О разрешимости выводимости замкнутых термов и выразимости операций над ними

Г. В. Боков

В работе исследуются алгебры замкнутых термов, операции которых задаются формулами первого порядка с единственным предикатом равенства. Для таких алгебр показано, что в общем случае проблема выводимости термов алгоритмически неразрешима. При рассмотрении частных случаев проблемы выводимости строится соответствие Галуа между операциями и конечными автоматами над термами. На его основе доказаны достаточные условия алгоритмической разрешимости частных случаев проблемы выводимости термов и проблемы выразимости операций над термами.

Ключевые слова: алгебры термов, проблема выводимости, проблема выразимости, автоматы над термами, соответствие Галуа.

1. Основные понятия и результаты

Пусть $\mathcal{F} := \left\{f_1^{(n_1)}, \ldots, f_k^{(n_k)}\right\}$ — конечное множество функциональных символов, в котором $f_i^{(n_i)}$ — это функциональный символ f_i арности n_i. Будем предполагать, что имеется счётный универсум переменных $\mathcal{U} = \{u_1, u_2, \ldots\}$. Определим понятие терма над множеством функциональных символов $\mathcal{F}$ и множеством переменных $X \subseteq \mathcal{U}$:

1) Если $x \in X$, то x — терм;
2) Если $f^{(n)} \in \mathcal{F}$ и $t_1, \ldots, t_n$ — термы, то $f(t_1, \ldots, t_n)$ — терм.

Обозначим через $T_{\mathcal{F}}(X)$ множество всех термов над множеством функциональных символов $\mathcal{F}$ и множеством переменных X. Если

$X = \varnothing$, то будем писать $T_{\mathcal{F}}$ вместо $T_{\mathcal{F}}(X)$. Чтобы множество $T_{\mathcal{F}}$ было непустым, далее будем предполагать, что $\mathcal{F}$ всегда содержит хотя бы один функциональный символ арности 0. Элементы множества $T_{\mathcal{F}}$ будем называть замкнутыми термами.

Для того, чтобы определить операции над термами, воспользуемся теорией первого порядка, в которой функциональными символами являются символы из множества $\mathcal{F}$, предикатным символом выступает предикат $=$, а логическими символами и кванторами являются символы из множества $S := \{\exists, \wedge, \neg\}$.

Пусть S' — множество логических символов из S. Обозначим через $\Phi(S')$ множество всех формул первого порядка, которые (помимо переменных, функциональных символов, предиката $=$ и скобок) содержат только логические символы и кванторы из S'. Если $S' = \varnothing$, то $\Phi(S')$ состоит только из формул вида $t = s$, где $t, s \in T_{\mathcal{F}}(\mathcal{U})$; если $S' = \{\exists, \wedge\}$, то $\Phi(S')$ — *примитивно позитивные* формулы [10]. Положим $\Phi^{(n)}(S')$ — формулы из $\Phi(S')$ с n свободными переменными, $\Phi_{\Pi} := \Phi(\{\exists, \wedge\})$ и $\Phi := \Phi(\{\exists, \wedge, \neg\})$.

Каждая формула $\mathfrak{A} \in \Phi^{(n)}$ задаёт n-местный предикат $\rho_{\mathfrak{A}}$ на множестве $T_{\mathcal{F}}$:

$$\rho_{\mathfrak{A}}(t_1, \ldots, t_n) = 1 \leftrightharpoons T_{\mathcal{F}} \models \mathfrak{A}(t_1, \ldots, t_n)$$

для любых $t_1, \ldots, t_n \in T_{\mathcal{F}}$, где $T_{\mathcal{F}} \models \mathfrak{A}(t_1, \ldots, t_n)$ означает истинность формулы $\mathfrak{A}$ на наборе термов $t_1, \ldots, t_n$ в множестве термов $T_{\mathcal{F}}$, то есть все замкнутые переменные пробегают элементы множества $T_{\mathcal{F}}$. Формулу $\mathfrak{A} \in \Phi^{(n+1)}$ будем называть допустимой, если $\rho_{\mathfrak{A}}(x_1, \ldots, x_n, y)$ является графиком [8] некоторой операции на $T_{\mathcal{F}}$, то есть соответствие $\omega_{\mathfrak{A}}$, заданное соотношением

$$\omega_{\mathfrak{A}}(t_1, \ldots, t_n) = t \leftrightharpoons \rho_{\mathfrak{A}}(t_1, \ldots, t_n, t) = 1$$

для любых $t_1, \ldots, t_n, t \in T_{\mathcal{F}}$, является n-местной операцией на множестве $T_{\mathcal{F}}$. Обозначим множество всех таких n-местной операций на множестве $T_{\mathcal{F}}$ через

$$O_{\mathcal{F}}^{(n)} := \{\omega_{\mathfrak{A}} \mid \mathfrak{A} \in \Phi^{(n+1)},\ \mathfrak{A} \text{ — допустима}\},$$
$$O_{\mathcal{F},\Pi}^{(n)} := \{\omega_{\mathfrak{A}} \mid \mathfrak{A} \in \Phi_{\Pi}^{(n+1)},\ \mathfrak{A} \text{ — допустима}\}.$$

Положим $O_{\mathcal{F}} := \cup_{n\geqslant 0} O_{\mathcal{F}}^{(n)}$ — множество всех операций на $T_{\mathcal{F}}$, $O_{\mathcal{F},\Pi} := \cup_{n\geqslant 0} O_{\mathcal{F},\Pi}^{(n)}$ — множество *примитивно позитивных* операций на $T_{\mathcal{F}}$.

Аргумент x_i операции $\omega(x_1,\ldots,x_n)$ будем называть существенным, если найдутся такие термы $t_1,\ldots,t_{i-1},t,s,t_{i+1},\ldots,t_n$, что значения $\omega(t_1,\ldots,t_{i-1},t,t_{i+1},\ldots,t_n)$ и $\omega(t_1,\ldots,t_{i-1},s,t_{i+1},\ldots,t_n)$ либо определены и не совпадают, либо одно значение определено, а другое не определено. Далее будем рассматривать операции с точностью до добавления и изъятия несущественных переменных. Когда не оговорено противное, будем предполагать, что операции из $O_{\mathcal{F}}$ не имеют несущественных переменных.

Пару $\langle T_{\mathcal{F}}(\mathcal{U});\Omega\rangle$, где $\Omega\subseteq O_{\mathcal{F}}$, будем называть алгеброй термов с универсумом $T_{\mathcal{F}}(\mathcal{U})$ и множеством операций Ω. Примерами таких алгебр являются:

1) Алгебра $\mathcal{F}$-слов [3] с универсумом $T_{\mathcal{F}}$ и множеством операций $\mathcal{F}$. Каждая операция $f\colon(t_1,\ldots,t_n)\mapsto f(t_1,\ldots,t_n),\ f\in\mathcal{F}^{(n)}$, задается формулой $y=f(x_1,\ldots,x_n)$.
2) Функции k-значной логики [9], для которых функциональными символами $\mathcal{F}$ являются константные символы из $E_k=\{0,1,\ldots,k-1\}$ и операциями $O_{\mathcal{F}}$ выступают функции k-значной логики P_k. Каждая функция $f\in P_k^n$ задается формулой
$$\bigwedge_{(\sigma_1,\ldots,\sigma_n)\in E_k^n}\Big(\big((x_1=\sigma_1)\wedge\ldots\wedge(x_n=\sigma_n)\big)\to\big(y=f(\sigma_1,\ldots,\sigma_n)\big)\Big),$$
в которой логическая связка $\to$ задаёт импликацию и выражается через $\wedge$ и $\neg$.
3) Классическое исчисление высказываний [7] с операцией *modus ponens*, для которого множество тавтологий Th является подмножеством $T_{\{\wedge,\vee,\neg,\to\}}(\mathcal{U})$ и операция *modus ponens* задается формулой $(x_1\to y)=x_2$.
4) Пропозициональные исчисления [12, 2], для которых множество тавтологий Th является подмножеством $T_{\mathcal{F}}(\mathcal{U})$, где $\mathcal{F}\subseteq P_2$, и $O_{\mathcal{F}}$ — это схемные операции вида
$$\frac{t_1,\ldots,t_m}{t_0},$$
где $t_i\in T_{\mathcal{F}}(\{z_1,\ldots,z_n\}),\ i=0,1,\ldots,m$. Каждая такая операция задается формулой
$$\exists z_1,\ldots,z_n\big((x_1=t_1)\wedge\ldots\wedge(x_n=t_n)\wedge(y=t_0)\big).$$

В данной работе будут рассмотрены не произвольные алгебры термов $\langle T_{\mathcal{F}}(\mathcal{U}); \Omega\rangle$, а лишь алгебры вида $\langle T_{\mathcal{F}}; \Omega\rangle$, которые будем называть алгебрами замкнутых термов.

