Записки научных
семинаров ПОМИ
Том 277, 2001 г.

В. Б. Жижкун

ВЕРХНИЕ ОЦЕНКИ ВЫСОТЫ ТЕРМОВ В РЕШЕНИИ ЗАДАЧИ КВАЗИУНИФИКАЦИИ

1. Введение

В исследованиях сложности логического вывода часто удается свести задачу поиска доказательства (например, по заданной схеме и некоторой дополнительной информации) к задачам, в которых неизвестными являются термы. Примерами таких задач являются унификация [5], решение уравнений в термах с подстановками [6, 3], квазиунификация [8]. В некоторых случаях изучение возникающих задач позволяет получить оценку сложности (высоты) их решений и, следовательно, оценку сложности самого доказательства [2, 4].

В работе [8] приводится метод, позволяющий свести задачу восстановления доказательства (с сечениями) по его схеме к задаче квазиунификации. Неразрешимость задачи квазиунификации была установлена в [9]. В [10] доказана разрешимость задачи для случая одной пары термов и приведен способ сведения задачи для нескольких пар термов к задаче для двух пар (с помощью введения новых функциональных знаков большой арности). В [7] получен алгоритм, строящий *наиболее общий квазиунификатор* для любой имеющей решение задачи квазиунификации (для некоторых не имеющих решения задач алгоритм не заканчивает работу). Наконец, в [8] указывается, что задача квазиунификации для случая, когда вхождения ненулевой глубины имеют лишь термы, начинающиеся с одноместных или нульместных функциональных знаков, может быть сведена к разрешимой задаче решения уравнений в свободной полугруппе.

В данной работе получены оценки сложности решения задачи квазиунификации как раз для последнего случая. Хотя известен общий способ решения систем уравнений в свободных полугруппах (иначе, уравнений в словах) [1], он решает гораздо

Работа выполнена при поддержке INTAS (грант 96-0760).

более общий класс задач, чем требуется для квазиунификации с указанными ограничениями, и поэтому оценки для него слишком грубы для прямого применения в теории доказательств. Поэтому представляется полезным получить оценки сложности решения задачи квазиунификации, не прибегая к [1]. Именно это и является целью данной работы, наряду с получением более простых алгоритмов для нахождения решения.

Структура работы. В разделе 2 вводятся основные понятия, используемые в работе. В разделе 3 приводятся несколько простых свойств строк для удобства изложения. Раздел 4 посвящен решению систем линейных неравенств, что будет использовано в дальнейшем. В разделе 5 приводятся алгоритм и оценки для решения задачи одноместной квазиунификации. В разделе 6 описываются (без доказательства) шаги алгоритма решения задачи "почти одноместной" квазиунуфикации. Раздел 7 содержит формальные обоснования этих шагов и оценки высоты решения задачи.

Автор выражает глубокую благодарность В. П. Оревкову и Б. Ю. Коневу за ряд ценных замечаний, позволивших значительно улучшить структуру и содержание работы.

§2. Основные понятия

Пусть имеется язык, в который входят функциональные знаки (для каждого из которых фиксирована арность) и неизвестные. *Термом* называется объект, построенный по следующим правилам:

1. неизвестная или нульместный функциональный знак – терм;
2. если $t_1, \dots, t_n$ – термы и f – n-местный функциональный знак, то $f(t_1, \dots, t_n)$ – терм.

Высотой терма t (обозначим $h[t]$) будем называть следующую величину:

1. если t – неизвестная или нульместный функциональный знак, то $h[t] = 0$;
2. если t имеет вид $f(t_1, \dots, t_n)$, то $h[t] = 1 + \max\limits_{1 \le k \le n} h[t_k]$.

Подстановкой назовем конечный список пар: $\sigma = \{x_1 \to t_1, \dots, x_n \to t_n\}$, где t_i – терм и x_i – неизвестная, имея ввиду, что при применении подстановки σ к терму T (обозначим $T\sigma$) мы *одновременно* замещаем все вхождения $x_1, \ldots, x_n$ на вхождения $t_1, \ldots, t_n$ соответственно. *Высотой* подстановки σ (обозначим $h[\sigma]$) называется максимум высоты входящих в нее термов.

Мы будем говорить, что подстановка σ *более общая* чем σ', если найдется подстановка δ такая, что $\sigma\delta = \sigma'$.

Подстановка σ называется *унификатором* пар термов $\{(s_1, t_1), \ldots, (s_k, t_k)\}$, если $s_1\sigma = t_1\sigma, \ldots, s_k\sigma = t_k\sigma$ (равенства понимаются как графические).

Подстановка σ называется *наиболее общим унификатором* пар термов, если она является унификатором и для любого унификатора σ' найдется подстановка δ такая, что $\sigma' = \sigma\delta$.

Система пар термов называется *унифицируемой*, если у нее есть унификатор. У любой унифицируемой системы есть наиболее общий унификатор и он единственен с точностью до переименования переменных [5].

Подстановка σ называется *квазиунификатором* пар термов $\{(s_1, t_1), \ldots, (s_k, t_k)\}$, если найдутся такие подстановки $\delta_1, \ldots, \delta_k$, что выполняются графические равенства:

$$\begin{cases} s_1\sigma\delta_1 = t_1\sigma \\ \quad \ldots \\ s_k\sigma\delta_k = t_k\sigma. \end{cases} \tag{1}$$

Мы будем также говорить, что σ (или, иногда, что набор $\{\sigma, \delta_1, \ldots, \delta_k\}$) является решением задачи квазиунификации (1).

Наиболее общим квазиунификатором (*универсальным* решением задачи квазиунификации) называется квазиунификатор σ такой, что для любого квазиунификатора σ' существует подстановка ρ, для которой $\sigma' = \sigma\rho$. У любой имеющей решение задачи квазиунификации есть универсальное решение (единственное, с точностью до переименования неизвестных) [7].

§3. Строки. Основные определения и свойства

Пусть у нас имеется конечный алфавит (набор) F. Элементы F будем называть *буквами* (*символами*) F. *Строкой* (*словом*) в F назовем любую конечную цепочку букв F. Пустую строку (не содержащую ни одной буквы) будем обозначать Λ, предполагая, что Λ не является буквой F.

Конкатенацией строк A и B (обозначается AB) назовем строку, получающуюся в результате приписывания B к A справа.

Строка A *равна* строке B (обозначается $A = B$), если в них на одинаковых позициях стоят одинаковые буквы.

Строка A является *началом* строки B (обозначается $A \leq B$), если найдется такая строка C, что $AC = B$.

Две строки называются *сравнимыми*, если одна из них является началом другой.

Длиной строки A (обозначается $|A|$) назовем количество вхождений букв в A. Очевидно, для любой строки A: $|A| \in \mathbf{N}$, где $\mathbf{N}$ обозначает множество натуральных чисел, включая 0.

Пусть $n \in \mathbf{N}$ и $n \leq |A|$. *Ограничением* A на n (обозначается $A|_n$) назовем строку B такую, что $B \leq A$ и $|B| = n$ (очевидно, что такая строка существует).

Приведем несколько очевидных свойств:

1. Если $AB = AC$, то $B = C$ (*сокращение слева*).
2. Если $BA = CA$, то $B = C$ (*сокращение справа*).
3. Если $A = B$ и $C = D$, то $AC = BD$.
4. Если $A = B$, то $|A| = |B|$.
5. Если $A = B$, $n \in \mathbf{N}$ и $n \leq |A|$, то $A|_n = B|_n$.
6. Если $n \in \mathbf{N}$ и $n \leq |A|$, то $(AB)|_n = A|_n$ для любой строки B.
7. Если $n = |A|$ и $A|_n = B$, то $A = B$.
8. $|AB| = |A| + |B|$.

Лемма 4.1. *Пусть A, B, C_1, C_2 – строки, такие что $C_1A = C_2B$. Тогда C_1 и C_2 сравнимы.*

Доказательство. Пусть, для определенности, $|C_1| \leq |C_2|$ и $|C_1| = n$. Тогда $(C_1A)|_n = (C_2B)|_n$, значит $C_1|_n = C_2|_n$. Но $C_1|_n = C_1$, значит $C_1 = C_2|_n$, откуда $C_1 \leq C_2$. □

§4. Решение систем линейных неравенств в натуральных числах

В данном разделе исследуются системы линейных неравенств специального вида, которые будут использованы для решения задачи одноместной квазиунификации. Раздел носит технический характер и может быть пропущен без существенного ущерба для понимания основного материала статьи.

Рассмотрим систему линейных неравенств с m переменными $x_1, \ldots, x_m \in \mathbf{N}$ и целыми коэффициентами $a_1, \ldots, a_n, b_1, \ldots, b_n$:

$$\begin{cases} a_1 + x_{i_1} \le b_1 + x_{j_1} \\ \quad \dots \\ a_n + x_{i_n} \le b_n + x_{j_n}. \end{cases} \tag{2}$$

Перенесем в (2) постоянные коэффициенты в левую часть, обозначив $c_k = a_k - b_k$:

$$\begin{cases} x_{i_1} + c_1 \le x_{j_1} \\ \quad \dots \\ x_{i_n} + c_n \le x_{j_n}. \end{cases} \tag{3}$$

Рассмотрим направленный граф, вершинами которого являются переменные $x_1,\dots,x_m$ системы (3), а дуги соответствуют неравенствам (3): дуга из x_p идет в x_q тогда и только тогда, когда найдется такое k, что k-е неравество системы имеет вид $x_p + c_k \le x_q$. Пусть дуга, соответствущая k-му неравенству системы, помечена c_k. Итак, мы получили направленный граф $G = (V, E)$, где V – множество вершин (оно совпадает со множеством переменных), $|V| = m$, E – множество дуг, $|E| = n$, и каждая дуга помечена целым числом.

