alpha, F' \rangle.$$
Правила F' определяются следующим образом: для каждого правила $(q, a, b \mapsto q') \in F$ добавим в F' правило $q, \tau_i(a), b \mapsto q'$. Доказательство того, что $L(N^+_\exists) = \tau_i(L(M^+))$ аналогично доказательству в теории конечных автоматов. По теореме 1 теперь эффективно построим детерминированный автомат $M^+_\exists$, который задает тот же язык, что и $N^+_\exists$. □

Очевидно, что конечный автомат с пустым оракулом работает также как обычный конечный автомат.

Пусть $\mathcal{K}$ — это класс языков, задаваемых конечными автоматами, а $\mathcal{K}^+$ — класс языков, задаваемых конечными автоматами с оракулами.

Теорема 4. $\mathcal{K} \subset \mathcal{K}^+$.

Доказательство. Рассмотрим множество слов $U_{x^2} = \{0^{x^2} \cdot 1 : x \in \omega\}$. Это множество не регулярно, но оно распознается автоматом M^+, оракул которого определяется так: единица стоит в точности под номером x^2 для всех x. □

Так как недетерминированные конечные автоматы с оракулами задают те же языки, что и детерминированные, то в дальнейшем везде под конечным автоматом с оракулом будем понимать детерминированный автомат.

3. Эффективные дополнения

При некоторых оракулах α по произвольному M^+ с α можно эффективно построить автомат, который задает дополнение языка $L(M^+)$, то есть каждый такой

α определяет подкласс языков, который замкнут относительно дополнения. В таких случаях удобно говорить, что оракул α допускает эффективное дополнение языков.

Определение 11 (Оракул допускает эффективное дополнение)**.** *Пусть дан оракул α. Если по произвольному автомату M^+ с оракулом α можно эффективно построить конечный автомат с тем же оракулом, который задает дополнение языка $L(M^+)$, то будем говорить, что оракул α* допускает эффективное дополнение*.*

Теорема 5. *Если оракул допускает эффективное дополнение, то проблема остановки для него разрешима.*

Доказательство. Пусть дан оракул α, который допускает эффективное дополнение. Тогда по произвольному автомату M^+ с оракулом α можно эффективно построить автомат $\bar{M}^+$ с тем же оракулом, задающий дополнение языка $L(M^+)$. Запустим автоматы M^+ и $\bar{M}^+$ на слове $\bar{w}$. Если $\bar{M}^+$ воспримет слово $\bar{w}$, то M^+ его не воспримет, то есть, не остановится. Таким образом, по произвольному M^+ с оракулом α и произвольному входному слову $\bar{w}$ можно эффективно определить — остановится M^+ на $\bar{w}$ или нет. □

Через $\alpha(i,j)$ обозначим подпоследовательность последовательности α, начиная с i-го символа последовательности и до j-го включительно, $|\beta|$ — количество элементов конечной последовательности β.

Лемма 1. *Пусть дан произвольный автомат M^+ с s состояниями и произвольное входное слово $\bar{w}$. Запустим M^+ на $\bar{w}$. Пусть $\alpha(x,y)$ — фрагмент оракула α после конца входного слова, который состоит из одинаковых символов и его длина больше s. Пусть $T = (t_0, t_1, \ldots, t_n)$ — последовательность состояний при работе M^+ на $\alpha(x,y)$.*

Тогда $T = (\epsilon, \pi, \ldots, \pi, \gamma)$, где $\gamma = \pi(0,m)$ для некоторого m, $\epsilon = (t_0, \ldots, t_{k-1})$, $\pi = (t_k, \ldots, t_{l-1})$, где

$$\begin{aligned} k &= \min\{u \geq 0 : (\exists w)(w > u \wedge t_u = t_w)\}, \\ l &= \min\{u : u > k \wedge t_u = t_k\}. \end{aligned}$$

Доказательство. Это следует из условия и семантики работы автомата M^+. □

Неформально лемма 1 говорит о том, что если автомат читает фрагмент оракула за входным словом, состоящий из одинаковых символов, и длина этого фрагмента больше s (число состояний), то у автомата не хватит состояний, чтобы прочитать все символы в разных состояниях. Получится так, что до некоторого момента может идти последовательность разных состояний ϵ, а затем некоторая последовательность состояний π будет повторяться (рис. 2).

