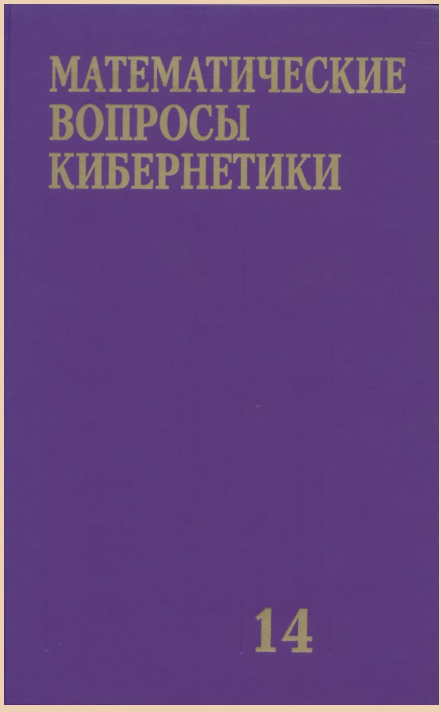
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 14



А. А. Чубарян

О сложности выводов в некоторых системах классического исчисления высказываний

Рекомендуемая форма библиографической ссылки: Чубарян А. А. О сложности выводов в некоторых системах классического исчисления высказываний // Математические вопросы кибернетики. Вып. 14. — М.: Физматлит, 2005. — С. 49–56. URL: http://library.keldysh.ru/mvk.asp?id=2005-49

О СЛОЖНОСТИ ВЫВОДОВ В НЕКОТОРЫХ СИСТЕМАХ КЛАССИЧЕСКОГО ИСЧИСЛЕНИЯ ВЫСКАЗЫВАНИЙ

А. А. ЧУБАРЯН

(ЕРЕВАН, АРМЕНИЯ)

В работе исследованы сложностные характеристики выводов в системах Фреге и в системах Фреге с правилом подстановки (единичной и мультипликативной). Для произвольной тавтологии φ введено понятие минимально-определяющей дизъюнктивной нормальной формы $\left(\mathscr{D}_{\varphi}^{min}\right)$ и доказано, что количество шагов кратчайшего вывода тавтологии φ в произвольной системе Фреге не превышает $c \cdot s \cdot l$, где s параметр характеризующий $\mathscr{D}_{\varphi}^{min}$, l — длина формулы φ и c — некоторая константа, зависящая от выбора системы Фреге. При этом указывается, что для произвольного n можно указать последовательность формул длины n, для которых параметр s имеет соответственно порядок n, n^2, n^3, ..., $n^{[\sqrt{n}\log_n 2]}$. В работе доказано также, что существует последовательность тавтологий длины n, для которых и в системах Фреге и в системах Фреге с правилом подстановки оценки количества шагов формул и общей длины выводов имеют порядок n и n^2 соответственно. Доказано также, что существуют тавтологии длины n, выводимые с единичной подстановкой не менее, чем за n шагов, а с мультипликативной подстановкой не более, чем за $\log_2 n$ шагов.

Введение

В обзорах [5, 8, 9] по теории сложности выводов указывается, что для классического исчисления высказываний (КИВ) экспоненциальные нижние оценки сложностей выводов формул фиксированной длины известны лишь в секвенциальных системах без правила сечения, в системах с правилом резолюции и в системах, в которых выводятся формулы в дизъюнктивных нормальных формах (д.н.ф.) и конъюктивных нормальных формах (к.н.ф.) с использованием лишь формул ограниченной глубины. В системах Фреге ($\mathscr{F}$) при тривиальной экспоненциальной верхней оценке сложностей выводов получены лишь линейные (для количества шагов) и квадратичные (для длины выводов) нижние оценки. Наличие даже таковых оценок для систем Фреге с правилом подстановки ($S\mathscr{F}$) авторы указанных обзоров отмечают в качестве открытых проблем.

Автором настоящей работы ранее были определены две системы доказательств классического исчисления высказываний: система $\mathscr{C}$ гильбертовского типа без правила сечения [4] и система $\mathscr{E}$, направленная на установление тавтологичности некоторой д.н.ф., строящейся по произвольной формуле [6]. Были описаны последовательности тавтологий длины n такие,

что сложности их выводов и в системе $\mathscr{C}$ и в системе $\mathscr{E}$ равны по порядку n, n^2, n^3, ..., $2^{\frac{n}{2}}$. Была доказана также полиномиальная эквивалентность этих двух систем, системы резолюций и секвенциальных систем без правила сечения, что позволило перенести вышеуказанные результаты для систем $\mathscr{C}$ и $\mathscr{E}$ и на последние две системы [7].

Интересна возможность перенесения этих результатов на иные системы КИВ.