Замечание. Если для $k \ne l$ выполняется $i_k = i_l$ и $j_k = j_l$, и кроме того, $c_k \le c_l$, то k-е неравенство (3) можно выкинуть, не меняя множество решений. Тогда G действительно будет *графом*, а не *мультиграфом*, и неравенства (3) можно индексировать парами (x_{i_k}, y_{i_k}), то есть писать $c_{v,w}$ вместо c_k, где $v + c_k = w$ – k-е неравенство (3).

Определение. *Пусть $q: V \to \mathbf{N}$ – разметка вершин графа G целыми неотрицательными числами. Назовем q допустимой, если для каждой дуги $(v, w) \in E$, помеченной $c_{v,w}$, выполняется неравенство: $q(v) + c_{v,w} \le q(w)$.*

Очевидно, каждая допустимая разметка G является решением (3), и обратно, каждое решение (3) задает допустимую разметку.

Пусть $V \ne \emptyset$. Будем строить допустимую разметку графа с помощью следующего алгоритма:

Алгоритм 4.1

1. $i := 0$, $U_0 := V$, $R_0 := \emptyset$, $q_0(v) := 0$ для всех $v \in V$

2. **Комментарий:** U_i, R_i, q_i уже построены

3. **Если** $U_i = \emptyset$, **то** *КОНЕЦ:* q_{i-1}*–допустимая разметка*
4. **Если** $i = m$, **то** *КОНЕЦ: решения нет*
5. $\bar{U} := \emptyset$, $\bar{R} := R_i$ $\bar{q}(v) := q_i(v)$ для всех $v \in V$
6. **Для всех** $v \in U_i$, **и для всех** w **таких, что** $(v, w) \in E$
7. **Если** $q_i(v) + c_{v,w} > \bar{q}(w)$, **то**
8. $\bar{U} := \bar{U} \cup \{w\}$
9. $\bar{R} := \left(\bar{R} \setminus \{(u, w) \mid u \in V)\}\right) \cup \{(v, w)\}$
10. $\bar{q}(w) := q_i(v) + c_{v,w}$
11. **Все**
12. **Все**
13. $U_{i+1} := \bar{U}$, $R_{i+1} := \bar{R}$, $q_{i+1}(v) := \bar{q}(v)$ для всех $v \in V$
14. $i := i + 1$, перейти к **2**.

Замечания. 1. Построенные в ходе работы алгоритма множества $R_1, R_2, \ldots$ не нужны для собственно работы алгоритма, однако будут использованы в дальнейшем для доказательства свойств построенного решения.

2. Для всех i разметка q_{i+1} зависит только от разметки q_i и от структуры графа G, но не зависит от порядка, в котором на шаге 6 перебираются вершины v и w.

Докажем корректность работы *Алгоритма* 4.1.

Лемма 4.1. *Если в графе G есть цикл, сумма пометок на дугах которого положительна, то у G не существует допустимых разметок.*

Доказательство. Пусть для цикла $v = v_1 \to v_2 \to \ldots \to v_k = v$ выполнено $c_{v_1,v_2} + \ldots + c_{v_{k-1},v_k} > 0$, и пусть q–допустимая разметка. Тогда по определению допустимости: $q(v) = q(v_k) \geq q(v_{k-1}) + c_{v_{k-1},v_k} \geq q(v_{k-2}) + c_{v_{k-2},v_{k-1}} + c_{v_{k-1},v_k} \geq \cdots \geq q(v_1) + c_{v_1,v_2} + \ldots + c_{v_{k-1},v_k} > q(v)$, что невозможно. □

Определение. *В графе G назовем длиной пути количество дуг в этом пути и весом пути сумму пометок входящих в него дуг.*

Лемма 4.2. *Если вершина v входит в множество U_i, то в графе G существует путь $v_0 \to \ldots \to v_i = v$ длины i, обладающий следующими свойствами:*
1) *его вес в точности равен $q_i(v)$;*
2) *$v_j \in U_j$ для всех $j \leq i$.*

Доказательство. Строим нужный путь по индукции.

При $i = 0$–очевидно. Пусть предположение верно для всех $v \in U_i$. Пусть $w \in U_{i+1}$. Тогда существует вершина $v \in U_i$ такая, что $(v, w) \in E$ и $q_{i+1}(w) = q_i(v) + c_{v,w}$. По индукционному предположению существует путь $v_0 \to \ldots \to v_i = v$ с весом $q_i(v)$. Путь $v_1 \to \ldots \to v_k \to v \to w$ с весом $q_i(v) + c_{v,w} = q_{i+1}(w)$ – искомый. $\Box$

Лемма 4.3. *Для любого i, для которого построено U_i и для любого $j < i$ выполнено: $q_j(v) \leq q_i(v)$ для всех $v \in V$.*

Доказательство. Легко показывается по индукции. $\Box$

Лемма 4.4. *Для любого i, для которого построены U_i и U_{i+1} и для всех $v \in V$*

$$q_i(v) \neq q_{i+1}(v) \iff v \in U_{i+1}.$$

Доказательство. Из приведенного алгоритма видно, что вершина v добавляется в U_{i+1} тогда и только тогда, когда на i-м шаге меняется значение $\bar{q}(v)$, т.е. $q_{i+1}(v) \neq q_i(v)$. $\Box$

Лемма 4.5. *Для любой вершины v, для любого i такого, что построено U_i, для любого пути в v длины i с весом W выполняется: $W \leq q_i(v)$.*

Доказательство. По индукции. При $i = 0$: очевидно. Пусть это верно для некоторого i, и пусть $v_0 \to \ldots \to v_i \to v$ – путь длины $i+1$ с весом W, и пусть построено U_{i+1} (а значит, и q_{i+1}). Тогда $W - c_{v_i,v} = c_{v_0,v_1} + \ldots + c_{v_{i-1},v_i} \leq q_i(v_i)$. Пусть $k \leq i$ – наименьшее такое, что $q_k(v_i) = q_i(v_i)$. Либо $k = 0$ и $v_i \in V = U_0$, либо $k > 0$, тогда $q_{k-1}(v_i) \neq q_k(v_i)$ и, стало быть (лемма 4.4), $v_i \in U_k$. В обоих случаях $v_i \in U_k$, откуда заключаем, что $q_{k+1}(v) \geq q_k(v_i) + c_{v_i,v}$. Тогда $W \leq q_i(v_i) + c_{v_i,v} = q_k(v_i) + c_{v_i,v} \leq q_{k+1}(v) \leq q_{i+1}(v)$. $\Box$

Лемма 4.6. *Если $v \in U_i$ для некоторого $i > 0$, то для любого пути, заканчивающегося в v, длины меньше i его вес строго меньше $q_i(v)$.*

Доказательство. По леммам 4.3, 4.4 заключаем, что $q_{i-1}(v) < q_i(v)$, поэтому если W – вес некоторого пути в v длины не больше $i-1$, то (лемма 4.5) $W \leq q_{i-1}(v) < q_i(v)$. $\Box$

Лемма 4.7. *Если $U_m \neq \emptyset$, то в графе G существует цикл с положительным весом и, следовательно, для него нет допустимых разметок.*

Доказательство. Пусть $v \in U_m$. Тогда (лемма 4.2) существует путь с весом $q_m(v)$: $v_0 \to \ldots \to v_m = v$, состоящий из $(m+1)$-ой вершины, причем $v_i \in U_i$. Так как всего вершин m, среди $v_0,\dots,v_m$ есть хотя бы две одинаковые. Пусть $v_i = v_j$, причем $i < j$. Рассмотрим путь $v_0 \to \dots v_{i-1} \to v_i \to v_{j+1} \to \dots \to v_m$. Его длина меньше m, и по прежнему $v_m = v$. По лемме 4.6 вес этого пути меньше $q_m(v)$, значит вес выкинутого куска $v_i \to v_{i+1} \to \dots \to v_j$ положителен. Осталось заметить, что это цикл. □

Лемма 4.8. *Если существует $i < m$ такое, что $U_{i+1} = \emptyset$, то q_i – допустимая разметка.*

Доказательство. Допустим, что q_i не является допустимой разметкой, то есть найдутся две соединенные дугой вершины v и w, для которых $q_i(v) + c_{v,w} > q_i(w)$. Пусть $j \leq i$ – наименьшее число такое, что $q_j(v) = q_i(v)$. Тогда $v \in U_j$ (лемма 4.4). Заметим, что $j \neq i$, так как в противном случае U_{i+1} содержало бы по крайней мере w. Тогда по определению q_{j+1} должно выполняться неравенство $q_j(v) + c_{v,w} \leq q_{j+1}(w)$. Таким образом, мы получили $q_i(w) < q_i(v)+c_{v,w} \leq q_j(v)+c_{v,w} \leq q_{j+1}(w)$, что невозможно (лемма 4.3) ввиду того, что $j + 1 \leq i$. □

Осталось собрать все леммы.