Определение 12. *С помощью $\alpha_{x!}$ будем обозначать оракул в алфавите $\{0,1\}$ такой, что:*

1. $\alpha_{x!}(0) = 1$,
2. *i-ую от $i+1$-ой единицы отделяет $i!$ нулей.*

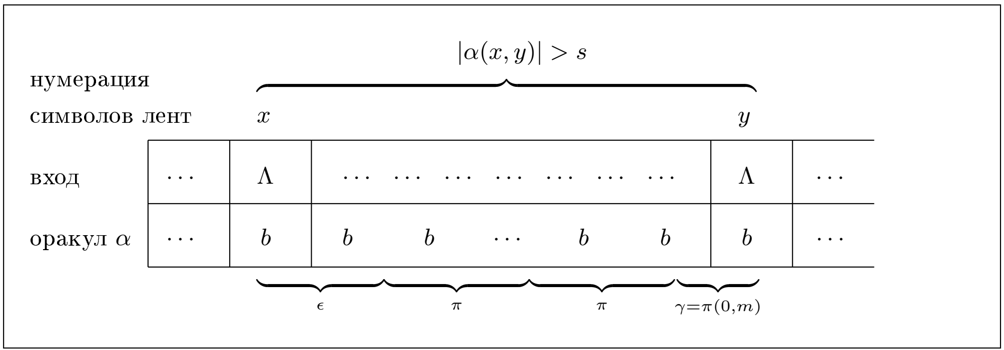

Рис. 2: Повторяющаяся последовательность состояний

Теорема 6. *Оракул $\alpha_{x!}$ допускает эффективное дополнение.*

Доказательство. Рассмотрим произвольный автомат

$$M^+ = \langle \{0, 1, \Lambda\}, \{0, 1, \Lambda\}, Q, q_0, Q_f, \alpha_{x!}, F\rangle$$

с s состояниями и произвольное входное слово. Пусть t_i — состояние, в котором M^+ прочитал i-ую единицу оракула после конца входного слова. Пусть $T = (t_{2s}, \dots, t_{3s})$. Согласно семантике M^+ в T есть одинаковые элементы. Возьмём i и j (рис. 3) такие, что:

$$\begin{aligned} i &= \min\{u \geq 2s : (\exists w)(w > u \wedge t_u = t_w)\}, \\ j &= \min\{u : u > i \wedge t_u = t_i\}. \end{aligned}$$

и рассмотрим две последовательности α_1 — фрагмент оракула, начиная с i-ой единицы и до $i+1$-ой включительно после конца входного слова и α_2 — фрагмент оракула, начиная с j-ой единицы и до $j+1$-ой включительно после конца входного слова. Пусть T_1 — последовательность состояний при работе M^+ на α_1, T_2 — на α_2. Тогда, из леммы 1 следует, что $T_1 = (t_i, \epsilon_1, \pi_1, \dots, \pi_1, \gamma_1, t)$, $T_2 = (t_i, \epsilon_2, \pi_2, \dots, \pi_2, \gamma_2, r)$. Из семантики работы автомата M^+ следует, что $\epsilon_1 = \epsilon_2$ и $\pi_1 = \pi_2$. Обозначим их просто ϵ и π.

Покажем, что $\gamma_1 = \gamma_2$. Так как $\gamma_1 = \pi(0, m_1)$, $\gamma_2 = \pi(0, m_2)$ для некоторых m_1, m_2, то достаточно показать, что $m_1 = m_2$. Из определения оракула следует, что $|\alpha_1| - 2 = (i + \mathfrak{c})!$, $|\alpha_2| - 2 = (j + \mathfrak{c})!$, где $\mathfrak{c}$ — количество единиц оракула до конца входного слова. m_1 определяется из соотношения:

$$(i + \mathfrak{c})! - |\epsilon| \equiv m_1 \pmod{|\pi|},$$

m_2 из соотношения:

$$(j + \mathfrak{c})! - |\epsilon| \equiv m_2 \pmod{|\pi|}.$$

Так как

$$|\epsilon| < s, |\pi| \leq s,$$

то $m_1 = m_2$ и, следовательно, $\gamma_1 = \gamma_2$ (рис. 4).

Тогда, так как M^+ — детерминированный, то $t = r$, то есть $(i+1)$-ую и $(j+1)$-ую единицы M^+ прочитает в одном и том же состоянии. Рассуждая аналогично, можно показать, что для $k > 1$ единицы под номерами $i+k$ и $j+k$ автомат M^+ прочитает в одном и том же состоянии. Это означает, что за j-ой единицей оракула после конца входного слова будут появляться только те состояния, которые появлялись на фрагменте оракула от i-ой до j-ой единицы. Таким образом, если среди состояний при работе автомата M^+ до j-ой единицы оракула после конца входного слова нет заключительного, то его не будет и далее, то есть M^+ не останавливается.

Теперь построим автомат M_1^+:

$$M_1^+ = \langle \Sigma, \Delta, Q \times D, \langle q_0, d_0 \rangle, (Q \setminus Q_f) \times \{d_{3s}\}, \alpha_{x!}, F' \rangle,$$

такой, что

$$L(M_1^+) = \overline{L(M^+)}.$$

Здесь $D = \{d_0, \dots, d_{3s}\}$, программа F' определяется следующим образом:

1. Для каждого правила $(q, a, b \mapsto q_1) \in F$, где $a \neq \Lambda$ добавим в F' правило: $\langle q, d_0 \rangle, a, b \mapsto \langle q_1, d_0 \rangle$.