Пусть $L \subseteq T_{\mathcal{F}}$ некоторое множество термов, тогда будем говорить, что терм $t \in T_{\mathcal{F}}$ выводим из термов множества L с помощью операций Ω, если t можно за конечное число шагов получить из L с помощью операций Ω. Выводимость терма t из множества термов L с помощью операций Ω будем обозначать через $L \vdash_{\Omega} t$. Множество всех выводимых из L термов обозначим через

$$[L]_{\Omega} := \{t \in T_{\mathcal{F}} \mid L \vdash_{\Omega} t\}.$$

Нетрудно заметить, что $[L]_{\Omega}$ является алгебраическим оператором замыкания на множестве термов $T_{\mathcal{F}}$. По аналогии, для произвольного $L' \subseteq T_{\mathcal{F}}$ будем говорить, что L' выводимо из L с помощью операций Ω, и писать $L \vdash_{\Omega} L'$, если $L' \subseteq [L]_{\Omega}$.

Определим массовую проблему ВЫВОДИМОСТЬ:
Дано: $\Omega \subseteq O_{\mathcal{F}},\ |\Omega| < \infty,\ L \subseteq T_{\mathcal{F}},\ |L| < \infty,\ t \in T_{\mathcal{F}}$;
Вопрос: $L \vdash_{\Omega} t$?

Теорема 1. *Если $\mathcal{F}$ содержит функциональные символы арности 0 и 2, то найдутся такие конечные множества $\Omega \subseteq O^{(1)}_{\mathcal{F},\Pi}$ и $L \subseteq T_{\mathcal{F}}$, что множество $[L]_{\Omega}$ является неразрешимым.*

Как следствие из теоремы 1 получаем, что в такой общей формулировке проблема ВЫВОДИМОСТЬ алгоритмически неразрешима.

Следствие 1. *Проблема ВЫВОДИМОСТЬ алгоритмически неразрешима.*

Следует отметить, что алгоритмическая неразрешимость проблемы ВЫВОДИМОСТЬ для алгебр термов со свободными переменными следует из неразрешимости классического исчисления высказываний [13, 6, 1]. Теорема 1 показывает, что это верно и для класса алгебр замкнутых термов. В данной работе будут рассмотрены два частных случая этой проблемы.

Для конечного множества операций $\Omega \subseteq O_{\mathcal{F}}$ определим массовую проблему ВЫВОДИМОСТЬ(Ω):
Дано: $L \subseteq T_{\mathcal{F}},\ |L| < \infty,\ t \in T_{\mathcal{F}}$;
Вопрос: $L \vdash_{\Omega} t$?

Для конечного множества операций $\Omega \subseteq O_{\mathcal{F}}$ и конечного множества термов $L \subseteq T_{\mathcal{F}}$ определим массовую проблему ВЫВОДИМОСТЬ(Ω, L):
Дано: $t \in T_{\mathcal{F}}$;
Вопрос: $L \vdash_{\Omega} t$?

Напомним, что множество операций $\Omega \subseteq O_{\mathcal{F}}$ называется клоном, если

1) Ω содержит все проекции $e_i^{(n)}$ $(i = 1, \ldots, n,\ n \in \mathbb{N})$, определенные равенством $e_i^{(n)}(x_1, \ldots, x_n) = x_i$;
2) для любых $\omega \in \Omega^{(n)}$, $\omega_1, \ldots, \omega_n \in \Omega^{(m)}$ $(n, m \in \mathbb{N})$ операция $\omega' := \omega(\omega_1, \ldots, \omega_n)$ (суперпозиция операции ω и операций $\omega_1, \ldots, \omega_n$), определенная как $\omega'(t_1, \ldots, t_m) = \omega(\omega_1(t_1, \ldots, t_m), \ldots, \omega_n(t_1, \ldots, t_m))$ на любом наборе $(t_1, \ldots, t_m) \in T_{\mathcal{F}}^m$, также принадлежит Ω.

Стоит отметить, что каждая проекция $e_i^{(n)}$ $(i = 1, \ldots, n,\ n \in \mathbb{N})$ принадлежит $O_{\mathcal{F}}$, поскольку задается формулой $x_i = y$, и каждая суперпозиция $\omega(\omega_1, \ldots, \omega_n)$ также принадлежит $O_{\mathcal{F}}$, поскольку задается формулой

$$\exists y_1, \ldots, y_n \big(\mathfrak{A}_1(x_1, \ldots, x_m, y_1) \wedge \ldots \wedge \mathfrak{A}_n(x_1, \ldots, x_m, y_n) \wedge \mathfrak{B}(y_1, \ldots, y_n, y)\big),$$

где $\mathfrak{A}_1, \ldots, \mathfrak{A}_n, \mathfrak{B}$ — формулы, задающие операции $\omega_1, \ldots, \omega_n$ и ω, соответственно.

Для $\Omega \subseteq O_{\mathcal{F}}$ обозначим через $[\Omega]$ наименьший клон в $O_{\mathcal{F}}$, содержащий Ω. Таким образом определенный оператор замыкания $[\cdot]$ обладает следующим свойством.

Лемма 1. *Если $\Omega \subseteq O_{\mathcal{F},\Pi}$, то $[\Omega] \subseteq O_{\mathcal{F},\Pi}$.*

Для конечного множества операций $\Omega \subseteq O_{\mathcal{F}}$ определим массовую проблему ВЫРАЗИМОСТЬ(Ω):
Дано: $\omega \in O_{\mathcal{F}}$;
Вопрос: $\omega \in [\Omega]$?

Лемма 2. *Если $\Omega \subseteq O_{\mathcal{F},\Pi}$ и ВЫРАЗИМОСТЬ(Ω) алгоритмически разрешима, то ВЫВОДИМОСТЬ(Ω) также алгоритмически разрешима.*

Определим понятие автомата над термам. Существует несколько равносильных определений автомата над термами [4, 11]. Рассмотрим одно из них, в котором (конечный) автомат над термами $T_{\mathcal{F}}$ определяется как $\mathcal{A} := \langle \mathcal{F},\ Q,\ \varphi,\ Q_F \rangle$, где Q — (конечное) множество состояний автомата, $Q_F \subseteq Q$ — множество заключительных состояний, φ — функция переходов, сопоставляющая каждому элементу $f^{(n)} \in \mathcal{F}$ функцию $\varphi_f : Q^n \to Q$. Множество всех конечных автоматов над термами $T_{\mathcal{F}}$ обозначим через $A_{\mathcal{F}}$.

Отображение $\varphi\colon \mathcal{F} \to P_Q$, где P_Q — множество функций на Q, естественным образом расширяется до отображения $\varphi\colon T_{\mathcal{F}}(\{x_1, \ldots, x_n\}) \to P_Q^{(n)}$ $(n \in \mathbb{N})$ по правилу

$$\varphi_{f(t_1,\ldots,t_m)} = \varphi_f(\varphi_{t_1}, \ldots, \varphi_{t_m})$$

для любых $f \in \mathcal{F}^{(m)},\ t_1, \ldots, t_m \in T_{\mathcal{F}}(\{x_1, \ldots, x_n\}),\ m \in \mathbb{N} \cup \{0\}$, и $\varphi_{x_i}(x_1, \ldots, x_n) = x_i,\ i = 1, \ldots, n$. Легко заметить, что для любого $t \in T_{\mathcal{F}}$ функция φ_t является константой из Q.

Будем говорить, что автомат $\mathcal{A}$ принимает терм $t \in T_{\mathcal{F}}$, если $\varphi_t \in Q_F$. Таким образом, каждый автомат $\mathcal{A} \in A_{\mathcal{F}}$ определяет одноместный предикат $\rho_{\mathcal{A}}$ на множестве термов $T_{\mathcal{F}}$, заданный множеством термов, принимаемых автоматом $\mathcal{A}$.

Аналогично можно определить n-местные $(n \geqslant 2)$ предикаты на $T_{\mathcal{F}}$, заданными конечными автоматами. Для этого закодируем наборы $(t_1, \ldots, t_n) \in T_{\mathcal{F}}^n$ термами $T_{\mathcal{F}'}$ над некоторым конечным множеством функциональных символов $\mathcal{F}'$ [11]. Положим $\mathcal{F}' := (\mathcal{F} \cup \{\perp\})^n$, где $\perp$ — это новый символ арности 0, не принадлежащий $\mathcal{F}$. Арность функционального символа $f_1^{(k_1)} \ldots f_n^{(k_n)}$ есть $\max(k_1, \ldots, k_n)$.