Теорема 4.1. *Предложенный алгоритм не более чем за m итераций определяет неразрешимость системы* (3) *или выдает ее решение.*

Доказательство. Непосредственное следствие лемм 4.7, 4.8. □

Покажем, что *Алгоритм* 4.1 позволяет строить "наименьшее" решение (3). Пусть $q: V \to \mathbf{N}$ – построенное решение, то есть существует $k \leq m$ такое, что $U_{k+1} = \emptyset$, $q = q_k$. Положим $R := R_k$.

Лемма 4.10. *В каждую вершину G входит не более одной дуги из множества R.*

Доказательство. Действительно, при добавлении в R_i дуги (v, w), из него предварительно выкидываются все дуги, ведущие в w. □

Лемма 4.11. *Если дуга $(v, w) \in R$, то $q(v) + c_{v,w} = q(w)$.*

Доказательство. Пусть $i \leq k$ – наименьшее такое число, что выполняется $q_i(w) = q(w)$. Тогда дуга (v, w) была добавлена в R_i и не затрагивалась в R_j для $j > i$. Кроме этого, $q_{i-1}(v) + c_{v,w} = q_i(w)$. Теперь заметим, что $q_{i-1}(v) = q(v)$, иначе, если $q_{i-1}(v) <$

$q(v)$, то выполнялось бы $q(v) + c_{v,w} > q_{i-1}(v) + c_{v,w} = q_i(w) = q(w)$, что невозможно ввиду допустимости q. Таким образом, $q(v) + c_{v,w} = q(w)$. $\square$

Лемма 4.12. *Если $(v, w) \in R$, то $q(w) > 0$.*

Доказательство. Из условия следует, что $w \in U_i$ для некоторого $i > 0$. Значит (лемма 4.4), $q(w) \geq q_i(w) > q_{i-1}(w) \geq q_0(w) = 0$. $\square$

Лемма 4.13. *Для любой вершины v существует путь $v_0 \to \dots \to v_i = v$, такой что:*

1) *для всех $j < i$: $(v_j, v_{j+1}) \in R$;*
2) *$q(v_0) = 0$;*
3) *вес пути равен $q(v)$.*

Доказательство. В каждую вершину G входит не более одной дуги из R, поэтому мы можем двигаться "в обратном направлении", то есть для v найдется ровно одна вершина w, такая что $(w, v) \in R$, и т.д. Мы никогда не попадем в цикл, поэтому такой процесс для любой вершины оборвется, то есть будет построен нужный путь $v_0 \to \dots \to v_i = v$. Заметим, что $q(v_0) = 0$. Действительно, в v_0 не входят дуги из R, значит v_0 ни разу не добавлялясь в U_j с $j > 0$, следовательно для всех j: $q_j(v_0) = 0$.

По лемме 4.11: $q(v) = q(v_i) = q(v_{i-1}) + c_{v_{i-1},v_i} = \dots = q(v_0) + c_{v_0,v_1} + \dots + c_{v_{i-1},v_i} = c_{v_0,v_1} + \dots + c_{v_{i-1},v_i}$, откуда следует 3). $\square$

Пусть $[x]^+$ обозначает положительный срез x:

$$[x]^+ = \begin{cases} x, & \text{если } x \geq 0 \\ 0, & \text{если } x < 0. \end{cases}$$

Лемма 4.14. *Для всех $v \in V$ верно неравенство $q(v) \leq \sum_{i=1}^{n} [c_i]^+$.*

Доказательство. Из леммы 4.13 следует, что для всех $v \in V$ существует простой путь, заканчивающийся в v, вес которого равен $q(v)$ (простым путем мы называем путь, котором каждая вершина встречается не более одного раза). Очевидно, вес простого пути в G не превосходит $\sum_{i=1}^{n} [c_i]^+$. $\square$

Лемма 4.15. *Для всех $v \in V$ верно неравенство $q(v) \leq (|V| - 1) \cdot \max\limits_i [c_i]^+$.*

Доказательство. Аналогично доказательству леммы 4.14. Нужно лишь заметить, что в простом пути не более $m - 1 = |V| - 1$ дуг. $\square$

Лемма 4.16. *Для любых* $v, w \in V$ *верно неравенство* $|q(v) - q(w)| \leq (|V| - 1) \cdot \max_i [c_i]^+$.

Доказательство. Следствие леммы 4.15. $\square$

Лемма 4.17. *Для всех* $u \in V$

$$q(u) \leq \sum_{v \in V} \max\{[c_{v,w}]^+ \mid w \in V, (v,w) \in E\} = \sum_{k=1}^{m} \max\{[c_q]^+ \mid i_q = k\}.$$

Доказательство. Пусть $v_0 \to \cdots \to v_p \to u$ – простой путь из леммы 4.13. Его вес

$$W = c_{v_0,v_1} + \cdots + c_{v_p,u} \leq \max\{[c_{v_0,w}]^+ \mid (v_0,w) \in E\} + \ldots$$
$$+ \max\{[c_{v_p,w}]^+ \mid (v_p,w) \in E\} \leq \sum_{v \in V} \max\{[c_{v,w}]^+ \mid w \in V, (v,w) \in E\}.$$

$\square$

Теорема 4.2. *Если* $t: V \to \mathbf{N}$ *– решение* (3), *то для всех* $v \in V$ *выполнено* $q(v) \leq t(v)$.

Доказательство. Пусть существует решение t и $v \in V$. Рассмотрим путь $v_0 \to \ldots \to v_k = v$, построенный в лемме 4.13. Просуммируем неравенства, соответствующие дугам этого пути: $v_0 + c_{v_0,v_1} + \ldots + v_{k-1} + c_{v_{k-1},v_k} \leq v_1 + \ldots + v_k$. Или, после сокращений, $v_0 + c_{v_0,v_1} + \ldots + c_{v_{k-1},v_k} \leq v_k = v$. Так как $t(v_0) \geq 0$, то для допустимости t необходимо $t(v) \geq c_{v_0,v_1} + \ldots + c_{v_{k-1},v_k} = q(v)$. $\square$

§5. Одноместная квазиунификация

Рассмотрим задачу квазиунификации для пар термов (s_1, t_1), $\ldots, (s_n, t_n)$ в случае, когда все $s_1, \ldots, s_n, t_1, \ldots, t_n$ содержат лишь одноместные функциональные знаки.

Пусть F – конечный алфавит функциональных знаков, V – конечный алфавит неизвестных. Тогда любой терм можно записать как $f_1 \ldots f_k X$, где $f_1, \ldots, f_k$ – элементы F, а $X \in V$. В таких предположениях переформулируем определение терма более удобным для наших целей способом.

Определение. *Термом называется пара* (A, X), *где* A *– строка в алфавите* F *и* $X \in V$.

Определение. *Терм (A,X) равен терму (B,Y) (обозначается $(A,X)=(B,Y)$), если $A \equiv B$ и $X=Y$.*

Определение. *Подстановкой называется пара отображений $\varkappa = (K,k)$, где $K: V \to F^*$ и $k: V \to V$ (через F^* обозначено множество слов в алфавите F).*

Определение. *Результатом применения подстановки $\varkappa = (K,k)$ к терму (A,X) называется терм $(AK(X),k(X))$.*

Пусть $X_1,\dots,X_m$ – все неизвестные из алфавита V, т.е. $|V|=m$. Пусть задан набор пар термов $\langle (A_1,X_{i_1}),(B_1,X_{j_1})\rangle, \dots, \langle (A_n,X_{i_n}),(B_n,X_{j_n})\rangle$, причем $1 \le i_k, j_k \le m$ для $k=1..n$. Задача квазиунификации в новых обозначениях состоит в нахождении подстановок $\sigma=(S,s)$, $\delta_1=(D_1,d_1)$, $\dots$, $\delta_n=(D_n,d_n)$ таких, что выполняются следующие равенства для термов:

$$\left\{\begin{array}{l} (A_1S(X_{i_1})D_1(s(X_{i_1})), d_1(s(X_{i_1}))) = (B_1S(X_{j_1}), s(X_{j_1})) \\ \quad \dots \\ (A_nS(X_{i_n})D_n(s(X_{i_n})), d_n(s(X_{i_n}))) = (B_nS(X_{j_n}), s(X_{j_n})). \end{array}\right. \tag{4}$$

Исходя из определения равенства для термов, получаем эквивалентную систему для строк и символов:

$$\left\{\begin{array}{l} A_1S(X_{i_1})D_1(s(X_{i_1})) \equiv B_1S(X_{j_1})) \\ \quad \dots \\ A_nS(X_{i_n})D_n(s(X_{i_n})) \equiv B_nS(X_{j_n})) \\ d_1(s(X_{i_1})) = s(X_{j_1}) \\ \quad \dots \\ d_n(s(X_{i_n})) = s(X_{j_n}). \end{array}\right. \tag{5}$$

Пусть $\sigma=(S,s)$ является решением задачи квазиунификации, т.е. найдутся нужные нам $\delta_1=(D_1,d_1),\dots\delta_n=(D_n,d_n)$. Построим подстановки $\sigma^*=(S^*,s^*)$, $\delta_1^*=(D_1^*,d_1^*)$, $\dots$, $\delta_n^*=(D_n^*,d_n^*)$ следующим образом:

1. для всех $i=1..m$ $\;s^*(X_i)=X_i$;
2. для всех $i=1..m$ $\;S^*(X_i)\equiv S(X_i)$;
3. для всех $k=1..n$ $\;D_k^*(X_{i_k}) \equiv D_k(s(X_{i_k}))$, $D_k^*(X_l)\equiv \Lambda$ для всех $l \ne i_k$;
4. для всех $k=1..n$ $\;d_k^*(X_{i_k})=X_{j_k}$, $d_k^*(X_l)=X_l$ для всех $l\ne i_k$.

