ՀԱՅԱՍՏԱՆԻ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИ
NATIONAL ACADEMY OF SCIENCES OF ARMENIA
ДОКЛАДЫ ԶԵԿՈՒՅՑՆԵՐ REPORTS

Том 109 2009 № 3

ПРИКЛАДНАЯ МАТЕМАТИКА

УДК 621.39.1: 519.34

А. А. Чубарян, А. С. Налбандян

Сравнение эффективности систем Фреге с различными модификациями правила подстановки

(Представлено чл.-кор. НАН РА И.Д. Заславским 11/V 2009)

Ключевые слова: *система Фреге, сложность вывода, правила подстановки с ограничением на глубину, полиномиальная эквивалентность, экспоненциальное ускорение*

1. Основные понятия и определения. Напомним общепринятые критерии сложностных характеристик выводов, методы сравнения эффективности различных систем доказательств классического исчисления высказываний, систем Фреге и различных модификаций правила подстановки. Длину формулы φ, определяемую как количество всех вхождений в нее логических связок, обозначим через $|\varphi|$. Очевидно, что линейной функцией от $|\varphi|$ оцениваются и полная длина формулы, понимаемая как количество всех символов, и количество вхождений переменных.

Каждая из рассматриваемых систем Ф содержит конечное множество схем аксиом и конечное множество схематически заданных правил вывода. Вывод в системе Ф (Ф-вывод) определяется как конечная последовательность формул, каждая из которых либо является аксиомой, либо получается из предыдущих по правилам вывода.

l-сложность (длина) вывода определяется как сумма длин всех формул вывода, t-сложность — как количество шагов вывода, l-сложность (t-сложность) формулы φ в системе Ф определяется как минимальное значение среди l-сложностей (t-сложностей) Ф-выводов формулы φ и обозначается через l_φ^Φ (t_φ^Φ).

Пусть Φ_1 и Φ_2 суть пропозициональные системы доказательств. Следуя [1], напомним понятие полиномиальной сводимости.

Определение 1. *Φ_1 $p - l$-сводится к Φ_2 ($\Phi_1 \preceq_l \Phi_2$), если существует такой полином $p(\ )$, что для любой тавтологии φ $l_\varphi^{\Phi_2} \leqslant p\left(l_\varphi^{\Phi_1}\right)$.*

Определение 2. *Φ_1 $p - l$-эквивалентна Φ_2 ($\Phi_1 \sim_l \Phi_2$), если $\Phi_1 \preceq_l \Phi_2$ и $\Phi_2 \preceq_l \Phi_1$.*

Понятие $p - l$-эквивалентности соответствует общепринятому понятию p-эквивалентности.

Аналогично вводятся понятия $p - t$-сводимости и $p - t$-эквивалентности.

Определение 3. *Φ_1 имеет экспоненциальное l-ускорение (t-ускорение) относительно Φ_2, если существует последовательность тавтологий φ_n таких, что $l_\varphi^{\Phi_2} > 2^{\theta\left(l_\varphi^{\Phi_1}\right)}$ $\left(t_\varphi^{\Phi_2} > 2^{\theta\left(t_\varphi^{\Phi_1}\right)}\right)$.*

Каждая система Фреге $\mathcal{F}$ содержит перечислимое множество пропозициональных переменных, некоторое конечное, функционально полное множество пропозициональных связок. $\mathcal{F}$ определяется конечным множеством схематически заданных правил вывода $\dfrac{A_1 A_2 \ldots A_k}{B}$ (при $k = 0$ соответствующее правило определяет схему аксиом). $\mathcal{F}$ непротиворечива и полна.