2. Для каждого правила $(q_f, \Lambda, b \mapsto q_1) \in F$, добавим в F' правила $\langle q_f, d_i \rangle, \Lambda, b \mapsto \langle q_f, d_i \rangle$ для всех $0 \leq i \leq 3s$,

3. Для каждого правила $(q, \Lambda, 0 \mapsto q_1) \in F$, где $q \notin Q_f$ добавим в F' правила $\langle q, d_i \rangle, \Lambda, 0 \mapsto \langle q_1, d_i \rangle$ для всех $0 \leq i \leq 3s$,

4. Для каждого правила $(q, \Lambda, 1 \mapsto q_1) \in F$, где $q \notin Q_f$ добавим в F' правила $\langle q, d_i \rangle, \Lambda, 1 \mapsto \langle q_1, d_{i+1} \rangle$ для всех $0 \leq i \leq 3s - 1$.

Пункт (1) означает, что M_1^+ работает также как и M^+ пока входное слово не кончилось.

Пункт (2) означает, что если в M^+ перешли в заключительную конфигурацию, то в M_1^+ зацикливаемся, т.е не останавливаемся.

Пункты $(3), (4)$ означают, что M_1^+ работает также как и M^+, но если M^+ читает символ 1 в $\alpha_{x!}$ после конца входного слова, то M_1^+ «считает» этот символ.

Таким образом, если M^+, прочитав $C = 3s$ единиц в $\alpha_{x!}$ после конца входного слова не остановится, то он не остановится вообще. Но тогда M_1^+ перейдет в состояние $\langle q, d_{3s} \rangle$ для некоторого $q \notin Q_f$, т.е воспримет входное слово.

Следовательно, $L(M_1^+) = \overline{L(M^+)}$.

Итак, оракул $\alpha_{x!}$ допускает эффективное дополнение. □

Определение 13. *Через α_x будем обозначать оракул в алфавите $\{0, 1\}$ такой, что:*

1. $\alpha_x(0) = 1$,

2. *i-ую от $i+1$-ой единицы отделяет i нулей.*

Теорема 7. *Оракул α_x допускает эффективное дополнение.*

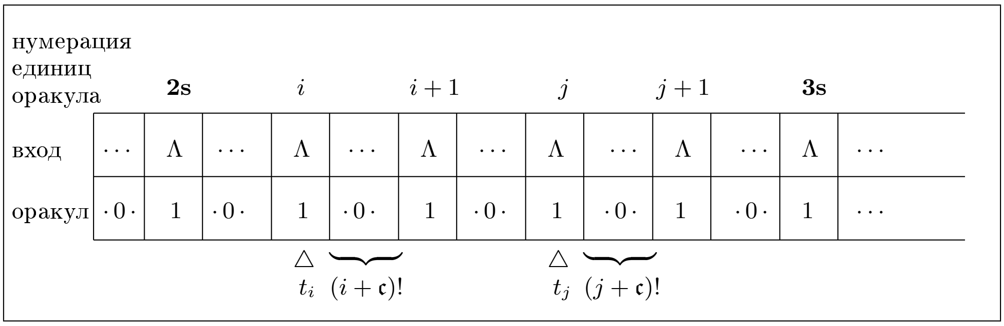

Рис. 3: Фрагмент оракула $\alpha_{x!}$ за входным словом, при чтении единиц которого появятся одинаковые состояния

