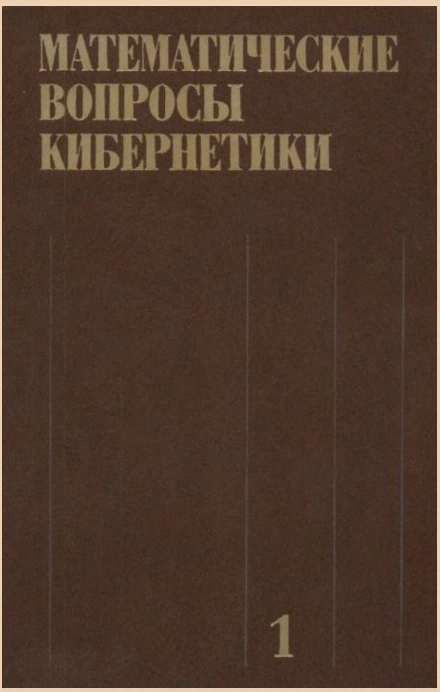

С. С. Марченков

О сложности проблемы разрешения для некоторых классов предикатных формул

Рекомендуемая форма библиографической ссылки: Марченков С. С. О сложности проблемы разрешения для некоторых классов предикатных формул // Математические вопросы кибернетики. Вып. 1. — М.: Физматлит, 1988. — С. 191–200. URL: http://library.keldysh.ru/mvk.asp?id=1988-191

О СЛОЖНОСТИ ПРОБЛЕМЫ РАЗРЕШЕНИЯ ДЛЯ НЕКОТОРЫХ КЛАССОВ ПРЕДИКАТНЫХ ФОРМУЛ

С. С. МАРЧЕНКОВ

(МОСКВА)

В большинстве работ по сложности разрешения логических теорий, как правило, верхняя оценка временной сложности разрешения получается существенно выше нижней оценки или же обе оценки даются в терминах сложности недетерминированных вычислений. Одним из немногих исключений в этом направлении является работа [4]. В ней среди других результатов устанавливаются близкие верхняя и нижняя оценки временной сложности детерминированного разрешения проблемы выполнимости для двух классов формул узкого исчисления предикатов. Один из этих классов состоит из всех замкнутых формул, которые имеют в предваренной нормальной форме кванторный префикс вида $\exists \cdots \exists \forall \exists \cdots \exists$ и содержат лишь одноместные предикатные символы. Если через $DT(T(n))$ обозначить класс множеств, распознаваемых одноленточными детерминированными машинами Тьюринга за время $T(n)$, то, как установлено в [4], при некотором естественном кодировании предикатных формул и для подходящих констант $c_1 > c_2 > 1$ множество всех выполнимых формул первого класса лежит в

$$DT\left(c_1^{n/\log n}\right) \setminus DT\left(c_2^{n/\log n}\right)\,^{*)}.$$

Формулы другого класса имеют в предваренной нормальной форме кванторный префикс вида $\exists \cdots \exists \forall \exists \cdots \exists \forall$ и удовлетворяют еще некоторым дополнительным условиям (см. определение класса $\mathfrak{B}$ ниже). Множество всех выполнимых формул этого класса при соответствующем выборе констант $c_1 > c_2 > 1$ лежит в

$$DT\left(c_1^{c_1^{n/\log n}}\right) \setminus DT\left(c_2^{c_2^{n/\log n}}\right).$$

В настоящей статье доказывается, что аналогичные результаты имеют место уже для собственных подклассов рассматриваемых классов. Именно, в первом случае достаточно ограничиться формулами с префиксом $\forall \exists \exists$, а во втором — формулами с префиксом $\forall \exists \exists \forall$.

Введем необходимые определения и обозначения. Через $\mathfrak{A}$ обозначим класс всех замкнутых формул узкого исчисления предикатов (без равенства), которые имеют в предваренной нормальной форме кванторный префикс вида $\forall \exists \exists$ и содержат лишь одноместные предикатные символы. Через $\mathfrak{B}$ обозначим класс всех замкнутых формул с префиксом $\forall x \exists y_1 \exists y_2 \forall z$, которые содержат лишь двуместные предикатные символы и не имеют атомарных формул вида $P(z, x)$, $P(z, y_1)$, $P(z, y_2)$.

*) Все логарифмы рассматриваются по основанию 2.

Через Sat — $\mathfrak{A}$(Sat — $\mathfrak{B}$) обозначим множество всех формул из $\mathfrak{A}(\mathfrak{B})$, выполнимых в непустой области. Ниже в теоремах 1, 2 предполагается, что задано некоторое «естественное» кодирование формул из классов $\mathfrak{A}$, $\mathfrak{B}$ словами в фиксированном (например, двоичном) алфавите. Не останавливаясь на деталях такого кодирования, отметим лишь, что предикатные формулы из классов $\mathfrak{A}$, $\mathfrak{B}$, содержащие n вхождений предикатных символов, будут иметь длину кодов порядка $n \log n$.