Подстановкой принято называть некоторое отображение $\sigma = \begin{pmatrix} \varphi_1 & \varphi_2 & \cdots & \varphi_s \\ p_1 & p_2 & \cdots & p_s \end{pmatrix}$, ($s \geqslant 1$), где p_i ($1 \leqslant i \leqslant s$) — пропозициональные переменные, а φ_i ($1 \leqslant i \leqslant s$) — пропозициональные формулы. Для произвольной формулы A через $A\sigma$ обозначается результат применения подстановки σ к формуле A, т. е. формула, получающаяся повсеместной заменой каждого вхождения переменных p_i, если таковые имеются, формулами φ_i, соответственно. Правило подстановки записывается в виде $\dfrac{A}{A\sigma}$.

Если количество переменных, для которых допустимы одновременная подстановка, не ограничено, то такое правило подстановки называется *мультипликативным*, а если заранее указывается некоторая константа $k \geqslant 1$ и каждый раз позволяется делать замену всех вхождений не более, чем k различных переменных, то имеется *k-ограниченное* правило подстановки. Для $k = 1$ подстановку принято называть единичной.

Глубину пропозициональной формулы φ, понимаемую в общепринятом смысле, обозначим через $d(\varphi)$. Подстановку σ назовем *m-глубинно-ограниченной*, если для некоторой константы $m \geqslant 0$, $d(\varphi_i) \leqslant m$ ($1 \leqslant i \leqslant s$). Подстановка называется *переименованием* при $m = 0$.

Для дальнейших рассмотрений мы зафиксируем конкретную систему Фреге $\mathcal{F}$. Систему, получаемую из $\mathcal{F}$ добавлением мультипликативного правила подстановки без каких-либо ограничений, обозначим через $S\mathcal{F}$. Системы, полученные при добавлении к $\mathcal{F}$ k-ограниченного правила подстановки или m-глубинно-ограниченного правила подстановки, будем обозначать соответственно через $S_k\mathcal{F}$ и $S^m\mathcal{F}$.

Отметим, что в силу полиномиальной эквивалентности как по длине, так и по шагам различных систем Фреге [2] наши результаты не зависят от выбора той или иной системы Фреге.

В [3-5] доказано, что

1) $\forall k \geqslant 1$ $S\mathcal{F} \sim_l S_k\mathcal{F}$,

2) $\forall k_1, k_2$ $(k_1, k_2 \geqslant 1)$ $S_{k_1}\mathcal{F} \sim_t S_{k_2}\mathcal{F}$,

3) $\forall k \geqslant 1$ $S\mathcal{F}$ имеет экспоненциальное t-ускорение относительно $S_k\mathcal{F}$,

4) $\forall k \geqslant 1$ $S\mathcal{F}$ имеет экспоненциальное t-ускорение относительно $\mathcal{F}$.

В настоящей работе исследованы системы Фреге с глубинно-ограниченными правилами подстановки и указано на их существенное отличие от систем с k-ограниченными правилами подстановки.

2. Основные результаты. В качестве исследуемой из технических соображений зафиксируем систему Фреге $\mathcal{F}$, использующую лишь связки $\supset$ и $\neg$ и основанную на следующих схемах аксиом:

$A \supset (B \supset A)$,

$(A \supset B) \supset ((A \supset (B \supset C)) \supset (A \supset C))$,

$(\neg A \supset B) \supset ((\neg A \supset \neg B) \supset A)$, где A, B и C — произвольные формулы,

и правиле вывода modus ponens.

Теорема.

1. $\forall m \geqslant 0$ $S\mathcal{F} \sim_l S^m\mathcal{F}$,

2. $\forall m_1, m_2$ $(m_1, m_2 \geqslant 1)$ $S^{m_1}\mathcal{F} \sim_t S^{m_2}\mathcal{F}$,

3. $\forall m \geqslant 1$ $S\mathcal{F}$ имеет экспоненциальное t-ускорение относительно $S^m\mathcal{F}$,

4. $\forall m \geqslant 1$ $S^m\mathcal{F}$ не имеет экспоненциального t-ускорения относительно $\mathcal{F}$.