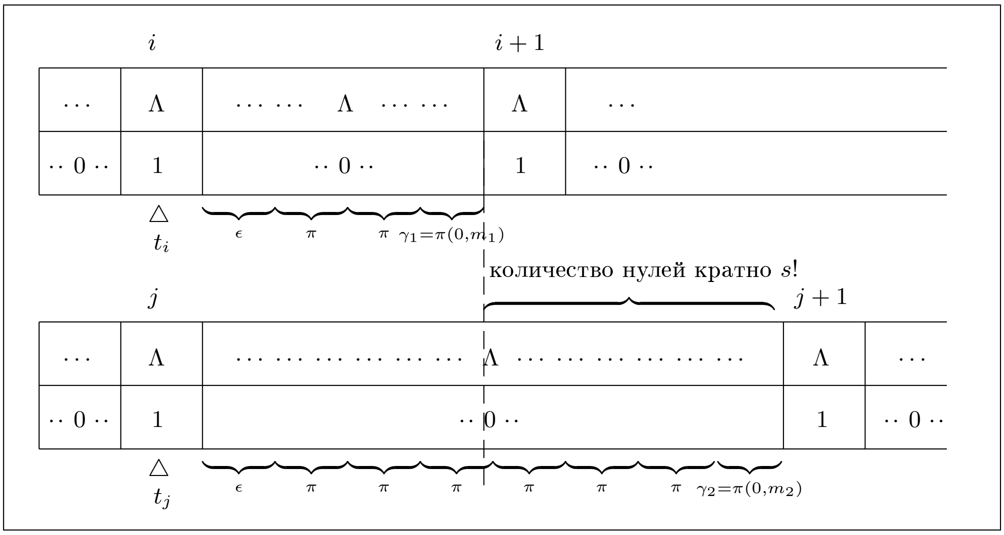

Рис. 4: Фрагменты оракула $\alpha_{x!}$ за входным словом, на которых автомат работает одинаковым образом

Доказательство. Рассмотрим произвольный автомат

$$M^+ = \langle \{0, 1, \Lambda\}, \{0, 1, \Lambda\}, Q, q_0, Q_f, \alpha_x, F \rangle$$

с s состояниями и произвольное входное слово. Пусть t_i — состояние, в котором M^+ прочитал $(i \times s!)$-ую единицу оракула после конца входного слова. Пусть $T = (t_2, \dots, t_{s+2})$. Согласно семантике M^+ в T есть одинаковые элементы. Возьмём i и j (рис. 5) такие, что:

$$i = \min\{u \geq 2 : (\exists w)(w > u \wedge t_u = t_w)\},$$
$$j = \min\{u : u > i \wedge t_u = t_i\}.$$

и рассмотрим две последовательности α_1 — фрагмент оракула, начиная с $(i \times s!)$-ой единицы и до $(i \times s! + 1)$-ой включительно после конца входного слова и α_2 — фрагмент оракула, начиная с $(j \times s!)$-ой единицы и до $(j \times s! + 1)$-ой включительно после конца входного слова. Пусть T_1 — последовательность состояний при работе M^+ на α_1, T_2 — на α_2. Тогда, из леммы 1 следует, что $T_1 = (t_i, \epsilon_1, \pi_1, \dots, \pi_1, \gamma_1, t)$, $T_2 = (t_i, \epsilon_2, \pi_2, \dots, \pi_2, \gamma_2, r)$. Из семантики работы автомата M^+ следует, что $\epsilon_1 = \epsilon_2$ и $\pi_1 = \pi_2$. Обозначим их просто ϵ и π.

Покажем, что $\gamma_1 = \gamma_2$. Так как $\gamma_1 = \pi(0, m_1)$, $\gamma_2 = \pi(0, m_2)$ для некоторых m_1, m_2, то достаточно показать, что $m_1 = m_2$. Из определения оракула следует, что $|\alpha_1| - 2 = i \times s! + \mathfrak{c}$, $|\alpha_2| - 2 = j \times s! + \mathfrak{c}$, где $\mathfrak{c}$ — количество единиц оракула до конца входного слова. m_1 определяется из соотношения:

$$i \times s! + \mathfrak{c} - |\epsilon| \equiv m_1 \pmod{|\pi|},$$

m_2 из соотношения:

$$j \times s! + \mathfrak{c} - |\epsilon| \equiv m_2 \pmod{|\pi|}.$$

Так как

$$|\epsilon| < s, |\pi| \leq s,$$

то $m_1 = m_2$ и, следовательно, $\gamma_1 = \gamma_2$ (рис. 6).

Тогда, так как M^+ — детерминированный, то $t = r$, то есть $(i \times s! + 1)$-ую и $(j \times s! + 1)$-ую единицы M^+ прочитает в одном и том же состоянии. Рассуждая аналогично, можно показать, что для $k > 1$ единицы под номерами $i \times s! + k$ и $j \times s! + k$ автомат M^+ прочитает в одном и том же состоянии. Это означает, что за $(j \times s!)$-ой единицей оракула после конца входного слова будут появляться только те состояния, которые появлялись на фрагменте оракула от $(i \times s!)$-ой до $(j \times s!)$-ой единицы. Таким образом, если среди состояний при работе автомата M^+ до $(j \times s!)$-ой единицы оракула после конца входного слова нет заключительного, то его не будет и далее, то есть M^+ не останавливается.