В основе доказательства теорем 1, 2 лежит подходящее кодирование вычислений на альтернирующих магазинных и стековых автоматах предикатными формулами рассматриваемого вида. Магазинный автомат (см., например, [1]) имеет входную ленту, с которой он может только считывать, магазинную ленту (или просто магазин) и конечное управляющее устройство. В начале вычисления на входную ленту записывается входное слово, ограниченное с обеих сторон специальным маркером *, который не принадлежит входному слову. Входная головка автомата устанавливается на левый символ *. В магазин записывается специальный символ Z — маркер дна. Автомат приводится в начальное состояние. В процессе работы над входным словом магазинный автомат может сдвигать входную головку в обе стороны, не выходя за пределы, ограниченные маркером *. Он может также записывать в магазин и удалять из магазина символы, отличные от Z. При этом символ, записанный в магазин последним, удаляется из него первым. Автомат не может удалить из магазина начальный символ Z. Автомат заканчивает вычисление, попадая в заключительное состояние.

Альтернирующий магазинный автомат (см. [2, 3]) отличается от приведенного наличием экзистенциальных и универсальных состояний. Находясь в экзистенциальном состоянии, альтернирующий автомат может (как и недетерминированный автомат) перейти в одно из непосредственно следующих состояний, даваемых функцией переходов автомата. При этом конфигурация автомата, содержащая экзистенциальное состояние, считается допускающей (т. е. в конечном итоге приводящей к заключительному состоянию), если допускающей является конфигурация, содержащая одно из непосредственно следующих состояний. Для универсального состояния в этом случае допускающими должны быть все конфигурации, содержащие непосредственно следующие состояния.

Пусть Σ — входной алфавит альтернирующего магазинного автомата M, $* \notin \Sigma$, Γ — магазинный алфавит, $Z \in \Gamma$, K — множество внутренних состояний, δ — функция переходов. Как и в работе [4], в технических целях удобно разбить множество K на семь попарно непересекающихся подмножеств $K_1, \ldots, K_7$. В соответствии с этим функция δ также разбивается на семь подфункций $\delta_1, \ldots, \delta_7$. В состояниях из K_1 автомат M будет только читать входную ленту. Поэтому

$$\delta_1\colon\ K_1 \times (\Sigma \cup \{*\}) \to K.$$

Без ограничения общности будем считать, что начальное состояние автомата M принадлежит множеству K_1.

В состояниях из K_2 автомат M осуществляет движение головки по входной ленте,

$$\delta_2\colon\ K_2 \to K \times \{-1, +1\}.$$

В состояниях из K_3 автомат M читает «верхний» символ магазина,

$$\delta_3\colon\ K_3 \times \Gamma \to K.$$

Для определенности предполагаем, что заключительное состояние автомата M принадлежит множеству K_3.

В состояниях из K_4 автомат M записывает новый символ в магазин,

$$\delta_4\colon K_4 \to K \times (\Gamma \setminus \{Z\}).$$

В состояниях из K_5 автомат M удаляет «верхний» символ из магазина,

$$\delta_5\colon K_5 \to K.$$

K_6 — это экзистенциальные, а K_7 — универсальные состояния автомата M,

$$\delta_6\colon K_6 \to 2^K \setminus \{\varnothing\}, \quad \delta_7\colon K_7 \to 2^K \setminus \{\varnothing\}.$$

Конфигурацией автомата M будем называть четверку (σ, i, p, γ), где σ — слово в алфавите Σ, $1 \leqslant i \leqslant |\sigma| + 2$, $p \in K$, γ — слово в алфавите Γ, имеющее ровно одно (самое левое) вхождение символа Z (здесь $|\sigma|$ означает длину слова σ). Конфигурация (σ, i, p, γ) отвечает случаю, когда автомат M, находясь в состоянии p, обозревает i-ю букву слова $*\sigma*$, записанного на входной ленте, а его магазин содержит слово γ. Определим далее понятие допускающей конфигурации. Пусть f — заключительное состояние автомата M. Тогда при любом i, $1 \leqslant i \leqslant |\sigma| + 2$, конфигурацию (σ, i, f, Z) будем считать *допускающей*. Таким образом, требуется, чтобы в заключительный момент вычисления магазин автомата M содержал лишь символ Z. Это требование, как нетрудно видеть, носит чисто технический характер. Далее, конфигурацию (σ, i, p, γ) считаем *допускающей*, если:

1) $p \in K_1$ и $(\sigma, i, \delta_1(p, a), \gamma)$ — допускающая конфигурация, где a — i-й символ слова $*\sigma*$;

2) $p \in K_2$ и $(\sigma, i+\varepsilon, q, \gamma)$ — допускающая конфигурация, где $\delta_2(p) = (q, \varepsilon)$;

3) $p \in K_3$ и $(\sigma, i, \delta_3(p, b), \gamma)$ — допускающая конфигурация, где $b \in \Gamma$ и $\gamma = \gamma' b$;

4) $p \in K_4$ и $(\sigma, i, q, \gamma b)$ — допускающая конфигурация, где $\delta_4(p) = (q, b)$;

5) $p \in K_5$ и $(\sigma, i, \delta_5(p), \gamma')$ — допускающая конфигурация, где $\gamma = \gamma' b$ и $b \in \Gamma \setminus \{Z\}$;

6) $p \in K_6$ и (σ, i, q, γ) — допускающая конфигурация для некоторого $q \in \delta_6(p)$;

7) $p \in K_7$ и (σ, i, q, γ) — допускающая конфигурация для всех $q \in \delta_7(p)$.