Доказательство пункта 1 основано на результате Басса [6] о полиномиальной l-сводимости $S\mathcal{F}$ к $S^0\mathcal{F}$, аналогично которому доказывается полиномиальная l-сводимость $S^m\mathcal{F}$ к $S^0\mathcal{F}$ для любого $m \geqslant 0$. Для доказательства пункта 2 достаточно показать, что $S^m\mathcal{F} \sim_t S^1\mathcal{F}$ для любого $m \geqslant 1$, что доказывается "пошаговым" достроением m-глубинно-ограниченной подстановки 1-глубинно-ограниченными подстановками, вводя при необходимости новые переменные, как это делалось при доказательстве соответствующего утверждения для k-ограниченных подстановок в [3].

При доказательстве пункта 3 устанавливается, что для формул

$$\varphi_n = p_1 \supset (p_2 \supset (p_3 \supset (\ldots \supset (p_n \supset p_1)\ldots))) \; n \geqslant 2,$$

$$t^{S\mathcal{F}}_{\varphi_n} = O(\log_2 n) \quad \text{и} \quad t^{S^m\mathcal{F}}_{\varphi_n} = \Omega(n) \quad \text{для любого} \quad m \geqslant 1.$$

Доказательство пункта 4 основано i) на ряде свойств τ-множеств подформул произвольной формулы φ, введенных в [5], и ii) на установленных в [7] свойствах подстановок, обеспечивающих ускорение выводов. Следуя [5], для произвольной формулы φ определим τ-множество ее подформул следующим образом:

$\tau(\varphi) = \{\varphi\} \cup \tau_1(\varphi)$, где

$\tau_1(\varphi) = \emptyset$, если φ пропозициональная переменная,

$\tau_1(\varphi_1 \supset \varphi_2) = \tau(\varphi_2) \setminus \tau(\varphi_1)$,

$\tau(\neg\varphi_1) = \overline{\varphi_1}$.

Доказательство утверждения пункта 4 основано на следующих фактах.

а) Используя общепринятую $0-1$-нумерацию подформулы формулы φ, доказывается, что для произвольной тавтологии φ $\tau(\varphi)$ является подмножеством подформул, имеющих номера, состоящие из одних единиц;

б) $\tau(B) \subseteq \tau(A) \cup \tau(A \supset B)$;

в) $\tau(A\sigma) \subseteq \{\varphi \mid \exists\psi \in \tau(A)$ и $\varphi = \psi\sigma\}$;

г) "удвоение" количества шагов выводов при переходе от системы с подстановкой к системе без правила подстановки происходит лишь при применении и к A, и к $A\sigma$ одновременно какого-либо иного правила вывода, что сопровождается "удвоением" количества подформул τ-множества выводимой формулы, располагающихся в ней "матрешкой" в силу свойств а).

В силу утверждения пункта 2 доказательство пункта 4 достаточно провести для системы $S^1\mathcal{F}$, но при 1-глубинно-ограниченной подстановке с учетом а), б), в) количество подформул τ-множества формулы, выводимой согласно ситуации г), может возрасти лишь на единицу, что указывает на отсутствие у глубинно-ограниченного правила подстановки того преимущества, которое описано в [7] для подстановок без ограничений на глубины подставляемых формул, а формулы "матрешки" глубины n выводятся в системах Фреге за количество шагов, ограниченное полиномом от n.