Теперь построим автомат M_1^+:

$$M_1^+ = \langle \Sigma, \Delta, Q \times D, \langle q_0, d_0 \rangle, (Q \setminus Q_f) \times \{d_{(s+2)!}\}, \alpha_x, F' \rangle,$$

такой, что

$$L(M_1^+) = \overline{L(M^+)}.$$

Здесь $D = \{d_0, \dots, d_{(s+2)!}\}$, программа F' определяется аналогично теореме 6. □

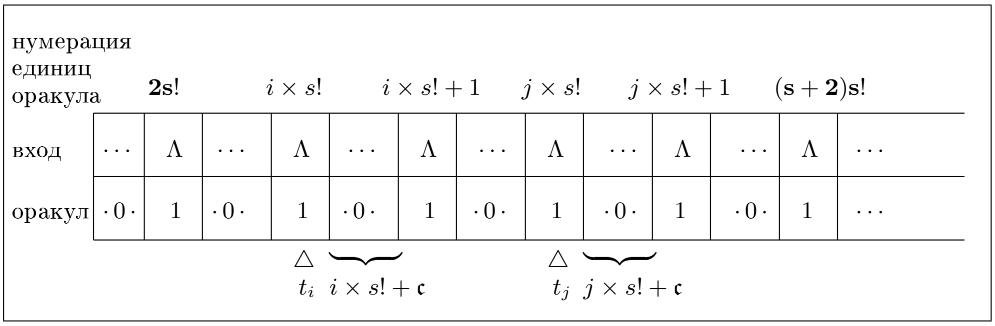

Рис. 5: Фрагмент оракула α_x за входным словом, при чтении единиц которого появятся одинаковые состояния

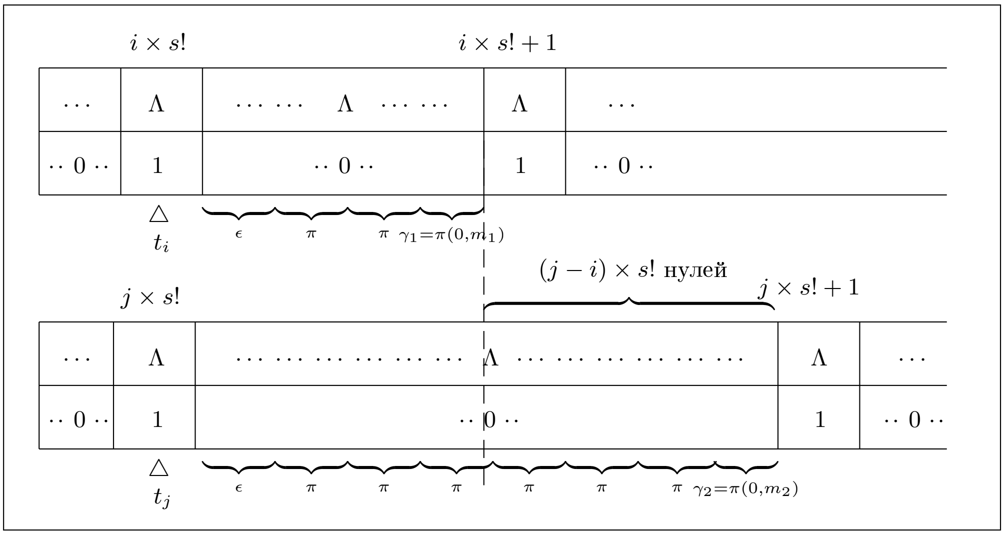

Рис. 6: Фрагменты оракула α_x за входным словом, на которых автомат работает одинаковым образом

4. Разрешимость теорий

В [5] доказан результат, что по любой формуле автоматной системы можно эффективно построить конечный автомат, который проверяет истинность формулы. По существу, это утверждение следует из того, что конечные автоматы замкнуты относительно теоретико-множественных операций, проекции.

Классы языков, задаваемых конечными автоматами с оракулами, замкнуты относительно пересечения, проекции и, в некоторых случаях (примеры оракулов $\alpha_{x!}$, α_x), относительно дополнения, поэтому мы сформулируем и докажем подобный [5] результат.

Определение 14 (Оракул расширенно-автоматной системы). *Пусть дана расширенно-автоматная система Ω сигнатуры $\Xi = \langle R_1^{r_1}, \dots, R_n^{r_n} \rangle$. Через α_i обозначим оракул автомата M_i^+, который распознает отношение $R_i^{r_i}$. Оракул $\alpha = \alpha_1 \otimes \dots \otimes \alpha_n$ назовём* оракулом расширенно-автоматной системы Ω.

Теорема 8. *Пусть дана расширенно-автоматная система Ω сигнатуры $\Xi = \langle R_1^{r_1}, \dots, R_n^{r_n} \rangle$. Пусть α — оракул Ω, который допускает эффективное дополнение.*

Тогда по любой формуле $\phi(\bar{x})$ этой системы можно эффективно построить конечный автомат с оракулом α, распознающий язык L_ϕ.

Доказательство. Индукция по сложности формулы:

1. Для атомных формул $R_i^{r_i}(x)$ утверждение следует из определения расширенно-автоматного отношения.

2. Для $\phi_1(\bar{x}) \wedge \phi_2(\bar{x})$, $(\exists x_j)\phi(\bar{x})$ — из теорем 2, 3 соответственно.