Нетрудно убедиться, что тогда для всех $k = 1..n$ выполняются равенства:

$$A_k S^*(X_{i_k}) D_k^*(s^*(X_{i_k})) = B_k S^*(X_{j_k})) \ i \ d_k^*(s^*(X_{i_k})) = s^*(X_{j_k}),$$

то есть σ^* является решением (5), и кроме того, σ^* – более общий квазиунификатор, чем σ.

Таким образом, если задача (4) имеет решение, то найдется решение $\sigma^* = (S^*, s^*)$, для которого верны 1–4. Назовем такое решение (4) *нормальным*. Для такого σ^* автоматически выполняется $d_k^*(s^*(X_{i_k})) = s^*(X_{j_k})$, поэтому, обозначив $P_k := D_k^*(X_{i_k})$ и $S_k := S^*(X_k)$, получим, что разрешимость (4) равносильна разрешимости следующей системы уравнений в словах:

$$\begin{cases} A_1 S_{i_1} P_1 = B_1 S_{j_1} \\ \quad \dots \\ A_n S_{i_n} P_n = B_n S_{j_n}. \end{cases} \tag{6}$$

По любому нормальному решению (5) можно построить решение (6), взяв P_k и S_k, как определено выше, и обратно, по любому решению (6) находится решение (5), если воспользоваться определением P_k и S_k и 1–4.

Кроме того, для любых σ_1 и σ_2, нормальных решений (4), и соответствующих им решений (6) строк $S_1^1, \dots, S_m^1$, $P_1^1, \dots, P_n^1$ и $S_1^2, \dots, S_m^2$, $P_1^2, \dots, P_n^2$ верно утверждение:

$$\sigma_1 \text{ более общее, чем } \sigma_2 \iff S_k^1 \le S_k^2 \quad k = 1..m$$

Итак, нахождение универсального решения задачи квазиунификации (4) равносильно нахождению универсального (иначе, наименьшего) решения (6), то есть такого, что каждая его строка является началом (а это мы и обозначили "$\le$") соответствующей строки любого другого решения (6).

Заметим, что систему (6) можно переписать в виде системы неравенств для слов:

$$\begin{cases} A_1 S_{i_1} \le B_1 S_{j_1} \\ \quad \dots \\ A_n S_{i_n} \le B_n S_{j_n}. \end{cases} \tag{7}$$

Обозначим $a_i = |A_i|$, $b_i = |B_i|$, $x_i = |S_i|$. Для существования решения системы (7) необходимо (но не достаточно), чтобы была разрешима в натуральных числах система линейных неравенств с m переменными:

$$\begin{cases} a_1 + x_{i_1} \le b_1 + x_{j_1} \\ \quad \dots \\ a_n + x_{i_n} \le b_n + x_{j_n}. \end{cases} \tag{8}$$

Системы такого вида исследуются в разделе 4, где строится алгоритм, находящий наименьшее (покомпонентно) решение (8), а также приводятся оценки величины компонент этого решения.

Возможны 2 ситуации:

1. Система (8) неразрешима, значит неразрешима и система (7);
2. Существует решение (8). Тогда существует набор $(t_1^0,\dots, t_m^0)$, который является решением (8) и для любого решения $(t_1,\dots,t_m)$ системы (8) для всех $i = 1..m$ выполняется $t_i^0 \le t_i$ (набор $(t_1^0,\dots,t_m^0)$ строится Алгоритмом 4.1). Мы покажем, что если система (7) разрешима, то существует ее решение $(T_i^0,\dots, T_m^0)$ такое, что $|T_i^0| = t_i^0$ для всех $i = 1,..m$. Таким образом, длины строк самого короткого решения системы (7) не превосходят $\max\{t_i^0 \mid 1 \le i \le m\}$.

Пусть $S = (T_1,\dots,T_m)$ – какое-то решение системы (7). Обозначим $t_i := |T_i|$. Очевидно, $(t_1,\dots,t_m)$ – решение соответствующей системы (8). Пусть $(t_1^0,\dots,t_m^0)$ – решение (8), полученное с помощью *Алгоритма* 4.1. Тогда для всех $k = 1..m$ верно $t_k^0 \le t_k$, поэтому для $k = 1..m$ существуют строки $T_k^0 := T_k|_{t_k^0}$. Покажем, что набор $(T_1^0, \dots, T_m^0)$ является решением системы (7).

Мы имеем: $A_kT_{i_k} \le B_kT_{j_k}$. Кроме того, $a_k + t_{i_k}^0 \le b_k + t_{j_k}^0$, где $a_k = |A_k|$ и $b_k = |B_k|$. Обозначим $\alpha_k := a_k + t_{i_k}^0, \beta_k := b_k + t_{j_k}^0$. Теперь $|A_kT_{i_k}| = a_k + t_{i_k} \ge a_k + t_{i_k}^0 = \alpha_k$, и аналогично $|B_kT_{j_k}| \ge \beta_k$, причем $\alpha_k \le \beta_k$. Тогда существуют строки $(A_kT_{i_k})|_{\alpha_k}$ и $(B_kT_{j_k})|_{\beta_k}$, и, кроме того, $(A_kT_{i_k})|_{\alpha_k} \le B_kT_{j_k}$, откуда заключаем, что $(A_kT_{i_k})|_{\alpha_k} \le (B_kT_{j_k})|_{\beta_k}$. Осталось заметить, что $(A_kT_{i_k})|_{\alpha_k} = A_kT_{i_k}^0$ и $(B_kT_{j_k})|_{\beta_k} = B_kT_{j_k}^0$, следовательно $A_kT_{i_k}^0 \le B_kT_{j_k}^0$ для всех $k = 1..m$. Значит, $(T_1^0, \dots, T_m^0)$ – решение (7).

По лемме 4.15 для всех $k = 1..m$ выполнено $|T_k^0| = t_k^0 \le \max\limits_i [|A_i| - |B_i|]^+(m-1)$. Таким образом, доказана следующая теорема:

Теорема 5.1. *Для разрешимой задачи квазиунификации* (4) *с одноместными функциональными знаками существует универсальное решение σ и соответствующие ему подстановки $\delta_1, \ldots, \delta_n$ такие, что:*

$$h[\sigma] \leq (m-1) \cdot \max_i \left[|A_i| - |B_i|\right]^+ ,$$

$$h[\delta_k] \leq (m-1) \cdot \max_i \left[|A_i| - |B_i|\right]^+ , k = 1..n.$$

где m – количество неизвестных и n – количество уравнений.

Доказательство. Оценка для $h[\sigma]$ следует из леммы 4.15, для $h[\delta_k]$ – из леммы 4.16. □

Для каждой неизвестной системы (4) определим следующую характеристику:

$$\delta[X_p] = \max\left\{[|A_k| - |B_k|]^+ \mid i_k = p\right\}$$

Теорема 5.2. *Для разрешимой задачи квазиунификации* (4) *с одноместными функциональными знаками существует универсальное решение σ и соответствующие ему подстановки $\delta_1, \ldots, \delta_n$ такие, что:*

$$h[\sigma] \leq \sum_{p=1}^{m} \delta[X_p],$$

$$h[\delta_k] \leq \sum_{p=1}^{m} \delta[X_p], k = 1..n,$$

где m – количество неизвестных и n – количество уравнений.

Доказательство. Следствие леммы 4.17. □

Осталось показать, как построить универсальное решение (6), при известном "минимальном" решении (8) $(t_1^0, \ldots, t_m^0)$.

Заметим, что ациклический направленный граф (V, R) (подграф G) задает на $x_1, \ldots, x_m$, а значит и на $S_1, \ldots, S_m$, частичный порядок (см. раздел 4). Будем перебирать $S_1, \ldots, S_m$ в этом порядке и последовательно строить $(Q_1, \ldots, Q_m)$ – решение (6): для каждой следующей неизвестной S_i либо $t_i^0 = 0$, тогда $Q_i := \Lambda$, либо для некоторого j, для которого строка Q_j уже построена, в (8) есть уравнение

$$a_k + x_j \leq b_k + x_i,$$

причем соответствующая этому неравенству дуга графа G входит в R, и стало быть (лемма 4.11) $a_k + t_j^0 = b_k + t_i^0$. В последнем случае в (7) есть неравенство

$$A_k S_j \leq B_k S_i.$$

Если $B_k \not\leq A_k Q_j$, то у (7) решения нет. В противном случае, Q_i определяется из равенства $A_k Q_j = B_k Q_i$ единственным образом (точнее, Q_i определяется единственным образом из неравенства $A_k Q_j \leq B_k Q_i$ при известном Q_j и условии $|A_k| + |Q_j| = |B_k| + |Q_i|$). Так мы полностью определим набор $(Q_1, \ldots, Q_m)$. Если этот набор не является решением (6), то (6) не имеет решения.