Институт проблем информатики и автоматизации НАН РА

А. А. Чубарян, А. С. Налбандян

Сравнение эффективности систем Фреге с различными модификациями правила подстановки

По сложностным характеристикам выводов сравниваются системы Фреге классического исчисления высказываний, дополненные различными модификациями правила подстановки: общепринятой мультипликативной подстановкой, мультипликативной подстановкой с ограничением на глубины подставляемых формул и подстановкой с ограничением на количество различных переменных, вместо которых одновременно делаются подстановки. Доказывается, что по длине выводов системы с различными модификациями правила подстановки полиномиально эквивалентны, а по шагам выводов системы с мультипликативным правилом подстановки без ограничений имеют экспоненциальное ускорение по отношению к системам с ограниченными правилами подстановки. Последние для разных параметров фиксированного типа ограничений полиномиально эквивалентны и по шагам выводов. Доказано также, что, в отличие от известного факта экспоненциального ускорения количества шагов выводов при переходе от систем Фреге без подстановок к системам Фреге даже с единичной подстановкой, но без ограничения на глубины подтавляемых формул, переход к системам с глубинно-ограниченным правилом подстановки не может приводить к ускорению шагов выводов.

Ա. Ա. Չուբարյան, Հ. Ս. Նալբանդյան

Տարբեր մոդիֆիկացիաների փեղադրման կանոնով Ֆրեգեի համակարգերի էֆեկտիվության հետազոտում

Համեմատվում են արտածումների բարդության բնութագրիչները տարբեր մոդիֆիկացիաների տեղադրման կանոնով Ֆրեգեի համակարգերում: Դիտարկվում են բազմակի տեղադրությունները՝ առանց որեւէ սահմանափակման, եւ բազմակի տեղադրություններ՝ տեղադրվող բանաձեւերի խորության սահմանափակմամբ: Ապացուցվում է, որ, ըստ արտածման երկարության, երկու հիշյալ տիպի տեղադրություններով Ֆրեգեի համակարգերը բազմանդամորեն համարժեք են: Ըստ արտածումների քայլերի, բազմանդամորեն համարժեք են տարբեր մեծություններով սահմանափակված խորությամբ տեղադրման կանոններով համակարգերը, մինչդեռ վերջիններիս նկատմամբ, առանց սահմանափակման տեղադրման կանոնով համակարգերը, ըստ քայլերի քանակի, ունեն ցուցչային արագացում:

Ապացուցված է նաեւ, որ, ի տարբերություն անսահմանափակ, նույնիսկ եզակի տեղադրման կանոնի, սահմանափակ խորությամբ տեղադրման կանոնը ի վիճակի չէ ապահովել ցուցչային արագացում առանց տեղադրման կանոնի Ֆրեգեի համակարգերի նկատմամբ:

A. A. Chubaryan, A. S. Nalbandyan

Comparison of the Efficiency of Frege Systems with Different Modifications of the Substitution Rule

We compare the proof in Frege systems with substitution rule without any restrictions and with depth-restricted substitution rule. We prove that any two depth-restricted substitution Frege systems are polynomially equivalent both by size and by steps. Frege

system with ordinary substitution rule and Frege system with depth-restricted substitution rule are also polynomially equivalent by size, but the first system has exponential speed-up over the second system by steps.

We also prove that the depth-restricted substitution rule cannot guarantee the exponential speed-up by steps over the Frege systems without substitution rule.

Литература

1. *Cook S. A., Reckhow A. R.* - Journal of Symbolic Logic. 1979. V. 44. P. 36-50.

2. *Pudlak P.* The Lengths of Proofs. Handbook of proof theory. North-Holland. 1998. P. 547-637.

3. *Chubaryan An. A., Chubaryan Arm. A., Aleksanyan S. R.* In: Mathematical Problems of Computer Science 30. Yerevan. 2008. P. 36-39.

4. *Чубарян А. А.* В сб.: Матем. вопр. кибернетики. Вып. 14. М. Физмат. 2005. С. 49-56.

5. *Цейтин Г. С., Чубарян А. А.* В сб.: Матем. вопр. кибернетики. и вычислит. техники. Ереван. Изд-во. АН АрмССР. 1975. С. 57-64.

6. *Buss S. R.* - Arch. Math. Logic. 1995. V. 34. P. 377-394.

7. *Чубарян А. А.* - Изв. НАН РА. Математика. 2000. Т. 35. N5. С. 21-29.