Определим по индукции понятие кода пары термов $t, s \in T_{\mathcal{F}}$. Пусть $t = f(t_1, \ldots, t_p)$ и $s = g(s_1, \ldots, s_q)$; положим

$$[t, s] := fg([t_1, s_1], \ldots, [t_q, s_q], [t_{q+1}, \perp], \ldots, [t_p, \perp]),$$

если $p \geqslant q$, и

$$[t, s] := fg([t_1, s_1], \ldots, [t_p, s_p], [\perp, s_{p+1}], \ldots, [\perp, s_q]),$$

если $p \leqslant q$.

Для более общего случая кодом термов $t_1, \ldots, t_n \in T_{\mathcal{F}}$, где $t_i = f_i(t_i^1, \ldots, t_i^{k_i}),\ i = 1, \ldots, n$, будем называть терм

$$[t_1, \ldots, t_n] := f_1 \ldots f_n([t_1^1, \ldots, t_n^1], \ldots, [t_1^m, \ldots, t_n^m]),$$

где m — арность символа $f_1 \dots f_n$ и $t_i^j = \perp$ для $j > k_i$.

Каждый автомат $\mathcal{A} \in A_{(\mathcal{F}\cup\{\perp\})^n}$ определяет n-местный предикат $\rho_{\mathcal{A}}(x_1, \dots, x_n)$ на множестве термов $T_{\mathcal{F}}$ ($n \in \mathbb{N}$), заданный условием

$$\rho_{\mathcal{A}}(t_1, \dots, t_n) = 1 \leftrightharpoons \mathcal{A} \text{ принимает терм } [t_1, \dots, t_n]$$

для любых $t_1, \dots, t_n \in T_{\mathcal{F}}$. Обозначим множество всех таких n-местных предикатов на множестве $T_{\mathcal{F}}$ через

$$R_{\mathcal{F}}^{(n)} := \{\rho_{\mathcal{A}} \mid \mathcal{A} \in A_{(\mathcal{F}\cup\{\perp\})^n}\}.$$

Положим $R_{\mathcal{F}} := \cup_{n\geqslant 0} R_{\mathcal{F}}^{(n)}$ — множество всех предикатов на $T_{\mathcal{F}}$.

Будем говорить, что операция $\omega \in O_{\mathcal{F}}^{(n)}$ сохраняет предикат $\rho \in R_{\mathcal{F}}^{(m)}$, если для любых $\overline{t_1}, \dots, \overline{t_n} \in T_{\mathcal{F}}^m$ выполнено

$$\overline{t_1}, \dots, \overline{t_n} \in \rho \Rightarrow \omega(\overline{t_1}, \dots, \overline{t_n}) \in \rho,$$

где $\overline{t_i} = (t_i^1, \dots, t_i^m)$, $i = 1, \dots, n$, и $\omega(\overline{t_1}, \dots, \overline{t_n}) = (\omega(t_1^1, \dots, t_n^1), \dots, \omega(t_1^m, \dots, t_n^m))$. По определению считаем, что пустой предикат сохраняет любая функция.

Лемма 3. *Существует алгоритм, который по любой паре* $(\omega, \rho) \in O_{\mathcal{F}} \times R_{\mathcal{F}}$ *выдает ответ «да», если* ω *сохраняет* ρ, *и «нет» — иначе.*

Отношение сохранения операцией предиката определяет соответствие Галуа между операциями $O_{\mathcal{F}}$ и предикатами $R_{\mathcal{F}}$ на множестве термов $T_{\mathcal{F}}$. Соответствие Галуа задается парой отображений:

$$\begin{aligned} \mathrm{Inv}\colon 2^{O_{\mathcal{F}}} \to 2^{R_{\mathcal{F}}}, &\quad \Omega \mapsto \{\rho \in R_{\mathcal{F}} \mid (\forall \omega \in \Omega)\ \omega \text{ сохраняет } \rho\}, \\ \mathrm{Pol}\colon 2^{R_{\mathcal{F}}} \to 2^{O_{\mathcal{F}}}, &\quad \Gamma \mapsto \{\omega \in O_{\mathcal{F}} \mid (\forall \rho \in \Gamma)\ \omega \text{ сохраняет } \rho\}, \end{aligned}$$

где 2^M — множество всех подмножеств множества M.

Теорема 2. *Если* $\Omega \subseteq O_{\mathcal{F}}$ *и* $[\Omega] = \mathrm{Pol}\,\mathrm{Inv}\,\Omega$, *то ВЫРАЗИМОСТЬ*$(\Omega)$ *алгоритмически разрешима.*

Как следствие из теоремы 2 и леммы 2 имеем.

Следствие 2. *Если* $\Omega \subseteq O_{\mathcal{F},\Pi}$ *и* $[\Omega] = \mathrm{Pol}\,\mathrm{Inv}\,\Omega$, *то ВЫВОДИМОСТЬ*$(\Omega)$ *алгоритмически разрешима.*

Данное утверждение можно усилить, если воспользоваться понятием локального замыкания множества операций [15, 16]. Локальным замыканием множества операций $\Omega \subseteq O_{\mathcal{F}}$ будем называть множество

$$\begin{aligned} \operatorname{Loc}\Omega := \{\omega \in O_{\mathcal{F}}^{(n)} \mid \forall L \subseteq T_{\mathcal{F}}^{(n)},\ |L| < \infty, \\ \exists \omega' \in \Omega^{(n)} :\ \omega\big|_L = \omega'\big|_L;\ n \in \mathbb{N}\}. \end{aligned}$$

Это множество всех n-арных операций ($n \in \mathbb{N}$) таких, что для любого конечного множества термов $L \subseteq T_{\mathcal{F}}^{(n)}$ найдется операция из Ω, совпадающая с ω на L.

Теорема 3. *Если $\Omega \subseteq O_{\mathcal{F},\Pi}$ и $\operatorname{Loc}[\Omega] = \operatorname{Pol}\operatorname{Inv}\Omega$, то ВЫВОДИМОСТЬ$(\Omega)$ алгоритмически разрешима.*

Для произвольного множества термов $L \subseteq T_{\mathcal{F}}$ обозначим через $R_{\mathcal{F}}^{(1)}(L) := \{\rho \in R_{\mathcal{F}}^{(1)} \mid L \subseteq \rho\}$ — множество одноместных предикатов, содержащих L. Множество термов $L \subseteq T_{\mathcal{F}}$ назовем автоматно-отделимым, если

$$L = \bigcap_{\rho \in R_{\mathcal{F}}^{(1)}(L)} \rho.$$

Теорема 4. *Если $\Omega \subseteq O_{\mathcal{F}},\ L \subseteq T_{\mathcal{F}}$ и $[L]_\Omega$ автоматно-отделимо, то проблема ВЫВОДИМОСТЬ(Ω, L) алгоритмически разрешима.*

Следует отметить, что понятие автоматной отделимости является обобщением конечной интерпретации [5], которое принято называть также финитной регулярной истинностной матрицей [6] или оценкой [7]. Из теоремы 4, в частности, следует известный результат для классического исчисления высказываний, что каждое конечно-аппроксимируемое исчисления разрешимо [6].

2. Доказательство утверждений

2.1. Доказательство теоремы 1

Без ограничения общности будем считать, что $\mathcal{F}$ состоит только из функциональных символов $1^{(0)},\ \cdot^{(2)}$, где 1 — функциональный символ арности 0, а $\cdot$ — функциональный символ арности 2. При этом терм $\cdot(x_1, x_2)$ будем обозначать через $(x_1 \cdot x_2)$ или просто через $x_1 x_2$. Расстановку скобок в терме

$$(x_1 \cdot (x_2 \cdot \ldots \cdot (x_{n-1} \cdot x_n)))$$

будем называть стандартной. Далее будем опускать некоторые скобки, считая, что терм $x_1 \cdot \ldots \cdot x_n$ имеет стандартную расстановку скобок.

Для доказательства неразрешимости множества термов воспользуемся понятием нормальной системы Поста [17]. Для этого рассмотрим частный случай таких систем — однородные системы продукций Поста или «Тэг» системы.

Однородные системы продукций Поста

Однородная система продукции Поста — это тройка $\Sigma = \langle A, V, l \rangle$, где $A = \{a_1, \ldots, a_n\}$ — конечный алфавит; V — множество пар вида (α, β), где $\alpha, \beta \in A^+$ и $|\alpha| = l$, A^+ — множество непустых слов в алфавите A; $l \geqslant 1$ — натуральное число. Будем предполагать, что для любых (α, β), $(\alpha', \beta') \in V$ слова α и α' различны.