Таким образом мы либо определим неразрешимость (6), либо построим решение (6) $(Q_1, \ldots, Q_m)$ такое, что $|Q_i| = t_i^0$. Так как такое решение единственно, оно и является универсальным решением (6).

§6. "Почти одноместная" квазиунификация. Неформальное описание

Пусть требуется решить задачу квазиунификации для пар термов

$$\langle g^{q_1}(s_1^1, \ldots, s_{q_1}^1), g^{q_1}(t_1^1, \ldots, t_{q_1}^1)\rangle, \ldots, \langle g^{q_p}(s_1^p, \ldots, s_{q_p}^p), g^{q_p}(t_1^p, \ldots, t_{q_p}^p)\rangle,$$

где g^q – q-местный функциональный знак, и все s_i^j и t_i^j содержат только неизвестные и одноместные функциональные знаки. Будем называть такую систему (и соответствующую задачу квазиунификации) *почти одноместной*.

Необходимо найти подстановки σ, δ_1, ... ,δ_p такие, что для $k = 1..p$ выполняется графическое равенство:

$$g^{q_k}(s_1^k, \ldots, s_{q_k}^k)\sigma\delta_k = g^{q_k}(t_1^k, \ldots, t_{q_k}^k)\sigma. \tag{9}$$

Ясно, что равенство (9) эквивалентно следующей системе равенств:

$$\begin{cases} s_1^k \sigma\delta_k = t_1^k \sigma \\ \ldots \\ s_{q_k}^k \sigma\delta_k = t_{q_k}^k \sigma. \end{cases} \tag{10}$$

Объединяя эти системы для всех $k = 1..p$, получаем систему в термах из $q_1 + \cdots + q_p$ уравнений.

Используя модификации определения терма и подстановки из предыдущего раздела, мы можем построить эквивалентную систему в словах и символах:

$$\begin{cases} A_l^k S(X_{i_l^k}) D_k(s(X_{i_l^k})) = B_l^k S(X_{j_l^k}) \\ d_k(s(X_{i_l^k})) = s(X_{j_l^k}) \\ k = 1..p,\ l = 1..q_k. \end{cases} \tag{11}$$

Мы будем говорить, что уравнения (11) с верхними индексами k для некоторого k *образуют k-ю группу*.

Основное отличие этой системы от системы (5) в том, что подстановка (D_k, d_k) общая для всех уравнений k-й группы, тогда как в (5) эти подстановки были различны для всех уравнений.

Для удобства обозначим $n := q_1 + \cdots + q_p$ и сменим нумерацию уравнений и неизвестных в системе: заменим A_l^k на A_{Q_k+l}, B_l^k на B_{Q_k+l}, i_l^k на i_{Q_k+l}, j_l^k на j_{Q_k+l}, где $Q_k = \sum_{i=1}^{k-1} q_i$. Очевидно, теперь r-е уравнение принадлежит k-й группе тогда и только тогда, когда $Q_k < r \le Q_{k+1}$.

Система (11) после переобозначений выглядит так:

$$\begin{cases} A_1 S(X_{i_1}) D_1(s(X_{i_1})) = B_1 S(X_{j_1}) \\ \quad \dots \\ A_n S(X_{i_n}) D_p(s(X_{i_n})) = B_n S(X_{j_n}) \\ d_1(s(X_{i_1})) = s(X_{j_1}) \\ \quad \dots \\ d_p(s(X_{i_n})) = s(X_{j_n}). \end{cases} \tag{12}$$

Для сведения системы (12) к системе уравнений в словах мы рассмотрим символьную часть этой системы, т.е. уравнения над символами:

$$\begin{cases} d_1(s(X_{i_1})) = s(X_{j_1}) \\ \quad \dots \\ d_p(s(X_{i_n})) = s(X_{j_n}). \end{cases} \tag{13}$$

Так как d_k для $k = 1..p$ может участвовать более чем в одном уравнении (13), мы не можем поступить так же, как в одноместном случае, просто положив $s(X_i) := X_i$ и $d_k(s(X_{i_t})) := s(X_{j_t})$.

Мы построим отношение эквивалентности “$\simeq$” на $X_1, \ldots, X_m$ такое, что $X_i \simeq X_j$ тогда и только тогда, когда необходимым условием для решения системы (13) является $s(X_i) = s(X_j)$. Теперь $X_1, \ldots, X_m$ разбиваются на f классов эквивалентности по “$\simeq$”. Построив s^* так, чтобы $s^*(X_i) = s^*(X_j) \iff X_i \simeq X_j$ и определив $d_1^*, \ldots, d_p^*$ из системы (13), мы покажем, что можно ограничиться поиском решений (12), символьная часть которых совпадает с $(s^*, d_1^*, \ldots, d_p^*)$.

Подставляя найденное нами s^* в (12) и вводя соответствующие обозначения, мы получим следующую систему уравнений в словах:

$$\begin{cases} A_1 S_{i_1} D_{k_1} \doteq B_1 S_{j_1} \\ \quad \ldots \\ A_n S_{i_n} D_{k_n} \doteq B_n S_{j_n} \end{cases} \tag{14}$$

для неизвестных S_i, D_k с константными строками $A_1, \ldots, A_n, B_1, \ldots, B_n$. Для начала, приведем систему (14) к виду, когда $A_i \doteq \Lambda$ для $i = 1..n$. Для этого решим более слабую систему неравенств:

$$\begin{cases} A_1 S_{i_1} \leq B_1 S_{j_1}, \\ \quad \ldots \\ A_n S_{i_n} \leq B_n S_{j_n} \end{cases} \tag{15}$$

Системы такого вида мы решали при рассмотрении одноместной квазиунификации. Пусть $(\widetilde{S}_1, \ldots, \widetilde{S}_n)$ – решение (15). Подставив в (14) выражения $\widetilde{S}_i T_i$ вместо S_i (здесь $T_1, \ldots, T_m$ – новые неизвестные) и выполнив ставшие после этого возможными сокращения, мы получим систему в *приведенной форме*:

$$\begin{cases} T_{i_1} D_{k_1} \doteq P_1 T_{j_1} \\ \quad \ldots \\ T_{i_n} D_{k_n} \doteq P_n T_{j_n} \end{cases} \tag{16}$$

с неизвестными T_i и D_k.

Далее мы будем решать (16) итеративно, получая на каждом шаге систему в приведенной форме с меньшим числом неизвестных и уравнений: мы покажем, что это всегда можно сделать, если в системе найдутся два уравнения с одним и тем же D_k в левой части. Таким образом, процесс упрощения системы остановится, когда в уравнениях (16) все D_k будут различны. Теперь заметим, что при этом условии очевидным универсальным решением (16) будет набор T_i и D_k такой, что $T_i = \Lambda$ и $D_{k_t} = P_t$. Так как при получении каждой новой системы мы выполняем вполне конкретные действия (а именно, подстановки неизвестных), то универсальное решение исходной системы однозначно восстанавливается по этому набору.

В следующем разделе приводится формальное описание этих шагов и оценки высоты полученного решения. В частности, будет доказан следующий результат:

Утверждение. *Для имеющей решение почти одноместной задачи квазиунификации $\mathfrak{U}$ существует универсальное решение σ и соответствующие ему подстановки $\delta_1, \ldots, \delta_p$ такие, что:*

$$h[\sigma] \leq \delta[\mathfrak{U}](2^t m - 1),$$

$$h[\delta_k] \leq \delta[\mathfrak{U}]2^t m, k = 1..p.$$

где m – количество неизвестных, p – количество уравнений, $n = q_1 + \cdots + q_p$, $t = \min\{m-1, n-p\}$, $\delta[\mathfrak{U}]$ – величина, не превосходящая максимальной высоты термов в $\mathfrak{U}$.

§7. "Почти одноместная" квазиунификация

Рассмотрим символьную часть системы (12), т.е. систему

$$\begin{cases} d_1(s(X_{i_1})) = s(X_{j_1}) \\ \quad \ldots \\ d_p(s(X_{i_n})) = s(X_{j_n}). \end{cases} \tag{17}$$

Мы построим "символьные" подстановки s^*, d_1^*, ..., d_p^* такие, что если (12) разрешима, то существует универсальное решение (12) с такими подстановками.

Исходя из (17), построим на $X_1, \ldots, X_m$ отношение эквивалентности "$\simeq$" по следующим правилам:

$$1.\ \frac{X_i = X_j}{X_i \simeq X_j} \qquad 2.\ \frac{X_{i_l} \simeq X_{i_r},\ Q_k < l \leq Q_{k+1},\ Q_k < r \leq Q_{k+1}}{X_{j_l} \simeq X_{j_r}}$$

$$3.\ \frac{X_i \simeq X_j,\ X_j \simeq X_k}{X_i \simeq X_k}$$

Лемма 7.1. *Если s, $d_1, \dots, d_p$ – решение* (17) *и $X_i \simeq X_j$, то $s(X_i) = s(X_j)$.*

Доказательство. Будем доказывать по индукции по длине вывода отношения $X_i \simeq X_j$. База соответствует правилу 1: если $X_i = X_j$, то, очевидно, $s(X_i) = s(X_j)$.