В настоящей работе выводы в системе $\mathscr{E}$ моделируются в системах Фреге. На основе введённого в [6] понятия минимально-определяющей д.н.ф. $\left(\mathscr{D}_{\varphi}^{min}\right)$ для произвольной тавтологии (твт) φ доказывается, что каждая твт φ выводима в произвольной системе Фреге не более, чем за $c \cdot s \cdot l$ шагов, где $s = S(\varphi)$ — сложность вывода пустого конъюнкта из $\mathscr{D}_{\varphi}^{min}$, l — длина φ, c — константа, зависящая от выбора системы Фреге.

Показано также, что для достаточно большого n и каждого p $\left(1 \leqslant p \leqslant \left[\sqrt{n} \log_n 2\right]\right)$ существуют формулы φ_p^n, длины которых имеют порядок n, а $S(\varphi_p^n) = n^p$, следовательно, в системах Фреге выстраивается вышеупомянутая иерархия формул по верхним оценкам сложностей выводов.

В работах [5, 10] обсуждается вопрос получения нижних оценок количества шагов выводов в системах Фреге с подстановками. В частности, Басс в [5] указывает в качестве открытой проблему получения суперлогарифмической нижней оценки количества шагов выводов в $S\mathscr{F}$. Ургарт в [10] доказал, что не могут не существовать формулы с длиной $\theta(n)$, количества шагов выводов которой в $S\mathscr{F}$ не менее $\theta(n \log n)$. Однако еще в 1981 г. в качестве некоего вспомогательного результата нами была получена линейная нижняя оценка количества шагов выводов в классической, интуиционистской и минимальной системах исчисления высказываний гильбертовского типа с правилом единичной подстановки [3]. Эти оценки были получены с использованием введенного в [2] понятия τ-множества, непосредственное применение которого в системах Фреге представляется затруднительным. В настоящей работе для произвольной тавтологии вводится понятие множества существенных подформул, и на его основе доказывается существование последовательности формул длины n, для которых в обеих системах $\mathscr{F}$ и $S\mathscr{F}$ количество шагов и длина выводов оцениваются соответственно функциями порядка n и n^2. Указывается также на возможность увеличения числа шагов выводов при переходе от единичных подстановок к мультипликативным.

Ввиду того, что в работе исследуются выводы в ряде систем, отметим, что в каждой из них вывод рассматривается как последовательность формул, каждая из которых является аксиомой данной системы или получается из предыдущих по одному из правил вывода данной системы. Вывод в системе Ф будем называть Ф-выводом.

Вывод называется приведенным, если результат вычеркивания из него любой формулы, кроме последней, не является выводом.

Длину формулы φ, понимаемую как количество всех символов в φ, будем обозначать через $|\varphi|$.

В качестве сложности вывода зафиксируем два понятия: количество различных формул (шагов) в выводе и суммарную длину всех формул вывода. Очевидно, что кратчайшие (в смысле того или иного критерия сложности) выводы являются приведенными.

В работе приводится описание системы $\mathscr{E}$ и даются основные свойства выводов в $\mathscr{E}$, далее выводы в $\mathscr{E}$ моделируются в системах Фреге. В конце работы оцениваются сложностные характеристики выводов в системах Фреге с правилом подстановки.

§ 1. Система $\mathcal{E}$

Мы будем пользоваться общепринятыми понятиями единичного булева куба E^n, пропозициональной формулы, тавтологии.

Согласно общепринятой терминологии пропозициональную формулу в дизъюнктивной нормальной форме мы рассматриваем как множество конъюнктов $\{\mathcal{K}_1, \mathcal{K}_2, \ldots, \mathcal{K}_s\}$, а конъюнкт $\mathcal{K}$ — как множество литералов (литерал — это переменная или переменная с отрицанием, причем ни в один конъюнкт не входит и переменная и ее отрицание).

Аксиомы системы $\mathcal{E}$ не фиксируются. Система $\mathcal{E}$ направлена на установление тавтологичности д.н.ф.. По определяемому ниже правилу к первоначальной системе конъюнктов прибавляется новый конъюнкт таким образом, что если первоначальная система тавтологична, то расширенная система так же тавтологична.

Единственным правилом вывода системы $\mathcal{E}$ является правило сокращения (элиминации), задаваемое следующим образом:

$$\frac{\mathcal{K}' \cup p \qquad \mathcal{K}'' \cup \bar{p}}{\mathcal{K}' \cup \mathcal{K}''} \qquad \text{э-правило,}$$

где $\mathcal{K}'$, $\mathcal{K}''$ — конъюнкты, а p — пропозициональная переменная.

Д.н.ф. $\mathcal{D} = \{\mathcal{K}_1, \mathcal{K}_2, \ldots, \mathcal{K}_s\}$ назовем *полной* (соответствует тавтологии), если из аксиом $\mathcal{K}_1, \mathcal{K}_2, \ldots, \mathcal{K}_s$ можно вывести пустой конъюнкт Λ.