Будем говорить, что система Σ применима к слову ξ, если существует пара $(\alpha, \beta) \in V$, для которой слово α является началом слова ξ, то есть $\xi = \alpha\gamma$, в противном случае — не применима. Результатом применения Σ к слову $\xi = \alpha\gamma$, где $(\alpha, \beta) \in V$, будем называть слово $\gamma\beta$. Факт применимости Σ будем обозначать через $\alpha\gamma \xrightarrow{\Sigma} \gamma\beta$.

Будем называть слово $\beta \in A^+$ Σ-продукцией слова $\alpha \in A^+$ и писать $\alpha \overset{\Sigma}{\Longrightarrow} \beta$, если существует конечная последовательность слов $\gamma_1, \ldots, \gamma_s \in A^*$ такая, что $\gamma_1 = \alpha, \gamma_s = \beta$ и $\gamma_i \xrightarrow{\Sigma} \gamma_{i+1}$, $i = 1, \ldots, s-1$. Также будем предполагать, что $\alpha \overset{\Sigma}{\Longrightarrow} \alpha$. Множество всех Σ-продукций слова α обозначим через $[\alpha]_\Sigma$.

Теорема 5 (Минский М. Л. [14]). *Существует однородная система продукций Поста Σ и такое слово η, для которых множество продукций $[\eta]_\Sigma$ неразрешимо.*

Кодирование слов термами

Определим своего рода кодирование, сопоставив каждой букве a_i алфавита A некоторый терм $\overline{a_i} \in T_{\{1,\ \cdot\}}$ однозначным образом. Положим $t_0 := x_1$ и $t_k := t_{k-1} \cdot t'_{k-1}$ при $k \geqslant 1$, где

$$t'_k := t_k\{x_1 \leftarrow x_{2^k+1}, \dots, x_{2^k} \leftarrow x_{2^{k+1}}\},$$

где $t\{x_1 \leftarrow s_1, \dots, x_n \leftarrow s_n\}$ означает подстановку в терме t вместо переменных $x_1, \dots, x_n$ термов $s_1, \dots, s_n$. Таким образом, терм t_k ($k \geqslant 0$) представляет собой полное дерево высоты k, листьям которого приписаны различные переменные $x_1, \dots, x_{2^k}$.

Кодом буквы $a_i \in A$ будем считать терм

$$\overline{a_i} := t_{\lceil \log_2 n \rceil}\{x_1 \leftarrow 1, \dots, x_i \leftarrow 11, \dots, x_{2^{\lceil \log_2 n \rceil}} \leftarrow 1\}, \ i = 1, \dots, n.$$

Несложно убедиться, что для любых $a, b \in A$ код $\overline{a}$ не является подтермом кода $\overline{b}$.

Далее, произвольному непустому слову $\alpha = a_{i_1} \dots a_{i_l}$ над алфавитом A сопоставим класс всех термов вида $\overline{a_{i_1}} \cdot \ldots \cdot \overline{a_{i_l}}$, с произвольной расстановкой скобок между элементами $\overline{a_{i_1}}, \dots, \overline{a_{i_l}}$. Произвольного представителя этого класса обозначим через $\overline{\alpha}$, которого будем называть кодом слова α. Таким образом, каждый представитель одного класса кодирует одно и тоже слово. Также положим

$$\begin{aligned}
\overrightarrow{\alpha} &:= (\overline{a_{i_1}} \cdot (\ \ldots \cdot (\overline{a_{i_{l-1}}} \cdot \overline{a_{i_l}}))),\\
\overleftarrow{\alpha} &:= (((\overline{a_{i_1}} \cdot \overline{a_{i_2}}) \cdot \ldots \ ) \cdot \overline{a_{i_l}}),\\
\overrightarrow{\alpha x} &:= (\overline{a_{i_1}} \cdot (\ \ldots \cdot (\overline{a_{i_l}} \cdot x))).
\end{aligned}$$

Построением множеств Ω и L

Пусть $\Sigma = \langle A, V, l \rangle$ — однородная система продукций Поста и $\eta \in A^*$ — непустое слово. Положим $L_\eta := \{\overrightarrow{\eta}\}$ и Ω_Σ — это множество операций

$$\begin{aligned}
\omega^1_\alpha(x) = y \ &\leftrightharpoons \ \exists z \big(x = \overrightarrow{\alpha z} \wedge y = z \cdot \overrightarrow{\beta}\big), \ (\alpha, \beta) \in V,\\
\omega^2_\alpha(x) = y \ &\leftrightharpoons \ x = \overrightarrow{\alpha} \wedge y = \overrightarrow{\beta}, \ (\alpha, \beta) \in V,\\
\omega^3_a(x) = y \ &\leftrightharpoons \ \exists u, v, z \big(x = ((u \cdot (\overline{a} \cdot v)) \cdot z) \wedge y = (((u \cdot \overline{a}) \cdot v) \cdot z)\big), \ a \in A,\\
\omega^4_a(x) = y \ &\leftrightharpoons \ \exists u, v \big(x = ((u \cdot \overline{a}) \cdot v) \wedge y = (u \cdot (\overline{a} \cdot v))\big), \ a \in A.
\end{aligned}$$

Свойства алгебры $(T_{\{1,\cdot\}}, \Omega_\Sigma)$

Лемма 4. *Если* $\xi, \beta, \zeta \in A^+$, *то* $(\overleftarrow{\xi} \cdot \overrightarrow{\beta}) \cdot \overrightarrow{\zeta} \vdash_{\Omega_\Sigma} \overleftarrow{\xi\beta} \cdot \overrightarrow{\zeta}$.

Доказательство. Доказывать будем индукцией по длине слова β. Если $|\beta| = 1$, то терм $(\overleftarrow{\xi} \cdot \overrightarrow{\beta}) \cdot \overrightarrow{\zeta}$ совпадает с $\overleftarrow{\xi\beta} \cdot \overrightarrow{\zeta}$. Пусть теперь $\beta = a\delta$, где $|\delta| \geqslant 1$; с помощью операции ω_a^3 из терма $(\overleftarrow{\xi} \cdot \overrightarrow{\beta}) \cdot \overrightarrow{\zeta}$ выводим терм $(\overleftarrow{\xi a} \cdot \overrightarrow{\delta}) \cdot \overrightarrow{\zeta}$. По индуктивному предположению $(\overleftarrow{\xi a} \cdot \overrightarrow{\delta}) \cdot \overrightarrow{\zeta} \vdash_{\Omega_\Sigma} \overleftarrow{\xi\beta} \cdot \overrightarrow{\zeta}$. Лемма доказана.

Следствие 3. *Если* $\beta, \zeta \in A^+$, *то* $\overrightarrow{\beta} \cdot \overrightarrow{\zeta} \vdash_{\Omega_\Sigma} \overleftarrow{\beta} \cdot \overrightarrow{\zeta}$.

Лемма 5. *Если* $\beta, \zeta \in A^+$, *то* $\overleftarrow{\beta} \cdot \overrightarrow{\zeta} \vdash_{\Omega_\Sigma} \overrightarrow{\beta\zeta}$.

Доказательство. Доказывать будем индукцией по длине слова β. Если $|\beta| = 1$, то терм $\overleftarrow{\beta} \cdot \overrightarrow{\zeta}$ совпадает с $\overrightarrow{\beta\zeta}$. Пусть $\beta = \delta a$, где $|\delta| \geqslant 1$; с помощью операции ω_a^4 из терма $\overleftarrow{\beta} \cdot \overrightarrow{\zeta}$ выводим терм $\overleftarrow{\delta} \cdot \overrightarrow{a\zeta}$. По индуктивному предположению $\overleftarrow{\delta} \cdot \overrightarrow{a\zeta} \vdash_{\Omega_\Sigma} \overrightarrow{\beta\zeta}$. Лемма доказана.

Следствие 4. *Если* $\beta, \zeta \in A^+$, *то* $\overrightarrow{\beta} \cdot \overrightarrow{\zeta} \vdash_{\Omega_\Sigma} \overrightarrow{\beta\zeta}$.

Лемма 6. *Если* $\xi \xrightarrow{\Sigma} \zeta$, *то* $\overrightarrow{\xi} \vdash_{\Omega_\Sigma} \overrightarrow{\zeta}$.