Пусть последним при выводе применялось правило 2. Значит для некоторых l и r $X_i = X_{j_l}$, $X_j = X_{j_r}$ и найдется k такое, что $Q_k < l, r \leq Q_{k+1}$. Это значит, что l-е и r-е уравнения принадлежат k-й группе:

$$\begin{cases} \quad\dots \\ d_k(s(X_{i_l})) = s(X_{j_l}) \\ \quad\dots \\ d_k(s(X_{i_r})) = s(X_{j_r}) \\ \quad\dots \end{cases}$$

По индукционному предположению $s(X_{i_l}) = s(X_{i_r})$, значит $s(X_i) = s(X_{j_l}) = d_k(s(X_{i_l})) = d_k(s(X_{i_r})) = s(X_{j_r}) = s(X_j)$.

Для правила 3 индукционный переход очевиден. □

Вернемся к решению системы (12).

Пусть построенное нами отношение "$\simeq$" разбивает множество $X_1, \dots, X_m$ на f классов эквивалентности $\Phi_1, \dots, \Phi_f$. Очевидно, $f \leq m$. Положим $s^*(X_l) = X_r$, если $X_l \in \Phi_r$. Кроме того, положим $d_k^*(X_l) = s^*(X_{j_r})$, если $X_{i_r} \in \Phi_l$ и r-е уравнение принадлежит k-й группе. Корректность последнего определения требует доказательства:

Лемма 7.2. *Если для некоторых l, r и q $X_{i_r} \in \Phi_l$ и $X_{i_q} \in \Phi_l$, причем r-е и q-е уравнения принадлежат одной группе, то $s^*(X_{j_r}) = s^*(X_{j_q})$.*

Доказательство. Из условия следует, что $X_{i_r} \simeq X_{i_q}$ и найдется k такое, что $Q_k < i_r, i_q \leq Q_{k+1}$. Тогда по правилу 2 построения "$\simeq$" заключаем, что $X_{j_r} \simeq X_{j_q}$, стало быть $s^*(X_{j_r}) = s^*(X_{j_q})$. □

Теорема 7.1. *Пусть $(S, s, D_1, d_1, \dots, D_p, d_p)$ – решение системы* (12). *Тогда можно построить $S^*, D_1^*, \dots, D_p^*$ такие, что $(S^*, s^*, D_1^*, d_1^*, \dots, D_p^*, d_p^*)$ – решение* (12), *причем (S^*, s^*) – более общая подстановка, чем (S, s).*

Доказательство. Определим $S^*, D_1^*, \dots, D_p^*$ следующим образом:

$S^*(X_k) = S(X_k)$ для всех $k = 1..m$.

$D_k^*(X_l) = D_k(s(X_r))$, где $X_r \in \Phi_l$. Это определение корректно, так как если $X_r \in \Phi_l$ и $X_q \in \Phi_l$, то $X_r \simeq X_q$ и, следовательно, $s(X_r) = s(X_q)$.

Подстановкой в (12) убеждаемся, что $(S^*, s^*, D_1^*, d_1^*, \dots, D_p^*, d_p^*)$ – действительно решение (12). Теперь пусть $P(X_k) = \Lambda$ для все k и $p(X_k) = s(X_l)$,где $X_l \in \Phi_k$ (корректность показывается аналогично). Тогда (обозначаем "$\circ$" композицию подстановок) $(S^*, s^*) \circ (P, p) = (S^*, s^* \circ p) = (S, s)$, так как если $X_k \in \Phi_l$, то $p(s^*(X_k)) = p(X_l) = s(X_k)$. То есть, (S^*, s^*) – более общая подстановка, чем (S, s). $\square$

Будем искать решение (12) при известных $s^*, d_1^*, \dots, d_p^*$. Обозначим $S_k = S(X_k), k = 1..m$ и $D_{(r,l)} = D_r(s^*(X_{i_q}))$, $l = 1..f$, $r = 1..p$, где q-е уравнение принадлежит r-й группе и $X_{i_q} \in \Phi_l$ (т.е. $s^*(X_{i_q}) = X_l$). Рассмотрим систему уравнений в словах с неизвестными $S_1, \dots, S_m, D_{1,1}, \dots, D_{p,f}$:

$$\begin{cases} A_1 S_{i_1} D_{k_1} = B_1 S_{j_1} \\ \quad \dots \\ A_n S_{i_n} D_{k_n} = B_n S_{j_n}, \end{cases} \tag{18}$$

где $1 \leq i_q, j_q \leq m$, а k_q – обозначение для (r_q, l_q), где $1 \leq r_q \leq p$ и $1 \leq l_q \leq f$.

Ясно, что решив систему (18), мы получим отображения $S^*, D_1^*, \dots, D_p^*$ такие, что $(S^*, s^*), (D_1^*, d_1^*), \dots, (D_p^*, d_p^*)$ – решение (12). При этом универсальному (т.е. самому короткому покомпонентно в смысле отношения "$\leq$" для строк) решению (18) будет соответствовать универсальное решение задачи квазиунификации (12). Это можно показать так же, как в предыдущем разделе для случая одноместных функциональных знаков.

Займемся решением системы (18).

Лемма 7.3. *Пусть $(S_1, \dots, S_m, D_{1,1}, \dots, D_{p,f})$ – решение (18). Тогда $(S_1, \dots, S_m)$ – решение системы неравенств (7) (см. раздел 5).*

Доказательство. Очевидно из определения отношения "$\leq$" для строк. $\square$

Из леммы 7.3 следует, что если $(S_1, \dots, S_m, D_{1,1}, \dots, D_{p,f})$ – решение (18) и $\widetilde{S}_1, \dots, \widetilde{S}_m$ – универсальное решение (7), то найдутся строки $T_1, \dots, T_m$ такие, что $S_k = \widetilde{S}_k T_k$ для $k = 1..m$. Поэтому нахождение $(S_1, \ldots, S_m, D_{1,1}, \ldots, D_{p,f})$ сводится к нахождению $(T_1, \ldots, T_m, D_{1,1}, \ldots, D_{p,f})$.

$(\widetilde{S}_1, \ldots, \widetilde{S}_m)$ – решение (7), значит найдутся строки $P_1, \ldots, P_n$ такие, что $(\widetilde{S}_1, \ldots, \widetilde{S}_m, P_1, \ldots, P_n)$ – решение (6), то есть $A_k \widetilde{S}_{i_k} P_k = B_k \widetilde{S}_{j_k}$. Подставив в (18) $S_k = \widetilde{S}_k T_k$ и используя равенства системы (6), мы получим систему в словах для неизвестных $T_1, \ldots, T_m, D_{1,1}, \ldots, D_{p,f}$, которая после сокращения слева (свойство 1 раздела 1) t-го уравнения на $A_t \widetilde{S}_{i_t}$, $t = 1..n$, будет выглядеть так:

$$\begin{cases} T_{i_1} D_{k_1} = P_1 T_{j_1} \\ \quad \ldots \\ T_{i_n} D_{k_n} = P_n T_{j_n}. \end{cases} \tag{19}$$

Назовем систему вида (19) *системой в приведенной форме*, а описанную процедуру *приведением системы*.

Очевидно, решение (18) получается из решения (19) приписыванием для всех k строк $\widetilde{S}_k$ слева к T_k.

Зададим на $T_1, \ldots, T_m$ отношение "$\simeq_0$" по следующим правилам:

$$1.\ \frac{T_i = T_j}{T_i \simeq_0 T_j} \qquad 2.\ \frac{T_{i_l} \simeq_0 T_{i_r},\ k_l = k_r}{T_{j_l} \simeq_0 T_{j_r}} \qquad 3.\ \frac{T_i \simeq_0 T_j,\ T_j \simeq_0 T_k}{T_i \simeq_0 T_k}$$

Лемма 7.4. $T_i \simeq_0 T_j \iff X_i \simeq X_j$.

Доказательство. Пусть $T_i \simeq_0 T_j$. Будем доказывать $X_i \simeq X_j$ по индукции по длине вывода $T_i \simeq_0 T_j$.

База: $T_i \simeq_0 T_j$ получено применением правила 1. Тогда $T_i = T_j$, значит $i = j$, откуда по правилу 1 для "$\simeq$" получаем $X_i \simeq X_j$. Пусть вывод $T_i \simeq_0 T_j$ заканчивается применением правила 3. Тогда по индукции выводимы $X_i \simeq X_k$ и $X_k \simeq X_j$, следовательно, выводимо $X_i \simeq X_j$. Если же $T_i \simeq_0 T_j$ получено с помощью 2, то для некоторых l и r верно $i = j_l$ и $j = j_r$. По индукционному предположению существует вывод $X_{i_l} \simeq X_{i_r}$ и, кроме того, $k_l = k_r$, что означает, что l-е и r-е уравнения принадлежат t-й группе для некоторого t, то есть $Q_t < i_l, i_r \leq Q_{t+1}$. Поэтому можно, применив правило 2 для "$\simeq$" к доказанному $X_{i_l} \simeq X_{i_r}$ получить $X_{j_l} \simeq X_{j_r}$.