Пусть s — начальное состояние автомата M. Говорим, что *слово* σ *допускается автоматом* M (или автомат M применим к слову σ), если начальная конфигурация $(\sigma, 1, s, Z)$ допускающая. Множество слов A допускается автоматом M, если A состоит из тех и только тех слов, которые допускаются автоматом M.

Теорема 1. *Существуют такие константы* $c_1 > c_2 > 1$, *что*

$$\mathrm{Sat} - \mathfrak{A} \in DT\left(c_1^{n/\log n}\right) \setminus DT\left(c_2^{n/\log n}\right).$$

Доказательство. То, что для подходящей константы $c_1 > 1$ имеет место включение

$$\mathrm{Sat} - \mathfrak{A} \in DT\left(c_1^{n/\log n}\right),$$

доказано в работе [4, теорема 10.1] (на самом деле там доказан более общий результат для класса предикатных формул с префиксом вида $\exists \cdots \exists \forall \exists \cdots \exists$ и одноместными предикатными символами).

Для доказательства другого утверждения мы воспользуемся тем, что класс

$$DEXPT \rightleftharpoons \bigcup_{c>0} DT(c^n)$$

множеств, распознаваемых одноленточными детерминированными машинами Тьюринга за экспоненциальное время, совпадает с классом множеств, допускаемых альтернирующими магазинными автоматами (см. [2, 3]). Зафиксируем некоторую константу $c > 1$ и выберем в классе $DEXPT$ такое множество A, что $A \notin DT(c^n)$. Ясно, что классу $DEXPT \setminus DT(c^n)$ принадлежит также и дополнение $\bar{A}$ к множеству A. Пусть M — альтернирующий магазинный автомат, который допускает множество $\bar{A}$. Таким образом, если Σ — алфавит множества A, то для любого слова σ в алфавите Σ имеем: $\sigma \in A$ тогда и только тогда, когда автомат M неприменим к слову σ.

Пусть Γ — магазинный алфавит автомата M. Стандартными рассуждениями можно показать, что автомату M достаточно иметь в алфавите Γ помимо символа Z всего лишь два символа 0, 1. Сделаем еще один шаг в этом направлении. Именно, сократим магазинный алфавит до двух символов 0, 1. С этой целью закодируем символы Z, 0, 1 соответственно словами 0, 01, 11. Это кодирование является однозначным, поскольку оно суффиксное. Нетрудно видеть, что автомат M можно перестроить в эквивалентный автомат M', который оперирует на магазинной ленте вместо символов Z, 0, 1 их кодами 0, 01, 11. Естественно, что в начальный момент магазин автомата M' содержит символ 0. Кроме того, в любой момент вычисления автомата M' его магазин содержит двоичное слово вида $0va$, где v есть конкатенация слов 01, 11, $a \in \{0, 1\}$ (слово va может быть, разумеется, пустым). Наконец, будем считать, что автомат M' записывает в магазин и удаляет символы из магазина, так сказать, пáрами 01, 11. Это значит, что если в состоянии $p' \in K_4'$ автомат M' записывает в магазин первый символ пары и $\delta_4'(p') = (q', a)$, то также $q' \in K_4'$ и, следовательно, в состоянии q' происходит запись в магазин второго символа пары. Аналогичным образом, если в состоянии $p' \in K_5'$ автомат M' удаляет из магазина второй символ пары и $\delta_5'(p') = q'$, то $q' \in K_5'$ и, значит, в состоянии q' автомат M' удаляет из магазина первый символ пары. Далее будем считать, что автомат M с самого начала удовлетворяет всем перечисленным выше требованиям.

Укажем теперь, как по альтернирующему магазинному автомату M и входному слову σ длины n эффективно построить формулу $G_\sigma \in \mathfrak{A}$ длины порядка $n \log n$ такую, что автомат M неприменим к слову σ тогда и только тогда, когда формула G_σ выполнима в непустой области. Здесь слово эффективно подразумевает не только наличие алгоритма, но детерминированность этого алгоритма и возможность выполнения его на одноленточной машине Тьюринга за полиномиальное время (в связи с этим напомним, что формулы из $\mathfrak{A}$ кодируются словами фиксированного алфавита). Нетрудно видеть, что при выполнении сформулированных условий найдется такая константа $c_2 > 1$ (зависящая от c и константы, определяющей порядок длин формул G_σ), что $\mathrm{Sat} - \mathfrak{A} \notin DT\left(c_2^{n/\log n}\right)$ (впрочем, строгое обоснование этого перехода составляет содержание утверждения 2.1 из работы [4]).

Формула G_σ будет иметь вид $\forall x \exists y_1 \exists y_2 H_\sigma(x, y_1, y_2)$, где $H_\sigma(x, y_1, y_2)$ — бескванторная формула, содержащая только переменные x, y_1, y_2. В доказательстве удобно вместо формулы G_σ строить ее функциональную форму $H_\sigma(x, g_0(x), g_1(x))$, где g_0, g_1 — одноместные функциональные символы.

Каждому состоянию из K в формуле H_σ будет соответствовать $n + 2$ предикатных символов (по числу позиций входной головки на слове $*\sigma*$). Если f, p, q, r, s — состояния автомата M, то соответствующие предикатные символы будут обозначаться F_i, P_i, Q_i, R_i, S_i ($i = 1, \ldots, n + 2$). Формула $H_\sigma(x, g_0(x), g_1(x))$ является конъюнкцией формул, приводимых ниже в п. 1, 2, 3.1—3.7.