Доказательство. Поскольку Σ применима к ξ, то $\xi = \alpha\gamma,\ |\alpha| = l$, и найдется такое $\beta \in A^+$, что $(\alpha, \beta) \in V$. Если γ — пустое, то $\zeta = \beta$ и с помощью операции ω_α^2 из терма $\overrightarrow{\xi}$ выводим терм $\overrightarrow{\zeta}$. Если же $|\gamma| > 0$, то $\zeta = \gamma\beta$ и выводима цепочка:

$$\overrightarrow{\alpha\gamma} \vdash_{\Omega_\Sigma} \overrightarrow{\gamma} \cdot \overrightarrow{\beta} \vdash_{\Omega_\Sigma} \overrightarrow{\gamma\beta}$$

где первый вывод есть применение операции ω_α^1, а второй — применение следствия 4. Лемма доказана.

Следствие 5. *Если* $\xi \overset{\Sigma}{\Rightarrow} \zeta$, *то* $\overrightarrow{\xi} \vdash_{\Omega_\Sigma} \overrightarrow{\zeta}$.

Лемма 7. *Если* $\overline{\xi} \vdash_{\Omega_\Sigma} \overline{\zeta}$, *то* $\xi \overset{\Sigma}{\Rightarrow} \zeta$.

Доказательство. Для $L \subseteq T_{\{1,\cdot\}}$ обозначим через $\langle L \rangle$ множество, содержащее L и все термы, получающие из L однократным применением операций Ω_Σ. Положим $L_0 = \{\overline{\xi}\},\ L_{k+1} = \langle L_k \rangle,\ k \geqslant 0$. Так как $\overline{\xi} \vdash_{\Omega_\Sigma} \overline{\zeta}$, то найдется $k \geqslant 0$, для которого $\overline{\zeta} \in L_k$ и $\overline{\zeta} \notin L_{k'}$ при $k' < k$.

Докажем лемму индукцией по k. Если $k = 0$, то $\overline{\zeta} = \overline{\xi}$ и $\xi \overset{\Sigma}{\Rightarrow} \zeta$. Пусть утверждение леммы верно для всех $k' < k$, докажем его для k.

Если $\overline{\zeta} = \omega_\alpha^1(t)$ для некоторого $t \in L_{k-1}$, то найдется пара $(\alpha, \beta) \in V$, для которой $t = \overrightarrow{\alpha\gamma}$ и $\overline{\zeta} = \overrightarrow{\gamma} \cdot \overrightarrow{\beta}$. Значит $\zeta = \gamma\beta$ и $\alpha\gamma \xrightarrow{\Sigma} \zeta$. По индуктивному предположению $\xi \overset{\Sigma}{\Rightarrow} \alpha\gamma$, следовательно, $\xi \overset{\Sigma}{\Rightarrow} \zeta$.

Если $\overline{\zeta} = \omega_\alpha^2(t)$ для некоторого $t \in L_{k-1}$, то найдется пара $(\alpha, \beta) \in V$, для которой $t = \overrightarrow{\alpha}$ и $\overline{\zeta} = \overrightarrow{\beta}$. По индуктивному предположению $\xi \overset{\Sigma}{\Rightarrow} \alpha$, следовательно, $\xi \overset{\Sigma}{\Rightarrow} \zeta$.

Если $\overline{\zeta} = \omega_\alpha^3(t)$ для некоторого $t \in L_{k-1}$, то $\overline{\zeta} = ((t_1 \cdot \overline{a}) \cdot t_2) \cdot t_3,\ a \in A,\ t_1, t_2, t_3 \in T_{\{1,\cdot\}}$. По выбору способа кодирования термы $t_1 \cdot \overline{a},\ (t_1 \cdot \overline{a}) \cdot t_2,\ ((t_1 \cdot \overline{a}) \cdot t_2) \cdot t_3$ и подтермы в $\overline{a}$ не могут быть кодами букв алфавита A, поэтому термы t_1, t_2, t_3 являются кодами подслов $\zeta_1, \zeta_2, \zeta_3$ слова ζ, то есть ζ представимо в виде $\zeta_1 a \zeta_2 \zeta_3$. Значит, терм $t = (t_1 \cdot (\overline{a} \cdot t_2)) \cdot t_3$ также является кодом слова ζ и по индуктивному предположению $\xi \overset{\Sigma}{\Rightarrow} \zeta$.

Если $\overline{\zeta} = \omega_\alpha^4(t)$ для некоторого $t \in L_{k-1}$, то $\overline{\zeta} = t_1 \cdot (\overline{a} \cdot t_2),\ a \in A,\ t_1, t_2 \in T_{\{1,\cdot\}}$. Аналогичными рассуждениями можно показать, что термы t_1, t_2 являются кодами подслов ζ_1, ζ_2 слова $\zeta = \zeta_1 a \zeta_2$. Значит, терм $t = (t_1 \cdot \overline{a}) \cdot t_2$ также является кодом слова ζ и по индуктивному предположению $\xi \overset{\Sigma}{\Rightarrow} \zeta$.

Лемма доказана.

Доказательство теоремы 1

По следствию 5 код любой продукции из $[\eta]_\Sigma$ выводим из множества L_η с помощью операций Ω_Σ. По лемме 7 любой код слова из $[L_\eta]_{\Omega_\Sigma}$ является кодом продукции из $[\eta]_\Sigma$. Поэтому, если бы множество термов $[L_\eta]_{\Omega_\Sigma}$ было разрешимо, то разрешимым было бы и множество продукций $[\eta]_\Sigma$. По теореме 5 существует такие Σ и η, для которых множество продукций $[\eta]_\Sigma$ неразрешимо. Следовательно, множество термов $[L_\eta]_{\Omega_\Sigma}$ также неразрешимо. Теорема доказана.

2.2. Доказательство леммы 1

Поскольку каждая проекция $e_i^{(n)}$ $(i = 1, \ldots, n,\ n \in \mathbb{N})$ принадлежит $O_{\mathcal{F},\Pi}$, то достаточно показать, что для любых операций $\omega \in O_{\mathcal{F},\Pi}^{(n)}$ и $\omega_1, \ldots, \omega_n \in O_{\mathcal{F},\Pi}^{(m)}$ $(n, m \in \mathbb{N})$ их суперпозиция $\omega(\omega_1, \ldots, \omega_n)$ также принадлежит $O_{\mathcal{F},\Pi}$.

В самом деле, если операции $\omega_1, \ldots, \omega_n, \omega$ задаются допустимыми формулами $\mathfrak{A}_1, \ldots, \mathfrak{A}_n, \mathfrak{B} \in \Phi_\Pi$, соответственно, то суперпозиция $\omega(\omega_1, \ldots, \omega_n)$ задается формулой

$$\mathfrak{C} := \exists y_1, \ldots, y_n \big(\mathfrak{A}_1(x_1, \ldots, x_m, y_1) \wedge \ldots \\ \ldots \wedge \mathfrak{A}_n(x_1, \ldots, x_m, y_n) \wedge \mathfrak{B}(y_1, \ldots, y_n, y)\big).$$

Поскольку формулы $\mathfrak{A}_1, \ldots, \mathfrak{A}_n, \mathfrak{B}$ не содержат символа $\neg$, то и $\mathfrak{C}$ не содержит этого символа. Следовательно, $\mathfrak{C} \in \Phi_\Pi$. Лемма 1 доказана.

2.3. Доказательство леммы 2

Примитивно позитивные формулы вида

$$\exists z_1, \ldots, z_m \left(x_{i_1} = t_1 \wedge \ldots x_{i_k} = t_k\right),$$

где $t_j \in T_{\mathcal{F}}(\{x_1, \ldots, x_n, z_1, \ldots, z_m\} \setminus \{x_{i_1}, \ldots, x_{i_k}\})$, $1 \leqslant j \leqslant k$ $1 \leqslant k \leqslant n$, будем называть формулами стандартного вида.

Лемма 8. *Любую примитивно позитивную формулу можно привести к стандартному виду.*

Доказательство. Пусть $\mathfrak{A} \in \Phi_\Pi^{(n)}$ — примитивно позитивная формула со свободными переменными $x_1, \ldots, x_n$. Поскольку $\mathfrak{A}$ не содержит отрицаний, то эквивалентными преобразованиями можно сместить все кванторы существования в левый край формулы и тем самым получить формулу вида

$$\exists z_1, \ldots, z_m \left(t_1 = s_1 \wedge \ldots t_k = s_k\right)$$

для некоторого $k \geqslant 1$, где $t_i, s_i \in T_{\mathcal{F}}(\{x_1, \ldots, x_n, z_1, \ldots, z_m\})$, $1 \leqslant i \leqslant k$.