3. Пусть $\phi_1(\bar{x}) = \neg\phi(\bar{x})$. Для $\phi(\bar{x})$ эффективно строится M^+, для которого, согласно условию, эффективно строится M_1^+, задающий дополнение языка $L(M^+)$. Тогда в качестве автомата для $\phi_1(\bar{x})$ возьмём M_1^+.

□

Следствие 2. *Пусть дана расширенно-автоматная система Ω. Если оракул системы Ω допускает эффективное дополнение, то $\mathrm{Th}(\Omega)$ — разрешима.*

Доказательство. Если оракул α системы Ω допускает эффективное дополнение, то по любой замкнутой формуле можно эффективно построить автомат M^+ с α, распознающий язык, задаваемый формулой. Если автомат остановится, то формула истинна, иначе ложна, то есть по любой формуле можно эффективно определить — истинна она или ложна. □

Теорема 9. *Пусть дана расширенно-автоматная система Ω'. Обогатим систему Ω' произвольным множеством автоматных отношений до системы Ω''. Тогда Ω'' будет расширенно-автоматной и в качестве её оракула можно взять оракул системы Ω'.*

Доказательство. Ясно, что система Ω'' будет снова расширенно-автоматной, так как каждое автоматное отношение распознается некоторым автоматом M^+ с пустым оракулом $\alpha_\emptyset$.

Пусть α — оракул системы Ω'. Так как $\alpha \otimes \alpha_\emptyset = \alpha$, то в качестве оракула системы Ω'' можно выбрать сам оракул α. □

Из теоремы 9 следует, что если мы обогащаем расширенно-автоматную систему, оракул которой допускает эффективное дополнение, автоматными отношениями, то получаем новую расширенно-автоматную систему, теория которой — разрешима.

В предыдущей главе мы рассмотрели оракулы $\alpha_{x!}$, α_x, которые допускают эффективное дополнение. По ним можно взаимно однозначно построить одноместные предикаты. Для оракула $\alpha_{x!}$ таким предикатом будет $U_{x!}$, который определяется следующим образом:

1. $u_0 = 2^0$,
2. $u_{i+1} = 2^{\log_2(u_i)+1+(i+1)!}$.

По оракулу α_x взаимно однозначно строится предикат U_x, который определяется так:

1. $u_0 = 2^0$,
2. $u_{i+1} = 2^{\log_2(u_i)+1+(i+1)}$.

Мы получаем, что единицы этих оракулов стоят в точности под номерами степеней элементов из $U_{x!}$, U_x соответственно.

Системы $(\omega, U_{x!})$, (ω, U_x) являются расширенно-автоматными. Их теории являются разрешимыми, так как оракулы $\alpha_{x!}$ и α_x допускают эффективное дополнение.

Любое натуральное число можно однозначно разложить в сумму различных степеней двойки в соответствии с его двоичной записью. Для краткости степени двойки мы будем называть **атомами**. Множество атомов числа x будем обозначать через $\mathrm{Atoms}(x)$.

Определение 15. *Отношение* $\mathtt{E}(x, y)$, *введённое в [4], означает, что* x *— атом, который встречается в разложении числа* y, *то есть:*

$$\mathtt{E}(x, y) \Longleftrightarrow x \in \mathrm{Atoms}(y)$$

Например,

$$19 = 16 + 2 + 1 = 2^4 + 2^1 + 2^0$$

$$(16, 19) \in \mathtt{E}, \text{ но } (4, 19) \notin \mathtt{E}.$$

Отношение $\mathtt{E}$ — автоматное, так как достаточно проверять, что $n \in \omega$ — степень двойки и единица двоичной записи числа x «стоит» над некоторой единицей двоичной записи числа y.

Системы $(\omega, 0, 1, <, +, \mathtt{E}, U_{x!})$, $(\omega, 0, 1, <, +, \mathtt{E}, U_x)$ (получены из системы $(\omega, 0, 1, <, +, \mathtt{E}^*)$ [2]) являются расширениями неавтоматных систем $(\omega, U_{x!})$, (ω, U_x) автоматными отношениями (каждую формулу с функциональными символами местности n можно преобразовать в эквивалентную ей формулу, где каждый функциональный символ заменен на некоторый предикатный символ местности $n+1$). Следовательно, их теории являются разрешимыми.

Покажем, что наш метод позволяет доказывать разрешимость, когда не применима элиминация кванторов и не выполняется свойство автоматности системы.

Рассмотрим систему $\Omega = (\omega, <, \mathtt{E}, U_{x!})$, которая представляет собой обогащение системы $(\omega, U_{x!})$ автоматными отношениями $<, \mathtt{E}$. Теория системы Ω — разрешима согласно следствию 2.

Докажем, что теория $\mathrm{Th}(\Omega)$ не допускает элиминацию кванторов. Мы будем доказывать, что теория $\mathrm{Th}(\Omega)$ не является модельно полной.