1. $\neg S_1(g_0(x))$.

2. $\underset{1\leqslant i\leqslant n+2}{\&} F_i(g_0(x))$.

3.1. $Q_i(x)\to P_i(x)$, где $p\in K_1$, $1\leqslant i\leqslant n+2$, a есть i-й символ слова $*\sigma*$ и $\delta_1(p, a)=q$.

3.2 $\underset{1\leqslant i+\varepsilon\leqslant n+2}{\&} (Q_{i+\varepsilon}(x)\to P_i(x))$, где $p\in K_2$ и $\delta_2(p)=(q, \varepsilon)$.

3.3. $\underset{1\leqslant i\leqslant n+2}{\&} (Q_i(g_a(x))\to P_i(g_a(x)))$, где $p\in K_3$ и $\delta_3(p, a)=q$.

3.4. $\underset{1\leqslant i\leqslant n+2}{\&} (Q_i(g_a(x))\to P_i(x))$, где $p\in K_4$ и $\delta_4(p)=(q, a)$.

3.5. $\underset{1\leqslant i\leqslant n+2}{\&} (Q_i(x)\to P_i(g_0(x)))\,\&\,(Q_i(x)\to P_i(g_1(x)))$, где $p\in K_5$ и $\delta_5(p)=q$, причем импликация $Q_i(x)\to P_i(g_0(x))$ имеется только для тех состояний p, в которых автомат M удаляет из магазина первый символ пары.

3.6. $\underset{1\leqslant i\leqslant n+2}{\&} ((Q_i(x)\vee\ldots\vee R_i(x))\to P_i(x))$, где $p\in K_6$ и $\delta_6(p)=\{q, \ldots, r\}$.

3.7. $\underset{1\leqslant i\leqslant n+2}{\&} (Q_i(x)\,\&\ldots\&\,R_i(x)\to P_i(x))$, где $p\in K_7$ и $\delta_7(p)=\{q, \ldots, r\}$.

Нетрудно видеть, что формула H_σ содержит не более dn предикатных символов, где константа d зависит только от автомата M. Поэтому длина кода формулы G_σ по порядку не превосходит $n\log n$. Ясно также, что выполняются условия на эффективность перехода от автомата M и слова σ к формуле G_σ.

При решении вопроса о выполнимости формулы $H_\sigma(x, g_0(x), g_1(x))$ достаточно, как известно, в качестве стандартной непустой области рассмотреть эрбрановский универсум U, который в данном случае состоит из всех термов вида $g_{j_k}(\ldots g_{j_1}(e)\ldots)$, где $j_k, \ldots, j_1\in\{0, 1\}$, $k\geqslant 0$ и e — символ константы. Терму $g_{j_k}(\ldots g_{j_1}(e)\ldots)$ мы сопоставим двоичное слово $0j_1\ldots j_k$, которое можно рассматривать как содержимое магазина автомата M (j_k — «верхний» символ магазина).

Предположим сначала, что автомат M неприменим к слову σ, и докажем, что в этом случае формула $H_\sigma(x, g_0(x), g_1(x))$ выполнима в универсуме U. С этой целью для всякого предикатного символа P_i, входящего в формулу H_σ, и любого терма $t\in U$ определим истинностное значение $P_i(t)$. Пусть $t=g_{j_k}(\ldots g_{j_1}(e)\ldots)$, а состояние p автомата M принадлежит либо множеству K_l, $l\neq 4$, 5, либо множеству K_4, причем в состоянии p автомат M тогда записывает в магазин первый символ пары, либо множеству K_5, причем в состоянии p автомат M удаляет тогда из магазина второй символ пары. Положим $v=0j_1, \ldots, j_k$ и найдем (если существуют) такие двоичные слова v_1, v_2 (возможно, пустые), что $v=v_1 0 v_2$ и слово v_2 представимо в виде конкатенации слов 01, 11. Для любого i, $1\leqslant i\leqslant n+2$, полагаем $P_i(t)$ истинным тогда и только тогда, когда конфигурация $(\sigma, i, p, 0v_2)$ — допускающая для автомата M.

Пусть $p\in K_4$ и в состоянии p автомат M записывает в магазин второй символ пары, либо $p\in K_5$ и в состоянии p автомат M удаляет из магазина первый символ пары. Тогда находим такие слова v_1, v_2, что $v=v_1 0 v_2 j_k$ и слово v_2 есть конкатенация слов 01, 11. Для любого i, $1\leqslant i\leqslant n+2$, полагаем $P_i(t)$ истинным в том и только том случае, если конфигурация $(\sigma, i, p, 0v_2j_k)$ — допускающая для автомата M. Во всех остальных случаях полагаем $P_i(t)$ истинным.

Докажем, что при выбранном распределении истинностных значений формула $H_\sigma(t, g_0(t), g_1(t))$ оказывается истинной для любого терма $t\in U$. Рассмотрим последовательно п. 1, 2, 3.1—3.7 определения формулы H_σ. Вновь предположим, что $t=g_{j_k}(\ldots g_{j_1}(e)\ldots)$ и $v=0j_1\ldots j_k$. Так как начальное состояние s принадлежит множеству K_1, то для двоичного слова $v0$, соответствующего терму $g_0(t)$, слово v_1, согласно определению, совпадает с v, а слово v_2 пусто. Далее, поскольку автомат M неприменим к слову σ, начальная конфигурация $(\sigma, 1, s, 0)$ недопускающая. Значит, $S_1(g_0(t))$ ложно, а $\neg S_1(g_0(t))$ истинно.