Минимально возможное количество шагов в $\mathcal{E}$-выводе Λ из полной д.н.ф. $\mathcal{D}$ назовем сложностью д.н.ф. $\mathcal{D}$ и обозначим через $S(\mathcal{D})$.

Пусть φ — пропозициональная формула и $\{p_1, p_2, \ldots, p_n\}$ — множество ее различных переменных. Для некоторого набора $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_m) \in E^m$ конъюнкт $\mathcal{K} = \left\{p_{i_1}^{\sigma_1}, p_{i_2}^{\sigma_2}, \ldots, p_{i_m}^{\sigma_m}\right\}$ $(1 \leqslant m \leqslant n)$ назовем *φ-определяющим*, если придавая каждой переменной p_{i_j} значение σ_j можно за реальное время определить значение формулы φ вне зависимости от значений остальных переменных (подробнее в [4]).

Полную д.н.ф. назовем *φ-определяющей* для тавт φ, если каждый конъюнкт из $\mathcal{D}$ является *φ-определяющим.*

Примеры.

1) Для произвольной тавт ее совершенная д.н.ф. является φ-определяющей.

2) Если $\varphi_k = p_1 \to (p_2 \to (p_3 \to (\ldots \to (p_{k-1} \to (p_k \to (\bar{p}_k \to p_1)))\ldots))))$ $(k \geqslant 2)$ φ_k-определяющими, в частности, являются следующие д.н.ф.

$$\mathcal{D}_1 = \{p_1;\ \bar{p}_1\}, \quad \mathcal{D}_2 = \{p_k;\ \bar{p}_k\}, \quad \mathcal{D}_3 = \{p_1 p_2,\ p_1 \bar{p}_2,\ \bar{p}_1\}$$

3) Если $\varphi_l = (p_1 \to p_2) \to ((p_2 \to p_3) \to (\ldots \to ((p_{l-1} \to p_l) \to (p_1 \to p_l))\ldots))$ $l \geqslant 3$ φ_l-определяющей, в частности, будет д.н.ф.

$$\mathcal{D} = \{p_1 \bar{p}_2;\ p_2 \bar{p}_3;\ \ldots;\ p_{l-1} \bar{p}_l;\ \bar{p}_1;\ p_l\}$$

4) Для дальнейших рассмотрений важную роль будет играть формула $\varphi_{k,m} = \bigvee\limits_{(\sigma_1, \ldots, \sigma_k) \in E^k} \bigwedge\limits_{j=1}^{m} \left(\bigvee\limits_{i=1}^{k} p_{ij}^{\sigma_i} \right)$ (при каждых фиксированных $k \geqslant 1$, $1 \leqslant m \leqslant 2^k - 1$), которая «выражает» следующее утверждение: в каждой $k \times m$ матрице, состоящей из нулей и единиц при $m \leqslant 2^k - 1$ можно так «перевернуть» строки (заменить 0 на 1 и 1 на 0), чтобы в каждом столбце была по крайней мере одна единица. Истинность этого утверждения нетрудно доказать индукцией по k. В силу структуры $\varphi_{k,m}$, очевидно, что каждый $\varphi_{k,m}$-определяющий конъюнкт содержит по крайней мере m литералов.

Лемма 1.1. *Если для некоторой тавтологии* φ m *— минимально возможное количество литералов, принадлежащих* φ*-определяющему конъюнкту, то для любой* φ*-определяющей д.н.ф.* $\mathcal{D}$ $S(\mathcal{D}) \geqslant 2^{m+1} - 1$.

Доказательство. Пусть n — количество различных переменных твт φ $(n \geqslant m)$, тогда каждая φ-определяющая д.н.ф. $\mathcal{D}$ должна принимать значение «1» на 2^n наборах, но так как каждый φ-определяющий конъюнкт может «покрывать» максимум 2^{n-m} точек, то в каждой φ-определяющей д.н.ф. $\mathcal{D}$ должно быть как минимум $\frac{2^n}{2^{n-m}} = 2^m$ конъюнктов, которые и будут рассматриваться в качестве аксиом для вывода Λ. В [2] доказано, что в приведенном выводе с количеством шагов t, количество аксиом не превышает $\frac{t+1}{2}$, следовательно, $2^m \leqslant \frac{S(\mathcal{D})+1}{2}$, откуда и следует требуемая оценка.

Определение. φ-определяющую д.н.ф., имеющую наименьшую сложность среди всех φ-определяющих назовем *минимально-определяющей д.н.ф.* (м.о.д.н.ф.) для твт φ и будем обозначать через $\mathcal{D}_\varphi^{min}$.