Теорема 10. *Теория* $\mathrm{Th}(\omega, <, \mathtt{E}, U_{x!})$ *не является модельно полной.*

Доказательство. Пусть u_a — элемент множества $U_{x!}$ с номером a. Определим отображение на ω:

$$h(x) = \begin{cases} 0, & \text{если } x = 0, \\ \sum\limits_{a \in B_1(x)} u_a + \sum\limits_{b \in B_2(x)} 2u_b & \text{иначе,} \end{cases}$$

где

$$B_1(x) = \{a \in \mathrm{Atoms}(x) : a \in U_{x!}\},$$
$$B_2(x) = \{a \in \mathrm{Atoms}(x) : a \notin U_{x!}\}.$$

Если $B_i(x) = \emptyset, i \in \{1, 2\}$, то соответствующую сумму образов атомов будем полагать равной нулю.

Замечание: если x — степень двойки, то $h(x)$ — также степень двойки по определению. Пусть $h(x)$ — степень двойки. Поскольку все атомы a_i в x — разные, все элементы u_{a_i} — разные, $u_j > 2u_i$ для любых $j > i$ и никакая конечная сумма разных степеней двойки степень двойки не даст, то x — степень двойки.

Покажем, что h — изоморфизм систем $\Omega_1 = (h[\omega], <, \mathtt{E}, U_{x!})$ и $\Omega = (\omega, <, \mathtt{E}, U_{x!})$.

Отношение $U_{x!}$ при таком выборе h сохраняется. Действительно, если $y \in U_{x!}$, то $B_1(y) = \{y\}$, а $B_2(y) = \emptyset$. Тогда $h(y) = u_y$, но u_y — элемент множества $U_{x!}$. В обратную сторону, пусть $h(y) \in U_{x!}$. Согласно замечанию выше, y — степень двойки. Пусть теперь $B_2(y) = \{y\}$. Тогда $y \notin U_{x!}$ и $u_y \in U_{x!}$ по определению, но $2u_y \notin U_{x!}$. Так как $h(y) = 2u_y$, то $h(y) \notin U_{x!}$. Противоречие. Значит $B_1(y) = \{y\}$, то есть $y \in U_{x!}$.

Покажем, что отношение $<$ также сохраняется. Пусть $x < y$. Рассмотрим два случая.

1. $\log_2 x < \log_2 y$, то есть y длиннее x, если рассматривать их двоичный код. Пусть $a_x = \max\{a : a \in \mathrm{Atoms}(x)\}$, $a_y = \max\{a : a \in \mathrm{Atoms}(y)\}$. Ясно, что

   $$2u_{a_x} > \sum_{d \in \mathrm{Atoms}(x)} u_d.$$

   Так как $u_j \geq 4u_i$ для любых $j > i$ и $a_y > a_x$, то

   $$u_{a_y} \geq 4u_{a_x} > 2 \sum_{d \in \mathrm{Atoms}(x)} u_d.$$

То есть, получаем, что:

$$h(x) \leq \sum_{d \in \mathrm{Atoms}(x)} 2u_d = 2 \sum_{d \in \mathrm{Atoms}(x)} u_d < 4u_{a_x} \leq u_{a_y} \leq h(y).$$

2. $\log_2 x = \log_2 y$.

$$\begin{aligned} \mathrm{Atoms}(x) = \mathrm{Atoms}(x) \cap \mathrm{Atoms}(y) + \mathrm{Atoms}(x) \setminus \mathrm{Atoms}(y), \\ \mathrm{Atoms}(y) = \mathrm{Atoms}(x) \cap \mathrm{Atoms}(y) + \mathrm{Atoms}(y) \setminus \mathrm{Atoms}(x). \end{aligned}$$

В соответствии с таким разложением x, y можно представить так:

$$\begin{aligned} x &= z + x', \\ y &= z + y', \end{aligned}$$

где

$$\begin{aligned} z &= \sum \mathrm{Atoms}(x) \cap \mathrm{Atoms}(y), \\ x' &= \sum \mathrm{Atoms}(x) \setminus \mathrm{Atoms}(y) \\ y' &= \sum \mathrm{Atoms}(y) \setminus \mathrm{Atoms}(x). \end{aligned}$$

Здесь под $\sum C$ мы понимаем сумму всех элементов множества C. Тогда $\log_2 x' < \log_2 y'$.