По предположению, $f \in K_3$. Поэтому в тех же обозначениях, что и выше, при определении значений $F_i(g_0(t))$ слово v_2 также оказывается пустым. А так как при любом i $(1 \leqslant i \leqslant n+2)$ конфигурация $(\sigma, i, f, 0)$ допускающая, то $F_i(g_0(t))$ истинно.

Переходя к п. 3.1, заметим, что при истинности $P_i(t)$ истинна и импликация $Q_i(t) \to P_i(t)$. Поэтому достаточно рассмотреть лишь случай, когда двоичное слово v представимо в виде $v_1 0 v_2$, где v_2 есть конкатенация слов 01, 11, а конфигурация $(\sigma, i, p, 0v_2)$ недопускающая (в этом случае $P_i(t)$ ложно). Но тогда непосредственно следующая конфигурация $(\sigma, i, g, 0v_2)$ — также недопускающая. Ясно, что в рассматриваемом случае если $q \in K_4$, то автомат M записывает в магазин первый символ пары, а если $q \in K_5$ — то удаляет из магазина второй символ пары. По определению получаем тогда, что $Q_i(t)$ также ложно, а импликация $(Q_i(t) \to P_i(t))$ истинна.

Аналогично рассматриваются п. 3.2, 3.3, 3.6, 3.7. В п. 3.4, как и выше, рассматриваем лишь случай, когда значение $P_i(t)$ ложно. Если в состоянии p в магазин записывается первый символ пары, то слово v необходимо представить в виде $v_1 0 v_2$, где v_2 есть конкатенация слов 01, 11. По предположению, конфигурация $(\sigma, i, p, 0v_2)$ недопускающая. Значит, непосредственно следующая конфигурация $(\sigma, i, p, 0v_2 a)$ — также недопускающая. Поскольку $q \in K_4$ и в состоянии q в магазин записывается второй символ пары, при определении значения $Q_i(g_a(t))$ двоичное слово va будет представлено в виде $v_1 0 v_2 a$. Но тогда, очевидно, мы должны определить значение $Q_i(g_a(t))$ ложным. Симметричным образом разбирается случай, когда в состоянии p в магазин записывается второй символ пары. Наконец, п. 3.5 рассматривается так же, как и п. 3.4. При этом ограничения, содержащиеся в п. 3.5, позволяют для терма $g_0(t)$ представить слово $v0$ в виде $v_1 0 v_2 0$, где v_2 есть конкатенация слов 01, 11.

Таким образом, если автомат M неприменим к слову σ, то формула $H_\sigma(x, g_0(x), g_1(x))$ выполнима в универсуме U и, следовательно, формула G_σ выполнима в непустой области.

Предположим теперь, что формула $H_\sigma(x, g_0(x), g_1(x))$ выполнима в универсуме U, и докажем, что автомат M неприменим к слову σ. Зафиксируем такие значения входящих в формулу H_σ предикатов, которые выполняют формулу H_σ. Индукцией по определению допускающей конфигурации докажем следующее утверждение.

Пусть (σ, i, p, γ) — допускающая конфигурация для автомата M. Тогда если $t \in U$, $t = g_{j_k}(\ldots g_{j_1}(e)\ldots)$ и $\gamma = j_1 \ldots j_k$, то $P_i(t)$ истинно.

Начало индукции очевидным образом обеспечивает п. 2 определения формулы H_σ (в качестве терма t здесь следует взять e). Далее, семи пунктам определения допускающей конфигурации отвечают п. 3.1—3.7 определения формулы H_σ. Все они рассматриваются по одной схеме. Рассмотрим, например, п. 5) определения допускающей конфигурации. Согласно этому пункту, конфигурация (σ, i, p, γ) оказывается допускающей потому, что допускающей является непосредственно следующая конфигурация (σ, i, q, γ'), где $q = \delta_5(p)$, $\gamma = \gamma' b$, $b \in \{0, 1\}$ (условию $b \neq Z$ из п. 5) отвечает условие на существование импликации $Q_i(x) \to P_i(g_0(x))$ в п. 3.5). Пусть $t = g_{j_k}(\ldots g_{j_1}(e)\ldots)$ и $\gamma = j_1 \ldots j_k b$. Тогда $\gamma' = j_1 \ldots j_k$ и, в силу индуктивного предположения, $Q_i(t)$ истинно. Из п. 3.5 получаем, что $P_i(g_b(t))$ также истинно (если в состоянии p из магазина удаляется второй символ пары, то получаем истинность лишь $P_i(g_1(t))$).

Остается теперь заметить, что в силу п. 1 определения формулы H_σ начальная конфигурация $(\sigma, 1, s, 0)$ не может быть допускающей, т. е. автомат M неприменим к слову σ. Теорема доказана.