Похожим образом доказываем, что $X_i \simeq X_j \Rightarrow T_i \simeq_0 T_j$. База и индукционный переход для правила 3 получаются аналогично. Если вывод $X_{j_l} \simeq X_{j_r}$ заканчивается применением правила 2, то l-е и r-е уравнения принадлежат t-й группе для некоторого t и $X_{i_l} \simeq X_{i_r}$. Стало быть найдется такое q $(1 \leq q \leq f)$, что $s^*(X_{i_l}) = s^*(X_{i_r}) = X_q$, а значит при переходе от (12) к (18) уравнения

$$A_l S(X_{i_l}) D_t(s(X_{i_l})) = B_l S(X_{j_l}) \text{ и } A_r S(X_{i_r}) D_t(s(X_{i_r})) = B_l S(X_{j_r})$$

заменяются на

$$A_l S_{i_l} D_{t,q} = B_l S_{j_l} \text{ и } A_r S_{i_r} D_{t,q} = B_r S_{j_r}$$

поэтому $k_l = k_r = (t, q)$. Кроме того, по индукционному предположению $T_{i_l} \simeq_0 T_{i_r}$, значит мы можем применить правило 2 и получить $T_{j_l} \simeq_0 T_{j_r}$. $\square$

Лемма 7.5. *Если для некоторых t и q выполнено $T_t \simeq_0 T_q$ и $T_t \neq T_q$, то найдутся такие l и r, что $i_l = i_r$, $k_l = k_r$, $T_{j_l} \simeq_0 T_{j_r}$ и $j_l \neq j_r$.*

Доказательство. Рассмотрим вывод $T_t \simeq_0 T_q$. Заменим в нем все применения правила 2, для которых $j_l = j_r$ (а значит, $T_{j_l} = T_{j_r}$), на применения правила 1 для T_{j_l} и T_{j_r}. Вывод при этом останется корректным. В результате останется хотя бы одно применение правила 2, иначе было бы $T_t = T_q$. Возьмем самое первое из них. Пусть оно имеет вид

$$\frac{T_{i_l} \simeq_0 T_{i_r},\ k_l = k_r}{T_{j_l} \simeq_0 T_{j_r}.}$$

Эквивалентность $T_{i_l} \simeq_0 T_{i_r}$ получена только с помощью правил 1 и 3, поэтому $T_{i_l} = T_{i_r}$, т.е. $i_l = i_r$. Кроме того, $k_l = k_r$ и $j_l \neq j_r$. Осталось заметить, что у нас имеется вывод $T_{j_l} \simeq_0 T_{j_r}$. $\square$

Лемма 7.6. *Если $k_l = k_r$, то $T_{i_l} \simeq_0 T_{i_r}$.*

Доказательство. Пусть $k_l = k_r = (t, q)$. По определению, $D_{k_l} = D_t(s^*(X_{i_l}))$, $D_{k_r} = D_t(s^*(X_{i_r}))$, значит $s^*(X_{i_l}) = s^*(X_{i_r}) = X_q$, то есть $X_{i_l} \simeq X_{i_r}$, значит $T_{i_l} \simeq_0 T_{i_r}$. $\square$

Из леммы 7.6 следует, что правило 2 для “$\simeq_0$” можно заменить на следующее более сильное:

$$\frac{k_l = k_r}{T_{j_l} \simeq_0 T_{j_r}},$$

однако лемму 7.5 удобнее доказывать именно для такого более слабого вывода отношения “$\simeq_0$”.

Теперь, пусть для (19) найдутся l и r такие, что $k_l = k_r$ и $T_{j_l} \neq T_{j_r}$. Тогда (лемма 7.6) выполнено $T_{i_l} \simeq_0 T_{i_r}$ и, следовательно, (правило 2 для "$\simeq_0$") выполнено $T_{j_l} \simeq T_{j_r}$. Значит (лемма 7.5), в (19) найдутся два уравнения следующего вида:

$$\begin{cases} \quad \dots \\ T_g D_{t,q} = P_{r_1} T_{p_1}, \\ \quad \dots \\ T_g D_{t,q} = P_{r_2} T_{p_2}, \\ \quad \dots \end{cases} \tag{20}$$

Если (18), а значит и (19), разрешима, то найдется такой набор строк $(T_1^*, \dots, T_m^*, D_{1,1}^*, \dots, D_{p,f}^*)$, что уравнения (19) превращаются в верные графические равенства, в частности,

$$T_g^* D_{t,q}^* = P_{r_1} T_{p_1}^* \quad \text{и} \quad T_g^* D_{t,q}^* = P_{r_2} T_{p_2}^*$$

Из этого заключаем, что $P_{r_1} T_{p_1}^* = P_{r_2} T_{p_2}^*$ для любого решения (19). По лемме 4.1, P_{r_1} и P_{r_2} сравнимы, пусть для определенности $P_{r_1} = P_{r_2} C$ для некоторой строки C. Тогда $C T_{p_1}^* = T_{p_2}^*$. Таким образом, в любом решении (19) строка $T_{p_2}^*$ однозначно определяется через $T_{p_1}^*$, следовательно, в (19) мы можем везде заменить T_{p_2} на $C T_{p_1}$ и решать новую систему, в которой переменных будет на одну меньше. При этом решение старой системы очевидным образом восстанавливается по решению новой.

Заметим, что в новой системе число уравнений также будет на единицу меньше: одно из уравнений, указанных в (20), можно убрать, так как после подстановки, ввиду $P_{r_1} = P_{r_2} C$, они будут совпадать.

Описанную процедуру назовем *сокращением* системы (19).

Итак, мы получили новую систему, с числом неизвестных и уравнений на единицу меньше, чем в исходной. Однако, полученная система не находится в приведенной форме: если в каком-то уравнении старой системы T_{p_2} стояла в левой части, то после процедуры сокращения это уравнение будет выглядеть так:

$$C T_{p_1} D_{t',q'} = P_{r_3} T_{p_3}$$

Применив процедуру *приведения* (лемма 7.3), мы получим систему в приведенной форме, то есть систему вида (19).

Нетрудно убедиться, что универсальное решение новой системы будет соответствовать универсальному решению старой, и наоборот.

Итак, пусть у нас есть приведенная система $\mathfrak{U}_0$, на неизвестных которой задано отношение "$\simeq_0$". С помощью *сокращения* и последующего *приведения* мы получим приведенную систему $\mathfrak{U}_1$, на неизвестных которой можно по тем же, что и для "$\simeq_0$", правилам задать отношение "$\simeq_1$".

Замечание. Мы отожествляем неизвестные $\mathfrak{U}_t$ и $\mathfrak{U}_{t+1}$, обозначая их T_i. На самом деле T_i из $\mathfrak{U}_t$ находится с T_i из $\mathfrak{U}_{t+1}$ в том же отношении, что и S_i из (18) с T_i из (19).

Лемма 7.7. *Если T_i и T_j являются переменными $\mathfrak{U}_{t+1}$, то*

$$T_i \simeq_{t+1} T_j \iff T_i \simeq_t T_j$$

.

Доказательство. Допустимый вывод $T_i \simeq_{t+1} T_j$ является допустимым выводом $T_i \simeq_t T_j$.

Вывод $T_i \simeq_t T_j$ можно перестроить в вывод $T_i \simeq_{t+1} T_j$ следующим образом: если при сокращении производилась подстановка $T_{p_2} \to CT_{p_1}$, то заменим в выводе все вхождения T_{p_2} на вхождения T_{p_1}. Если при сокращении q_1-е уравнение оказалось после подстановки совпадающим с q_2-м и было выкинуто из системы, то во всех применениях правила 2 для "$\simeq_t$" заменим $i_{q_1}, j_{q_1}, k_{q_1}$ на $i_{q_2}, j_{q_2}, k_{q_2}$ соответственно. Нетрудно видеть, что в результате такой замены мы получим допустимый вывод $T_i \simeq_{t+1} T_j$. $\square$

Таким образом, для $\mathfrak{U}_1$ будет справедливы леммы 7.5 и 7.6, а значит, определены процедуры приведения и сокращения. С их помощью мы получим $\mathfrak{U}_2$ с "$\simeq_2$" и т.д. Заметим, что эти процедуры не могут применяться более $\min\{m-1, n-p\}$ раз, так как в (19) всего лишь m неизвестных и n уравнений, причем в любой группе (а групп изначально p) не может остаться меньше одного уравнения (сокращение происходит всегда по двум уравнениям одной группы).

Пусть процесс остановился на системе $\mathfrak{U}_t$ вида (19). Если в $\mathfrak{U}_t$ для каких-то l и r $k_l = k_r$, то $T_{i_l} \simeq_t T_{i_r}$ (лемма 7.6). Если $T_{i_l} \neq Ti_r$, то по лемме 7.5, систему $\mathfrak{U}_t$ можно сократить, что неверно. Значит, $T_{i_l} = T_{i_r}$. Кроме того, т.к. $\mathfrak{U}_t$ несократимая и

$k_l = k_r$, то $T_{j_l} = T_{j_r}$. Поэтому, если у $\mathfrak{U}_t$ есть решение, а это следует из разрешимости исходной системы, то l-е и r-е уравнения совпадают, значит одно из них можно выкинуть. Таким образом, после всех таких выкидываний (не меняющих множество решений системы) останется система $\mathfrak{U}_{t+1}$, в которой для всех $l \neq r$ выполнено $k_l \neq k_r$. Если теперь n' – число уравнений в $\mathfrak{U}_{t+1}$, m' – число неизвестных, то можно так перенумеровать D_{k_r} что $\mathfrak{U}_{t+1}$ будет выглядеть следующим образом:

$$\begin{cases} T_{i_1} D_1 = P_1 T_{j_1} \\ \quad \dots \\ T_{i_{n'}} D_{n'} = P_{n'} T_{j_{n'}}. \end{cases} \tag{21}$$

Очевидно, универсальным решением этой системы является набор $(T_1^*, \dots, T_{m'}^*)$ такой, что $T_i^* = \Lambda$, $i = 1..m'$. При этом $(D_1^*, \dots, D_{n'}^*) = (P_1, \dots, P_{n'})$.