Пусть r, t такие натуральные числа, что $\mathrm{Atoms}(r) \cap \mathrm{Atoms}(t) = \emptyset$. Тогда

$$\sum_{a \in B_1(r+t)} u_a = \sum_{b \in B_1(r)} u_b + \sum_{c \in B_1(t)} u_c,$$

$$\sum_{d \in B_2(r+t)} u_d = \sum_{e \in B_2(r)} u_e + \sum_{f \in B_2(t)} u_f,$$

$$h(r+t) = \left(\sum_{b \in B_1(r)} u_b + \sum_{e \in B_2(r)} 2u_e \right) + \left(\sum_{c \in B_1(t)} u_c + \sum_{f \in B_2(t)} 2u_f \right) = h(r) + h(t).$$

Так как

$$\begin{aligned} \mathrm{Atoms}(z) \cap \mathrm{Atoms}(x') = \emptyset, \\ \mathrm{Atoms}(z) \cap \mathrm{Atoms}(y') = \emptyset, \end{aligned}$$

то

$$\begin{aligned} h(z + y') = h(z) + h(y'), \\ h(z + x') = h(z) + h(x'). \end{aligned}$$

Но $h(x') < h(y')$ по случаю 1, следовательно, $h(x) < h(y)$.

В обратную сторону доказательство тривиальное, поскольку предположение, что $h(x) < h(y)$ и $x \geq y$ сразу приводит к противоречию.

Отношение $\mathtt{E}$ при таком выборе h сохраняется. Пусть $x \, \mathtt{E} \, y$.

$$h(y) = \sum_{a \in B_1(y)} u_a + \sum_{b \in B_2(y)} 2u_b.$$

Ясно, что $h(x)$ является одной из сумм $\sum\limits_{a \in B_1(y)} u_a$, $\sum\limits_{b \in B_2(y)} 2u_b$ числа $h(y)$. Не теряя общности предположим, что $h(x) = \sum\limits_{a \in B_1(y)} u_a$. Так как $h(x)$ — степень двойки, а никакая конечная сумма разных степеней двойки не является снова степенью двойки, то никакая совокупность разных слагаемых суммы $\sum\limits_{b\in B_2(y)} 2u_b$ не даст снова $h(x)$. Таким образом, $h(x)$ будет принадлежать $\mathrm{Atoms}(h(y))$, то есть $h(x)\,\mathtt{E}\,h(y)$.

В обратную сторону. Пусть $h(x)\,\mathtt{E}\,h(y)$. $h(x)$ — степень двойки. Согласно замечанию выше x — также является степенью двойки. Так как никакая конечная сумма разных степеней двойки не является степенью двойки, то x встречается среди атомов числа y, то есть $x\,\mathtt{E}\,y$.

Итак, система Ω_1 изоморфна системе Ω. Более того система Ω_1 является подсистемой системы Ω, так как отношения системы Ω_1 — ограничения отношений системы Ω на множество $h(\omega)$.

Рассмотрим формулу

$$U_{x!}(y) \to (\forall z)(z < y \to \neg U_{x!}(z)),$$

которая утверждает, что y — минимальный элемент множества $U_{x!}$.

В системе Ω_1 элемент $x = 4$ является минимальным элементом множества $U_{x!}$, а в системе Ω — нет. Таким образом, система Ω_1 — не элементарная подсистема системы Ω, следовательно, теория $\mathrm{Th}(\Omega)$ — не модельно полна, поэтому не допускает элиминацию кванторов. $\square$

Заключение

Итак, мы ввели понятие конечных автоматов с оракулами и показали, что при некоторых ограничениях с их помощью можно доказывать разрешимость теорий. Приведен пример неавтоматной системы, теория которой не допускает элиминацию кванторов, но которая является расширенно-автоматной и её теория является разрешимой.

Нас интересуют следующие, оставшиеся открытыми в работе, вопросы:

- Существуют ли рекурсивные оракулы, проблема остановки для которых не разрешима?

- Всякий ли оракул, для которого проблема остановки разрешима, допускает эффективное дополнение?

- Пусть оракулы $\alpha_1, \cdots, \alpha_n$ допускают эффективное дополнение. Оракул $\alpha_1 \otimes \cdots \otimes \alpha_n$ допускает эффективное дополнение?

- Оценить сложность введённого метода установления истинности формулы в расширенно-автоматной системе.

Список литературы

[1] Булос Дж., Джеффри Р. Вычислимость и логика. М.: Мир, 1994.

[2] Дудаков С.М. Трансляционная теорема и автоматные структуры. // Вестник ТвГУ сер. Прикл. матем., 4(21), 2006. С. 5–35.

[3] Кейслер Г.,Чен Ч. Теория моделей. М.: Мир, 1977.

[4] Тайцлин М.А. Ограниченные псевдоконечная однородность и изолированность. // Вестник Тверского государственного университета, № 2, 2003. стр. 14-15.

[5] Blumensath A., Graedel E. Automatic structures. //Proc. 15th IEEE Symp. on Logic in Computer Science, 2000.

[6] Rabin M.O. Decidability of second-order theories and automata on infinite trees. // Transactions of the American Mathematical Society, V.141(7), 1969. P. 1-35.