Стековый автомат отличается от магазинного автомата наличием дополнительной стековой головки, которая может заходить внутрь магазина с целью его прочтения. В этом случае магазин автомата называют стеком. Мы считаем также, что запись символов в стек и удаление символов из стека проводится с помощью стековой головки. Альтернирующий стековый автомат определяется аналогично альтернирующему магазинному автомату. Мы предполагаем, что множество K внутренних состояний альтернирующего стекового автомата M разбито на девять непересекающихся подмножеств $K_1, \ldots, K_9$. Первые семь имеют тот же смысл, что и для магазинного автомата. Только в состояниях из K_3 автомат M читает символ стека, на котором в данный момент располагается стековая головка. В состояниях из K_8 стековая головка автомата M сдвигается внутри стека на одну клетку влево, а в состояниях из K_9 — вправо,

$$\delta_8\colon K_8 \to K, \quad \delta_9\colon K_9 \to K.$$

Предполагаем, что начальное состояние автомата M принадлежит множеству K_1, а заключительное — множеству K_3.

Конфигурацией альтернирующего стекового автомата M называется пятерка $(\sigma, i, p, \gamma, j)$, где σ, i, p, γ — такие же, как и для альтернирующего магазинного автомата, а $1 \leqslant j \leqslant |\gamma|$. Конфигурация $(\sigma, i, p, \gamma, j)$ называется *допускающей*, если либо $p = f$, $\gamma = Z$ и $j = 1$, где f — заключительное состояние автомата M, либо:

1) $p \in K_1$ и $(\sigma, i, \delta_1(p, a), \gamma, j)$ — допускающая конфигурация, где a есть i-й символ слова $*\sigma*$,

2) $p \in K_2$ и $(\sigma, i+\varepsilon, q, \gamma, j)$ — допускающая конфигурация, где $\delta_2(p) = (q, \varepsilon)$,

3) $p \in K_3$ и $(\sigma, i, \delta_3(p, b), \gamma, j)$ — допускающая конфигурация, где b есть j-й символ слова γ,

4) $p \in K_4$, $j = |\gamma|$ и $(\sigma, i, q, \gamma b, j+1)$ — допускающая конфигурация, где $\delta_4(p) = (q, b)$,

5) $p \in K_5$, $j = |\gamma|$ и $(\sigma, i, \delta_5(p), \gamma', j-1)$ — допускающая конфигурация, где $\gamma = \gamma' b$ и $b \in \Gamma \setminus \{Z\}$,

6) $p \in K_6$ и $(\sigma, i, q, \gamma, j)$ — допускающая конфигурация для некоторого $q \in \delta_6(p)$,

7) $p \in K_7$ и $(\sigma, i, q, \gamma, j)$ — допускающая конфигурация для любого $q \in \delta_7(p)$,

8) $p \in K_8$ и $(\sigma, i, \delta_8(p), \gamma, j-1)$ — допускающая конфигурация,

9) $p \in K_9$ и $(\sigma, i, \delta_9(p), \gamma, j+1)$ — допускающая конфигурация.

Будем говорить, что *автомат M применим к слову* σ (или слово σ допускается автоматом M), если начальная конфигурация $(\sigma, 1, s, Z, 1)$ допускающая.

Как и для магазинного автомата, будем далее предполагать, что стековый алфавит Γ состоит только из символов 0, 1. В связи с этим запись в стек и удаление символов из него происходит парами 01, 11, как это описано выше для магазинного автомата.

Теорема 2. *Существуют такие константы $c_1 > c_2 > 1$, что*

$$\mathrm{Sat} - \mathfrak{B} \in DT\left(c_1^{c_1^{n/\log n}}\right) \setminus DT\left(c_2^{c_2^{n/\log n}}\right).$$

Доказательство. Согласно теореме 12.1 из работы [4], существует такая константа $c_1 > 1$, что

$$\mathrm{Sat} - \mathfrak{B} \in DT\left(c_1^{c_1^{n/\log n}}\right).$$

С другой стороны, известно (см. [3, 4]), что класс

$$D2EXPT = \bigcup_{c>0} DT\left(c^{c^n}\right)$$

совпадает с классом множеств, допустимых альтернирующими стековыми автоматами. Зафиксируем некоторую константу $c > 1$ и выберем в классе $D2EXPT$ такое множество A, что $A \notin DT\left(c^{c^n}\right)$. Тогда, конечно, и

$$\overline{A} \in D2EXPT \setminus DT\left(c^{c^n}\right).$$

Пусть M — альтернирующий стековый автомат, который допускает множество $\overline{A}$. Таким образом, если Σ — алфавит множества A, то для любого слова σ в алфавите Σ имеем $\sigma \in A$ тогда и только тогда, когда автомат M неприменим к слову σ.

Как и в теореме 1, укажем алгоритм (выполнимый на детерминированной машине Тьюринга за полиномиальное время), который по произвольному слову σ длины n строит формулу $G_\sigma \in \mathfrak{B}$ длины порядка $n \log n$ такую, что формула G_σ выполнима в непустой области тогда и только тогда, когда автомат M неприменим к слову σ. Несложные рассуждения показывают (см. утверждение 2.1 из работы [4]), что в этом случае существует такая константа $c_2 > 1$ (зависящая от c и константы, определяющей порядок длин формул G_σ), что

$$\mathrm{Sat} - \mathfrak{B} \notin DT\left(c_2^{c_2^{n/\log n}}\right).$$

Формула G_σ будет иметь вид $\forall x \exists y_1 \exists y_2 \forall z H_\sigma(x, y_1, y_2, z)$, где H_σ — бескванторная формула, содержащая только двуместные предикатные символы. Как и в доказательстве теоремы 1, каждому состоянию $p \in K$ будет соответствовать $n+2$ предикатных символов P_i. Кроме того, в формулу H_σ входит двуместный предикатный символ Π. С содержательной точки зрения истинность $\Pi(t_1, t_2)$ означает, что двоичное слово, отвечающее терму t_1, является префиксом двоичного слова, отвечающего терму t_2. В остальном определение формулы H_σ базируется примерно на тех же идеях, что и определение формулы H_σ в теореме 1. Функциональная форма $H_\sigma(x, g_0(x), g_1(x), z)$ формулы G_σ является конъюнкцией формул, приводимых ниже в п. 1, 2, 3, 4.1—4.9.