Построим алгоритм решения задачи почти одноместной квазиунификации (11) и оценку на высоту универсального решения (11) (или, что то же, на длину строк универсального решения (18)).

Будем записывать подстановки в виде $\{T_1 \to C_1, \dots, T_m \to C_m\}$.

Пусть $\mathfrak{U}$ – система вида (18). Процедура ОКУ($\mathfrak{U}$) (Одноместная КвазиУнификация) возвращает:

1. $\emptyset$, если соответствующая $\mathfrak{U}$ система (7) неразрешима;

2. подстановку $\{S_1 \to \widetilde{S}_1 T_1, \dots, S_m \to \widetilde{S}_m T_m\}$, если существует $(\widetilde{S}_1, \dots, \widetilde{S}_m)$ – решение соответствующей системы (7). Здесь $T_1, \dots, T_m$ – новые неизвестные.

Процедура СократитьСлева($\mathfrak{U}$) выполняет сокращение каждого уравнения $\mathfrak{U}$ $A_i T_{i_1} D_{k_1} = B_i T_{j_1}$ на A_i слева.

Процедура Сократить($\mathfrak{U}, l, r$) производит сокращение $\mathfrak{U}$ по l-му и r-му уравнениям и возвращает:

1. $(\mathfrak{U}, \emptyset)$, если это невозможно;

2. $(\mathfrak{U}', \{T_i \to CT_j\})$, если возможно; здесь $\mathfrak{U}'$ – сокращенная система и при сокращении подставлялось CT_j вместо T_i.

Алгоритм 7.1

1. $\mathfrak{U}$ – система вида (18)
2. $\Sigma_0 :=$ *ОКУ*($\mathfrak{U}$)
3. **Если** $\Sigma_0 = \emptyset$, **то** КОНЕЦ: решения нет
4. $\mathfrak{U}_0 :=$ *СократитьСлева* ($\mathfrak{U}\Sigma_0$)

5. $v := 0$

6. $\mathfrak{U}_v$ – система вида (19) с n_v уравнениями с индексами $i_p^v, j_p^v, k_p^v, p = 1..n_v$

7. **Пока** *найдутся* $l \neq r$ *такие, что* $k_l^v = k_r^v$ *и* $T_{j_l^v} \neq T_{j_r^v}$ **выполнять**

8. $(\mathfrak{U}'_{v+1}, \Delta'_{v+1}) :=$ *Сократить* $(\mathfrak{U}_v, l, r)$

9. **Если** $\Delta'_{v+1} = \emptyset$, **то** КОНЕЦ: решения нет

10. $\Delta''_{v+1} :=$ *ОКУ* $(\mathfrak{U}'_{v+1})$

11. $\mathfrak{U}_{v+1} :=$ *СократитьСлева* $(\mathfrak{U}'_{v+1}\Delta''_{v+1})$

12. $\Sigma_{v+1} := \Sigma_v \circ \Delta'_{v+1} \circ \Delta''_{v+1}$

13. $v := v + 1$

14. **Все**

15. $\{T_1 \to \Lambda, \ldots, T_m \to \Lambda\} \circ \Sigma_v$ – решение $\mathfrak{U}$.

Если $\mathfrak{U}$ – система вида (18), то обозначим $\delta[\mathfrak{U}] = \max\limits_i [|A_i| - |B_i|]^+$ Очевидно, $\delta[\mathfrak{U}] = \max\limits_{1 \leq p \leq m} \delta[S_p; \mathfrak{U}]$, где $\delta[S_p; \mathfrak{U}]$ обозначена величина, введенная перед Теоремой 5.2, вычисленная по системе $\mathfrak{U}$.

$h[\Sigma_0] \leq \delta[\mathfrak{U}](m-1)$ по Теореме 5.1.

$h[\mathfrak{U}_0] \leq \delta[\mathfrak{U}\Sigma_0] \leq \delta[\mathfrak{U}] + h[\Sigma_0] \leq \delta[\mathfrak{U}]m$

$h[\mathfrak{U}'_{v+1}] \leq 2h[\mathfrak{U}_v]$, $\delta[\mathfrak{U}'_{v+1}] \leq h[\mathfrak{U}_v]$

$h[\Delta'_{v+1}] \leq h[\mathfrak{U}_v]$

Для $\mathfrak{U}'_{v+1}$: $\delta[T_p; \mathfrak{U}'_{v+1}] \neq 0$ может быть только для одной неизвестной T_p такой, что CT_p было подставлено в $\mathfrak{U}_v$ вместо T_q. Причем, очевидно, $\delta[T_p; \mathfrak{U}_v] \leq h[\mathfrak{U}_v]$. Поэтому по Теореме 5.2:

$h[\Delta''_{v+1}] \leq \sum\limits_p \delta[T_p; \mathfrak{U}'_{v+1}] \leq h[U_v]$.

$h[\mathfrak{U}_{v+1}] \leq \delta[\mathfrak{U}'_{v+1}\Delta''_{v+1}] \leq \delta[\mathfrak{U}'_{v+1}] + h[\Delta''_{v+1}] \leq 2h[\mathfrak{U}_v]$.

$h[\Sigma_{v+1}] \leq h[\Sigma_v] + h[\Delta'_{v+1}] + h[\Delta''_{v+2}] \leq h[\Sigma_v] + 2h[U_v]$.

Из $h[\mathfrak{U}_{v+1}] \leq 2h[\mathfrak{U}_v]$ и $h[\mathfrak{U}_0] \leq \delta[\mathfrak{U}]m$ заключаем, что $h[U_v] \leq 2^v \delta[\mathfrak{U}]m$. Тогда, учитывая, что $h[\Sigma_0] \leq \delta[\mathfrak{U}](m-1)$, получаем $h[\Sigma_v] \leq \delta[\mathfrak{U}](2^v m - 1)$.

Итак, доказана следующая теорема:

Теорема 7.2. *Для разрешимой почти одноместной задачи квазиунификации* (11) *существует универсальное решение* σ *и соответствующие ему подстановки* $\delta_1, \ldots, \delta_p$ *такие, что:*

$$h[\sigma] \leq \delta[\mathfrak{U}](2^t m - 1),$$

$$h[\delta_k] \leq \delta[\mathfrak{U}]2^t m, k = 1..p.$$

где m *– количество неизвестных,* p *– количество уравнений,* $n = q_1 + \cdots + q_p$ *и* $t = \min\{m-1, n-p\}$.

Доказательство. Вторая оценка следует из того, что последняя система, полученная в ходе работы алгоритма, выглядит как (6). □

Литература

1. Г. С. Маканин, *Проблемы разрешимости уравнений в свободной полугруппе.* Мат. сб., **103**, No. 2 (1977), 147–236.
2. В. П. Оревков, *Верхние оценки удлинения выводов при устранении сечений.* Зап. научн. семин. ЛОМИ, бф 176 (1988), 132–146.
3. В. П. Оревков, *Системы уравнений в термах с подстановками. Вопросы кибернетики. Сложность вычислений и прикладная математическая логика. М., Наука, 1988, 127–148.*
4. B. Konev, *Upper bound on the height of terms in proofs with cuts.* In Proceedings of First-order Theorem Proving–FTP'98 / 2nd International Workshop on First-order Theorem Proving, Vienna, Austria, 1998, 162–172.
5. J. A. Robinson, *A machine oriented logic based on resolution principle.* J. Assoc. Comput. Mach, **12** (1965), 23–41.
6. V. P. Orevkov, *Complexity of Proofs and Their Transformations in Axiomatic Theories.* Amer. Math. Soc., 1991.
7. M. Baaz, *Note on the Existence of Most General Semi-Unifiers.* Arith., proof theory and comput. complexity, Oxford University Press, 1993, 20–29.
8. M. Baaz, G. Salzer, *Semi-Unification and Generalizations of a Particularly Simple Form.* Lect. Notes Comp. Sci., 1995, 135–148.
9. A. J. Kfoury, J. Tiuryn, and P. Urzyczyn, *The Undecidability of the Semi-Unification Problem.* BUCS Tech Report, 1989.
10. P. Pudlák, *On a unification problem related to Kreisel's conjecture.* Commentationes Methematicae Universitatis Carolinae, **23, 9** (1988), 551–556.

Jijkoun V. Upper bounds on the height of terms in the solution of the semiunification problem.

In this paper we investigate on one decidable case of term semiunification problem, namely when all the functional symbols in the given terms have arity one, except, possibly, for outer symbols of terms, which have no restrictions. We propose an algorithm that builds a most general solution of the semiunification problem, and prove an upper bound on the height of this solution; the upper bound is linear by the height of terms in the given problem. Our method is to reduce the problem for terms to a special system of equations in free semigroups, and then to solve this system.

Санкт-Петербургское отделение
Математического института
им. В.А. Стеклова РАН
E-mail: valley@pdmi.ras.ru

Поступило 10 января 2001 г.