По лемме об унифицирующей подстановке [5] существует такая подстановка

$$\sigma\colon \{x_1, \ldots, x_n, z_1, \ldots, z_m\} \to T(\mathcal{F}, \{x_1, \ldots, x_n, z_1, \ldots, z_m\}),$$

что $t_i\sigma \equiv s_i\sigma$ для каждого $i = 1, \ldots, k$ и любая подстановка σ' с тем же свойством разлагается в произведение $\sigma' = \sigma\sigma''$, для некоторой подстановки σ''. Без ограничения общности будем считать, что

$$\sigma = \{x_1 \leftarrow t_1,\ \ldots,\ x_p \leftarrow t_p,\ z_1 \leftarrow s_1,\ \ldots,\ z_q \leftarrow s_q\},$$

где $t_i, s_j \in T(\mathcal{F}, \{x_{p+1}, \ldots, x_n, z_{q+1}, \ldots, z_m\}),\ i = 1, \ldots, p,\ j = 1, \ldots, q$.

Несложно убедиться, что формула $\mathfrak{A}$ эквивалентна формуле

$$\exists z_1, \ldots, z_m \left(x_1 = t_1 \wedge \ldots \wedge x_p = t_p\right),$$

которая имеет стандартный вид. Лемма доказана.

На множестве наборов термов $T^n_{\mathfrak{F}}(\mathcal{U})$, длины n ($n \geqslant 1$) определим отношением частичного порядка $\leqslant$. Для двух наборов $(t_1, \ldots, t_n)$, $(s_1, \ldots, s_n) \in T^n_{\mathfrak{F}}(\mathcal{U})$ положим $(t_1, \ldots, t_n) \leqslant (s_1, \ldots, s_n)$ всякий раз, когда найдется такая подстановка $\sigma\colon \mathcal{U} \to T^n_{\mathfrak{F}}(\mathcal{U})$, что термы σt_i и s_i совпадают для каждого $i = 1, \ldots, n$.

Каждая примитивно позитивная формула стандартного вида

$$\exists z_1, \ldots, z_m \left(x_1 = t_1 \wedge \ldots \wedge x_k = t_k\right)$$

определяет n-местный предикат $\rho_{\overline{t}}$ на множестве термов $T_{\mathfrak{F}}$, заданный условием

$$\rho_{\overline{t}}(s_1, \ldots, s_n) = 1 \rightleftharpoons \overline{t} \leqslant (s_1, \ldots, s_n),$$

где $\overline{t} = (t_1, \ldots, t_k, x_{k+1}, \ldots, x_n) \in T^n_{\mathfrak{F}}(\{x_{k+1}, \ldots, x_n, z_1, \ldots, z_m\})$. И, наоборот, каждый набор $(t_1, \ldots, t_n) \in T^n_{\mathfrak{F}}(\{x_1, \ldots, x_n, z_1, \ldots, z_m\})$ определяет примитивно позитивную формулу вида

$$\exists z_1, \ldots, z_m \left(x_1 = t_1 \wedge \ldots \wedge x_n = t_n\right).$$

Лемма 9. *Если $L \subseteq T_{\mathcal{F}},\ |L| < \infty$ и $t \in T_{\mathcal{F}}$, то $|\Omega_\Pi(L, t)| < \infty$.*

Доказательство. Рассмотрим произвольную операцию $\omega \in \Omega_\Pi(L, t)$ и пусть она задается формулой $\mathfrak{A} \in \Phi^{(n+1)}_\Pi$ со свободными переменными $x_1, \ldots, x_n, y$. По лемме 8 можно считать, что формула $\mathfrak{A}$ имеет стандартный вид и определяет предикат $\rho_{\overline{s}}$, где $\overline{s} \in T^{n+1}_{\mathcal{F}}(\mathcal{U}),\ i = 1, \ldots, k$. Так как $\omega \in \Omega_\Pi(L, t)$, то найдутся такие термы $t_1, \ldots, t_n \in L$, что $\omega(t_1, \ldots, t_n) = t$. Поэтому $\overline{s} \leqslant (t_1, \ldots, t_n, t)$.

Таким образом, каждая операция $\omega \in \Omega_\Pi(L, t)$ задается набором термов $\overline{s}$, для которого найдутся такие $t_1, \ldots, t_n \in L$, что $\overline{s} \leqslant (t_1, \ldots, t_n, t)$. Поскольку наборов $\overline{s} \in T^{n+1}_{\mathcal{F}}(\mathcal{U})$, удовлетворяющих условию $\overline{s} \leqslant (t_1, \ldots, t_n, t)$, конечное число (с точностью до переименования переменных), то операций из $\Omega_\Pi(L, t)$ также конечное число. Лемма доказана.

Доказательство леммы 2

Пусть $\Omega \subseteq O_{\mathcal{F},\Pi}$ — конечное множество примитивно-позитивных операций. Покажем, что для любого конечного множества термов $L \subseteq T_{\mathcal{F}}$ и терма $t \in T_{\mathcal{F}}$ выполнено включение $t \in [L]_\Omega$ тогда и только тогда, когда $\Omega_\Pi(L,t) \cap [\Omega] \neq \varnothing$.

Если $t \in [L]_\Omega$, то для некоторой операции $\omega \in [\Omega] \cap O^{(n)}_{\mathcal{F}}$ найдутся такие термы $t_1, \ldots, t_n \in L$, что $\omega(t_1, \ldots, t_n) = t$. Поэтому $\omega \in \Omega_\Pi(L,t)$.

Если $\omega \in \Omega_\Pi(L,t) \cap [\Omega]$, то по определению $\Omega_\Pi(L,t)$ найдутся такие термы $t_1, \ldots, t_n \in L$, что $\omega(t_1, \ldots, t_n) = t$. Так как $\omega \in [\Omega]$, то $t \in [L]_\Omega$.

Предположим, что проблема ВЫРАЗИМОСТЬ(Ω) алгоритмически разрешима. Опишем алгоритм, решающий проблему ВЫВОДИМОСТЬ(Ω). Получая на вход конечное множестве термов L и терм t, он последовательно пробегает множество операций $\Omega_\Pi(L,t)$, которое конечно по лемме 9. Если очередная операция ω принадлежит $[\Omega]$, то выдается ответ «да», терм $t \in [L]_\Omega$, иначе выдается ответ «нет», терм $t \notin [L]_\Omega$. Лемма 2 доказана.

2.4. Доказательство леммы 3

Рассмотрим автомат $\mathcal{A} = \langle \mathcal{F}, Q, \varphi, Q_F \rangle \in A_{(\mathcal{F}\cup\bot)^m}$, $m \geqslant 1$. Будем говорить, что предикат $\rho \subseteq Q^n$ представляет формулу $\mathfrak{A} \in \Phi^{(n)}$ посредством автомата $\mathcal{A}$, если для любых $q_1, \ldots, q_n \in Q$ $\rho(q_1, \ldots, q_n) = 1$ тогда и только тогда, когда найдутся такие наборы термов $(t^1_1, \ldots, t^m_1), \ldots, (t^1_n, \ldots, t^m_n) \in T^m_{\mathcal{F}}$, что $\varphi_{[t^1_i \ldots t^m_i]} = q_i$, $i = 1, \ldots, n$, и $\rho_{\mathfrak{A}}(t^j_1, \ldots, t^j_n) = 1$, $j = 1, \ldots, m$.

Лемма 10. *Для любого автомата $\mathcal{A} \in A_{(\mathcal{F}\cup\bot)^m}$, $m \geqslant 1$, и формулы $\mathfrak{A} \in \Phi$ существует предикат ρ, представляющий формулу $\mathfrak{A}$ посредством автомата $\mathcal{A}$.*

Доказательство. Пусть $\mathcal{A} = \langle \mathcal{F},\ Q,\ \varphi,\ Q_F \rangle$. Доказывать будем индукцией по глубине формулы $\mathfrak{A}$.

Если $\mathfrak{A}$ — это формула вида $t = s$, где $t, s \in T(\mathcal{F}, \{x_1, \ldots, x_n\})$, то по лемме об унифицирующей подстановке [5] существует такая подстановка

$$\sigma \colon \{x_1, \ldots, x_n\} \to T(\mathcal{F}, \{x_1, \ldots, x_n\}),$$

что $t\sigma \equiv s\sigma$. Без ограничения общности будем считать, что

$$\sigma = \{x_1 \leftarrow s_1,\ \ldots,\ x_k \leftarrow s_k\},$$

где $s_i \in T(\mathcal{F}, \{x_{k+1}, \ldots, x_n\}),\ i = 1, \ldots, k$. Возьмем в качестве ρ предикат

$$x_1 = \varphi_{[s_1 \ldots s_1]}(x_{k+1}, \ldots, x_n) \wedge \ldots \wedge x_k = \varphi_{[s_k \ldots s_k]}(x_{k+1}, \ldots, x_n).$$

Покажем, что ρ представляет $\mathfrak{A}$ посредством $\mathcal{A}$.