1. $\Pi(x, x) \& (\Pi(g_0(x), z) \to \Pi(x, z)) \& (\Pi(g_1(x), z) \to \Pi(x, z))$.
2. $\neg S_1(g_0(x), g_0(x))$.
3. $\underset{1 \leqslant i \leqslant n+2}{\&} F_i(g_0(x), g_0(x))$.

4.1. $Q_i(x, z) \to P_i(x, z)$, если $p \in K_1$, $1 \leqslant i \leqslant n+2$, a есть i-й символ слова $*\sigma*$ и $\delta_1(p, a) = q$.

4.2. $\underset{1 \leqslant i+\varepsilon \leqslant n+2}{\&} (Q_{i+\varepsilon}(x, z) \to P_i(x, z))$, если $p \in K_2$ и $\delta_2(p) = (q, \varepsilon)$.

4.3. $\underset{1 \leqslant i \leqslant n+2}{\&} (Q_i(g_a(x), z) \to P_i(g_a(x), z))$, если $p \in K_3$ и $\delta_3(p, a) = q$.

4.4. $\underset{1 \leqslant i \leqslant n+2}{\&} (Q_i(g_a(x), g_a(x)) \to P_i(x, x))$, если $p \in K_4$ и $\delta_4(p) = (q, a)$.

4.5. $\underset{1 \leqslant i \leqslant n+2}{\&} (Q_i(x, x) \to P_i(g_0(x), g_0(x))) \& (Q_i(x, x) \to P_i(g_1(x), g_1(x)))$, если $p \in K_5$ и $\delta_5(p) = q$. При этом первая импликация присутствует в формуле только для тех состояний p, в которых автомат M удаляет из стека первый символ пары.

4.6. $\underset{1 \leqslant i \leqslant n+2}{\&} ((Q_i(x, z) \vee \ldots \vee R_i(x, z)) \to P_i(x, z))$, если $p \in K_6$ и $\delta_6(p) = \{q, \ldots, r\}$.

4.7. $\underset{1 \leqslant i \leqslant n+2}{\&} (Q_i(x, z) \& \ldots \& R_i(x, z) \to P^i(x, z))$, если $p \in K_7$ и $\delta_7(p) = \{q, \ldots, r\}$.

4.8. $\mathop{\&}\limits_{\substack{1\leqslant i\leqslant n+2\\ a\in\{0,1\}}} (Q_i(x, z) \& \Pi(g_a(x), z) \to P_i(g_a(x), z))$, если $p \in K_8$ и $\delta_8(p) = q$.

4.9. $\mathop{\&}\limits_{\substack{1\leqslant i\leqslant n+2\\ a\in\{0,1\}}} (Q_i(g_a(x), z) \to P_i(x, z))$, если $p \in K_9$ и $\delta_9(p) = q$.

Нетрудно видеть, что для подходящей константы d (зависящей только от автомата M) число предикатных символов, входящих в формулу H_σ, ограничено сверху величиной dn, т. е. длина кода формулы G_σ имеет порядок $n \log n$. Выполнено также требование на эффективность перехода от слова σ к формуле G_σ. Отметим, наконец, что формула G_σ не содержит атомарных формул вида $P(z, x)$, $P(z, y_1)$, $P(z, y_2)$.

Как и в теореме 1, в качестве стандартной непустой области рассмотрим эрбрановский универсум U, который в данном случае вновь состоит из термов вида $g_{j_k}(\ldots g_{j_1}(e)\ldots)$, где e — символ константы. Терму $g_{j_k}(\ldots g_{j_1}(e)\ldots)$ сопоставим двоичное слово $v = 0j_1 \ldots j_k$, которое будет нести информацию о содержимом стека автомата M.

Предположим, что автомат M неприменим к слову σ, и докажем, что формула G_σ выполнима в универсуме U. Для любых термов $t_1, t_2 \in U$ и любого предикатного символа P из H_σ определим истинностное значение $P(t_1, t_2)$. Пусть двоичные слова u, v соответствуют термам t_1, t_2. Определяем значение $\Pi(t_1, t_2)$ истинным тогда и только тогда, когда слово u есть префикс слова v. Предположим далее, что либо $p \in K_l$, где $l \notin \{4, 5\}$, либо $p \in K_4$ и в состоянии p в стек записывается первый символ пары, либо $p \in K_5$ и в состоянии p из стека удаляется второй символ пары. Если $v = v_1 0 v_2$, $u = v_1 0 u_2$, v_2 есть конкатенация слов 01, 11 и u_2 является префиксом v_2, то для любого i, $1 \leqslant i \leqslant n+2$, полагаем $P_i(t_1, t_2)$ истинным тогда и только тогда, когда конфигурация $(\sigma, i, p, 0v_2, |0u_2|)$ допускающая для автомата M. Если состояние p не удовлетворяет сформулированным выше условиям, то слово v представляем в виде $v = v_1 0 v_2 a$, где v_2 есть конкатенация слов 01, 11 и $a \in \{0, 1\}$. Если теперь $u = v_1 0 u_2$ и u_2 — префикс слова $v_2 a$, то вновь полагаем $P_i(t_1, t_2)$ истинным в том и только том случае, когда конфигурация $(\sigma, i, p, 0v_2 a, |0u_2|)$ допускающая. Во всех остальных случаях полагаем значение $P_i(t_1, t_2)$ истинным.