Если для некоторых $q_1, \ldots, q_n \in Q$ выполнено $\rho(q_1, \ldots, q_n) = 1$, то $q_i = \varphi_{[s_i \ldots s_i]}(q_{k+1}, \ldots, q_n),\ i = 1, \ldots, k$. Можно считать, что в $\mathcal{A}$ все состояния достижимы [11], поэтому существуют такие термы $[t^1_{k+1} \ldots t^m_{k+1}], \ldots, [t^1_n \ldots t^m_n] \in T_{(\mathcal{F}\cup\perp)^m}$, что $\varphi_{[t^1_i \ldots t^m_i]} = q_i,\ i = k+1, \ldots, n$. Положим $\sigma_j = \{x_{k+1} \leftarrow t^j_{k+1}, \ldots, x_n \leftarrow t^j_n\}$ и $t^j_i = s_i\sigma_j$, $i = 1, \ldots, k,\ j = 1, \ldots, m$. Для любого $i = 1, \ldots, k$ имеем

$$\varphi_{[t^1_i \ldots t^m_i]} = \varphi_{[s_i \ldots s_i]}(\varphi_{[t^1_{k+1} \ldots t^m_{k+1}]}, \ldots, \varphi_{[t^1_n \ldots t^m_n]}) = \varphi_{[s_i \ldots s_i]}(q_{k+1}, \ldots, q_n) = q_i.$$

Так как $t\sigma \equiv s\sigma$, то

$$t\{x_1 \leftarrow t^j_1,\ \ldots,\ x_n \leftarrow t^j_n\} \equiv s\{x_1 \leftarrow t^j_1,\ \ldots,\ x_n \leftarrow t^j_n\},\ j = 1, \ldots, m. \tag{1}$$

Следовательно, $\rho_{\mathfrak{A}}(t^j_1, \ldots, t^j_n) = 1$ для любого $j = 1, \ldots, m$.

Если же для некоторых $q_1, \ldots, q_n \in Q$ нашлись такие наборы термов $(t^1_1, \ldots, t^m_1), \ldots, (t^1_n, \ldots, t^m_n) \in T^m_{\mathcal{F}}$, что $\varphi_{[t^1_i \ldots t^m_i]} = q_i, i = 1, \ldots, n$, и $\rho_{\mathfrak{A}}(t^j_1, \ldots, t^j_n) = 1,\ j = 1, \ldots, m$, то выполнено (1). Поэтому для любого $j = 1, \ldots, m$ подстановка

$$\widetilde{\sigma_j} = \{x_1 \leftarrow t^j_1,\ \ldots,\ x_n \leftarrow t^j_n\}$$

является решением уравнения $t = s$. По лемме об унифицирующей подстановке для каждого $j = 1, \ldots, m$ существует такая подстановка σ'_j, что $\widetilde{\sigma_j} = \sigma\sigma'_j$, причем,

$$x_i\widetilde{\sigma_j} = \begin{cases} s_i\sigma'_j,\ i = 1, \ldots, k, \\ x_i\sigma'_j,\ i = k+1, \ldots, n. \end{cases}$$

Для любого $i = 1, \ldots, k$ имеем

$$q_i = \varphi_{[t^1_i, \ldots, t^m_i]} = \varphi_{[s_i\sigma'_1 \ldots s_i\sigma'_m]} = \\ = \varphi_{[s_i \ldots s_i]}(\varphi_{[t^1_{k+1}, \ldots, t^m_{k+1}]}, \ldots, \varphi_{[t^1_n, \ldots, t^m_n]}) = \varphi_{[s_i \ldots s_i]}(q_{k+1}, \ldots, q_n).$$

Следовательно, $\rho(q_1, \ldots, q_n) = 1$.

Пусть $\mathfrak{A}$ — это формула вида $\mathfrak{B} \wedge \mathfrak{C}$, либо $\neg\mathfrak{B}$, либо $\exists x \mathfrak{B}(x)$. По предположению индукции существуют предикаты ρ_1 и ρ_2, представляющие посредством автомата $\mathcal{A}$ формулы $\mathfrak{B}$ и $\mathfrak{C}$ соответственно. Несложно убедиться, что предикаты $\rho_1 \wedge \rho_2$, $\overline{\rho_1}$ и $\exists x \rho_1(x)$ представляют посредством автомата $\mathcal{A}$ формулы $\mathfrak{B} \wedge \mathfrak{C}$, $\neg\mathfrak{B}$ и $\exists x \mathfrak{B}(x)$ соответственно. Лемма доказана.

Доказательство леммы 3

Рассмотрим произвольную пару $(\omega, \rho) \in O_{\mathcal{F}} \times R_{\mathcal{F}}$. Пусть $\omega \in O_{\mathcal{F}}^{(n)}$ и $\rho \in R_{\mathcal{F}}^{(m)}$. По определению найдется такая допустимая формула $\mathfrak{A} \in \Phi^{(n+1)}$ и такой автомат $\mathcal{A} = \langle \mathcal{F},\ Q,\ \varphi,\ Q_F \rangle \in A_{(\mathcal{F} \cup \perp)^m}$, что $\omega = \omega_{\mathfrak{A}}$ и $\rho = \rho_{\mathcal{A}}$. По лемме 10 существует $(n+1)$-местный предикат ρ', представляющий формулу $\mathfrak{A}$ посредством автомата $\mathcal{A}$. Положим

$$\widetilde{\rho}(y) := \exists x_1, \ldots, x_n \in Q_F \big(\rho'(x_1, \ldots, x_n, y)\big).$$

Если $\widetilde{\rho} \subseteq Q_F$, то для любых $(t_1^1, \ldots, t_1^m), \ldots, (t_n^1, \ldots, t_n^m) \in T_{\mathcal{F}}^m$, если $\varphi_{[t_i^1 \ldots t_i^m]} \in Q_F,\ i = 1, \ldots, n$, то

$$\varphi_{[\omega(t_1^1, \ldots, t_n^1) \ldots \omega(t_1^m, \ldots, t_n^m)]} \in Q_F.$$

Следовательно, ω сохраняет ρ.

Пусть нашлось такое $q_0 \notin Q_F$, что $\widetilde{\rho}(q_0) = 1$. По определению предиката $\widetilde{\rho}$ найдутся такие $q_1, \ldots, q_n \in Q_F$, что $\rho'(q_1, \ldots, q_n, q_0) = 1$. Поскольку ρ' представляет формулу $\mathfrak{A}$ посредством автомата $\mathcal{A}$, то найдутся такие наборы термов $(t_0^1, \ldots, t_0^m), (t_1^1, \ldots, t_1^m), \ldots, (t_n^1, \ldots, t_n^m) \in T_{\mathcal{F}}^m$, что $\varphi_{[t_i^1 \ldots t_i^m]} = q_i, i = 0, 1, \ldots, n$, и $\rho_{\mathfrak{A}}(t_1^j, \ldots, t_n^j, t_0^j) = 1,\ j = 1, \ldots, m$. Отсюда, $\omega(t_1^j, \ldots, t_n^j) = t_0^j$ для каждого $j = 1, \ldots, m$. Так как $\varphi_{[t_i^1 \ldots t_i^m]} \in Q_F,\ i = 1, \ldots, n$, и $\varphi_{[t_0^1 \ldots t_0^m]} \notin Q_F$, то ω не сохраняет ρ.

Таким образом, операция ω сохраняет предикат ρ тогда и только тогда, когда $\widetilde{\rho} \subseteq Q_F$. Поскольку множества $\widetilde{\rho}$ и Q_F конечны, то переборный алгоритм сможет за конечное число шагов дать ответ «да», если ω сохраняет ρ, и «нет» — иначе. Лемма 3 доказана.

2.5. Доказательство теоремы 2

Пусть $\Omega \subseteq O_{\mathcal{F}}$ — конечное множество операций. Опишем алгоритм, решающий проблему ВЫРАЗИМОСТЬ(Ω). Получая на вход операцию ω, он последовательно пробегает перечислимые множества операций $[\Omega]$ и предикатов $R_{\mathcal{F}}$. Если на i-ом шаге алгоритм остановился на паре (ω_i, ρ_i), то проверяются условия:

1) Если $\omega = \omega_i$, то выдается ответ «да», операция $\omega \in [\Omega]$;
2) Если все операции из Ω сохраняют ρ_i, а операция ω не сохраняет ρ_i, то выдается ответ «нет», операция $\omega \notin [\Omega]$.

Согласно лемме 3 существует алгоритм, который по любой паре $(\omega, \rho) \in O_{\mathcal{F}} \times R_{\mathcal{F}}$ проверяет, сохраняет ли операция ω предикат ρ. Поскольку $[\Omega] = \mathrm{Pol}\ \mathrm{Inv}\ \Omega$, то для любого предиката $\rho \in R_{\mathcal{F}}$, который сохраняют все операции из Ω, условие $\omega \notin [\Omega]$ равносильно тому, что ω не сохраняет ρ. Поэтому описанный процесс проверки принадлежности $\omega \in [\Omega]$ остановится за конечное число шагов. Теорема 2 доказана.

2.6. Доказательство теоремы 3

Пусть $\Omega \subseteq O_{\mathcal{F},\Pi}$ — конечное множество примитивно-позитивных операций. Опишем алгоритм, решающий проблему ВЫВОДИМОСТЬ(Ω). Получая на вход конечное множество термов L и терм t, он последовательно пробегает перечислимые множества операций $\mathrm{Loc}\ [\Omega]$ и предикатов $R_{\mathcal{F}}$. Если на i-ом шаге алгоритм остановился на паре (ω_i, ρ_i), то проверяются условия:

1) Если $\omega_i \in \Omega_\Pi(L, t)$, то выдается ответ «да», терм $t \in [L]_\Omega$;
2) Если все операции из Ω сохраняют ρ_i, а все операции из $\Omega_\Pi(L, t)$ не сохраняют ρ_i, то выдается ответ «нет», терм $t \notin [L]_\Omega$.

Покажем, что условие $\Omega_\Pi(L, t) \cap \mathrm{Loc}\ [\Omega] \neq \varnothing$ влечет за собой включение $t \in [L]_\Omega$. В самом деле, если $\omega \in \Omega_\Pi(L, t) \cap \mathrm{Loc}\ [\Omega]$, то существует операция $\omega' \in [\Omega]$, которая совпадает с ω на множестве L. Значит найдутся такие термы $t_1, \ldots, t_n \in L$, что $\omega(t_1, \ldots, t_n) = t$. Следовательно, $t \in [L]_\Omega$.

По условию теоремы $\mathrm{Loc}\ [\Omega] = \mathrm{Pol}\ \mathrm{Inv}\ \Omega$. Покажем, что для любого предиката $\rho \in R_{\mathcal{F}}$, который сохраняют все операции из Ω, если все операции из $\Omega_\Pi(L, t)$ не сохраняют ρ, то $t \notin [L]_\Omega$. Предположим противное, что все операции из $\Omega_\Pi(L, t)$ не сохраняют ρ, но $t \in [L]_\Omega$. Если $t \in [L]_\Omega$, то для некоторой операции $\omega \in [\Omega] \cap O_{\mathcal{F}}^{(n)}$ найдутся такие термы $t_1, \ldots, t_n \in L$, что $\omega(t_1, \ldots, t_n) = t$. Поэтому $\omega \in \Omega_\Pi(L, t)$ и ω сохраняет ρ, что противоречит предположению.

Из леммы 9 следует, что для любого конечного множества термов L и терма t множество операций $\Omega_\Pi(L, t)$ конечно. Согласно лемме 3 существует алгоритм, который по любой паре $(\omega, \rho) \in O_\mathcal{F} \times R_\mathcal{F}$ проверяет, сохраняет ли операция ω предикат ρ. Так как множество Ω конечно, то описанный процесс проверки принадлежности $t \in [L]_\Omega$ остановится за конечное число шагов. Теорема 3 доказана.

2.7. Доказательство теоремы 4

Пусть $\Omega \subseteq O_\mathcal{F}$ — конечное множество операций и $L \subseteq T_\mathcal{F}$ — конечное множество термов из условия теоремы. Последовательность термов

$$t_1,\ t_2,\ \ldots,\ t_{i_1},\ \ldots,\ t_{i_n},\ \ldots,\ t_j,\ \ldots$$

будем называть выводом в L, если для любого $j > 0$ терм t_j либо принадлежит L, либо существует такая операция $\omega \in \Omega$, что $t_j = \omega(t_{i_1}, \ldots, t_{i_n})$ для некоторых индексов $i_1, \ldots, i_n$ меньших j. Ясно, что максимальный вывод в L содержит все термы из $[L]_\Omega$.

Опишем алгоритм, решающий проблему ВЫВОДИМОСТЬ(Ω, L). Получая на вход терм t, он последовательно пробегает множество одноместных предикатов $R^{(1)}_\mathcal{F}$ и максимальный вывод в L. Если на i-ом шаге алгоритм остановился на паре (ρ_i, t_i), то проверяются условия:

1) Если $t = t_i$, то выдается ответ «да», терм $t \in [L]_\Omega$;
2) Если $L \subseteq \rho_i$ и все операции $\omega \in \Omega$ сохраняют предикат ρ_i, но $\rho_i(t) = 0$, то выдается ответ «нет», терм $t \notin [L]_\Omega$.

Согласно лемме 3 существует алгоритм, который по любой паре $(\omega, \rho) \in O_\mathcal{F} \times R_\mathcal{F}$ проверяет, сохраняет ли операция ω предикат ρ. Так как множества Ω и L конечны, то описанный процесс проверки принадлежности $t \in [L]_\Omega$ сойдется.

Поскольку для любого $\rho \in R^{(1)}_\mathcal{F}$ условие $[L]_\Omega \subseteq \rho$ равносильно тому, что $L \subseteq \rho$ и каждая операция $\omega \in \Omega$ сохраняет ρ, то описанный алгоритм решает проблему ВЫВОДИМОСТЬ(Ω, L). Теорема 4 доказана.

Список литературы

[1] Боков Г. В. Проблема полноты в исчислении высказываний // Интеллектуальные системы. — 2009. Т. 13, вып. 1–4. — С. 165–181.

[2] Боков Г. В. Об алгоритмической неразрешимости проблемы выразимости пропозициональных исчислений // Интеллектуальные системы. — 2013. Т. 17, вып. 1–4. — С. 271–292.

[3] Кон П. Универсальная алгебра. — М.: Мир, 1968.

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

[5] Кудрявцев В. Б., Гасанов Э. Э., Подколзин А. С. Введение в теорию интеллектуальных систем. — М.: Изд-во ф-та ВМиК МГУ, 2006.

[6] Кузнецов А. В. Неразрешимость общих проблем полноты, разрешимости и эквивалентности для исчислений высказываний // Алгебра и логика. — 1963. Т. 2, № 4. — С. 47–66.

[7] Новиков П. С. Элементы математической логики. — М.: Наука, 1973.

[8] Шенфилд Д. Математическая логика. — М.: Наука, 1975.

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

[10] Börner F. Basics of Galois Connections // Complexity of Constraints, Lecture Notes in Computer Science. — Berlin Heidelberg: Springer, 2008. V. 5250. — P. 38–67.

[11] Comon H., Dauchet M., Gilleron R., Löding C., Jacquemard F., Lugiez D., Tison S., Tommasi M. Tree Automata Techniques and Applications. — 2008. Available on: http://www.grappa.univ-lille3.fr/tata.

[12] Harrop R. On the existence of finite models and decision procedures // Proceedings of the Cambridge Philosophical Society. — 1958. V. 54. — P. 1–16.

[13] Linial S., Post E. L. Recursive unsolvability of the deducibility, Tarski's comleteness, and independence of axioms problems of the propositional calculus // Bulletin of the American Mathematical Society. — 1949. V. 55. — P. 50.

[14] Minsky M. L. Recursive unsolvability of Post's problem of "tag" and other topics in theory of Turing machines // Annals of Mathematics. — 1961. V. 74. — P. 437-455.

[15] Pöschel R. A general Galois theory for operations and relations and concrete characterization of related algebraic structures. / Report R–01/80, Zentralinstitut für Mathematik und Mechanik, Akademie der Wissenschaften der DDR. — Berlin, 1980.

[16] Pöschel R. Galois Connections for Operations and Relations // Galois Connections and Applications. Mathematics and Its Applications. — Netherlands: Springer, 2004. V. 565. — P. 231–258.

[17] Post E. L. Formal reduction of the general combinatorial decision problem // American Journal of Mathematics. — 1943. V. 65. — P. 197–215.