То, что указанный выбор предикатов выполняет в U формулу H_σ, устанавливаем так же, как и соответствующее утверждение в теореме 1. В качестве примера рассмотрим п. 4.8 определения формулы H_σ. Возьмем произвольные термы t_1, $t_2 \in U$ и предположим, что значение $P_i(g_a(t_1), t_2)$ ложно. Согласно определению, если двоичные слова u, v отвечают термам t_1, t_2, то в данном случае слово v представимо в виде $v_1 0 v_2$, где v_2 есть конкатенация слов 01, 11, $ua = v_1 0 u_2 a$, $u_2 a$ является префиксом v_2 и конфигурация $(\sigma, i, p, 0v_2, |0u_2 a|)$ не допускающая для автомата M. Так как $\delta_8(p) = q$ и $|0u_2 a| \geqslant 2$, то непосредственно следующая конфигурация $(\sigma, i, q, 0v_2, |0u_2|)$ также не допускающая. Ясно, что $q \notin K_4 \cup K_5$, ибо запись в стек и удаление из стека происходят с помощью стековой головки, которая в конфигурации $(\sigma, i, q, 0v_2, |0u_2|)$ не может находиться на правом конце стека. Поэтому в соответствии с определением истинностных значений мы должны положить $Q_i(t_1, t_2)$ также ложным. Тем самым импликация п. 4.8 становится истинной.

Пусть теперь формула $H_\sigma(x, g_0(x), g_1(x), z)$ выполнима в универсуме U. Докажем, что тогда автомат M неприменим к слову σ. Зафиксируем такие значения входящих в формулу H_σ предикатов, которые выполняют эту формулу в универсуме U. Индукцией по определению допускающей конфигурации докажем следующее утверждение.

Пусть $(\sigma, i, p, \gamma, j)$ — допускающая конфигурация для автомата M. Тогда для любых термов t_1, $t_2 \in U$, если двоичные слова u, v соответствуют термам t_1, t_2, $v = 0\gamma$, u — префикс v и $|u| = j + 1$, то $P_i(t_1, t_2)$ истинно.

Для доказательства заметим прежде всего, что если слово u, соответствующее терму t_1, является (непустым) префиксом слова v, соответствующего терму t_2, то в силу п. 1) значение $\Pi(t_1, t_2)$ истинно. Начало индукции теперь обеспечивает п. 3) определения формулы H_σ, где в качестве x следует взять терм e. Дальнейшим п. 1) — 9) определения допускающей конфигурации отвечают п. 4.1—4.9 определения формулы H_σ (при этом в п. 4.8 используется сформулированное выше свойство предиката Π). Рассмотрим, например, п. 5) определения допускающей конфигурации. Согласно этому пункту, конфигурация $(\sigma, i, p, \gamma, j)$ оказалась допускающей для автомата M потому, что допускающей является непосредственно следующая конфигурация $(\sigma, i, q, \gamma', j-1)$, где $q = \delta_5(p)$, $j = |\gamma|$, $\gamma = \gamma' b$ и $b \in \{0, 1\}$. Для определенности будем считать, что в состоянии p автомат M удаляет из стека первый символ пары. Это означает, что в п. 4.5 присутствуют обе импликации. Пусть термы t_1, t_2 таковы, что слова u, v, отвечающие этим термам, удовлетворяют условиям $v = 0\gamma$ и $u = v$ (ибо если u — префикс v и $|u| = j + 1 = |\gamma| + 1$, то, разумеется, $u = v$). По индуктивному предположению, если термы t_1', t_2' отвечают двоичным словам $u' = v' = 0\gamma'$, то $Q_i(t_1', t_2')$ истинно. Значит, одна из импликаций п. 4.5 дает истинность $P_i(t_1, t_2)$.

Вместе с тем очевидно, что в силу п. 2 начальная конфигурация $(\sigma, 1, s, 0, 1)$ не может быть допускающей, т. е. автомат M неприменим к слову σ. Теорема доказана.

СПИСОК ЛИТЕРАТУРЫ

1. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов.— М.: Мир, 1979.
2. Chandra A. K., Kozen D. C., Stockmeyer L. J. Alternation // J. Assoc. Comput. Mach.— 1981.— 28, № 1.— P. 114—133.
3. Ladner R. E., Lipton R. J., Stockmeyer L. J. Alternating pushdown automata // Proc. 19th IEEE Symp. Found. Comput. Sci., Ann Arbor, Mich.— 1978.— P. 92—106.
4. Lewis H. R. Complexity results for classes of quantificational formulas // J. Comput. System. Sci.— 1980.— 21.— P. 317—353.