Теорема 1.2. а) *Для произвольной твт* φ *длины* n

$$S\left(\mathcal{D}_\varphi^{min}\right) \leqslant 2^n.$$

б) *Для достаточно больших* n *существует последовательность формул* φ_n *таких, что*

$$\log_2 |\varphi_n| = \theta(n), \quad \log_2 S\left(\mathcal{D}_{\varphi_n}^{min}\right) = \Omega(2^n).$$

Доказательство. а) Как уже оговаривалось с.д.н.ф. является φ-определяющей, а для твт φ с длиной n, сложность ее с.д.н.ф. не превышает 2^n.

б) В силу замечания по поводу формул

$$\varphi_{k,\,m} = \bigvee_{(\sigma_1,\ldots,\sigma_k)\in E^k} \bigwedge_{j=1}^{m} \left(\bigvee_{i=1}^{k} p_{ij}^{\sigma_i} \right) \quad \left(k \geqslant 1,\ 1 \leqslant m \leqslant 2^k - 1\right)$$

и утверждения леммы 1.1, $S\left(\mathcal{D}_{\varphi_{k,\,m}}^{min}\right) \geqslant 2^m$. Обозначим через φ_n формулу $\varphi_{n,\,2^n-1}$. Очевидно, что

$\log_2 |\varphi_n| = \log_2 \left(n(2^n-1)\cdot 2^n\right) = \theta(n)$ и $\log_2 S\left(\mathcal{D}_{\varphi_n}^{min}\right) \geqslant \log_2 \left(2^{2^n-1}\right) = \theta(2^n)$.

Верхняя оценка для $\log_2 S\left(\mathcal{D}_{\varphi_n}^{min}\right) = O(2^n)$ следует из а).

§ 2. Сложность выводов в системах Фреге

Напомним общепринятые понятия систем Фреге [5, 8, 9].

Каждая система Фреге $\mathcal{F}$ использует некоторое конечное, функциональное полное множество пропозициональных связок. $\mathcal{F}$ определяется конечным множеством схематически заданных правил вывода $\frac{A_1 A_2 \ldots A_k}{B}$ (при $k = 0$ соответствующее правило определяет схему аксиом). $\mathcal{F}$ непротиворечива, т. е. для каждого правила вывода, если при некотором истинном значении переменных все A_i $(1 \leqslant i \leqslant k)$ принимают значение «истина» то и B принимает значение «истина». $\mathcal{F}$ полна, т. е. всякая твт выводима в $\mathcal{F}$.

В дальнейшем мы будем считать зафиксированной некоторую систему Фреге $\mathcal{F}$. Результат настоящей работы не зависит от выбора системы, однако для упрощения рассуждений мы будем предполагать, что в числе прочих язык $\mathcal{F}$ содержит логические связки $\neg$, $\rightarrow$, $\wedge$, $\vee$.

Теорема 2.1. *Каждая твт φ может быть выведена в $\mathcal{F}$ не более, чем за $c \cdot s \cdot l$ шагов, где $s = S\left(\mathcal{D}_{\varphi}^{min}\right)$, $l = |\varphi|$, а c — константа.*

Доказательство. Основываясь на методе Кальмара доказательства выводимости произвольной твт φ в КИВ, нетрудно заметить, что если конъюнкт $\mathcal{K} = \left\{p_{i_1}^{\sigma_1}, p_{i_2}^{\sigma_2}, \ldots, p_{i_m}^{\sigma_m}\right\}$ является φ-определяющим, то из посылки $\mathcal{K}$ можно вывести твт φ, выводя постепенно все подформулы φ, для которых конъюнкт $\mathcal{K}$ является определяющим, а значит для каждого φ-определяющего конъюнкта $\mathcal{K} = \left\{p_{i_1}^{\sigma_1}, p_{i_2}^{\sigma_2}, \ldots, p_{i_m}^{\sigma_m}\right\}$ формула

$$p_{i_1}^{\sigma_1} \wedge \left(p_{i_2}^{\sigma_2} \wedge \left(\ldots \wedge \left(p_{i_{m-1}}^{\sigma_{m-1}} \wedge p_{i_m}^{\sigma_m}\right)\ldots\right)\right) \to \varphi$$

может быть выведена в $\mathcal{F}$ не более, чем за $\tau \cdot l$ шагов для некоторой константы τ. э-правило «представляется» в системе $\mathcal{F}$ тавтологией $(\mathcal{K}' \wedge p \to \varphi) \to \left((\mathcal{K}'' \wedge \bar{p} \to \varphi) \to (\mathcal{K}' \wedge \mathcal{K}'' \to \varphi)\right)$ или $(p \to \varphi) \to ((\bar{p} \to \varphi) \to \varphi)$ при $\mathcal{K}' = \mathcal{K}'' = \Lambda$. Следовательно, любой $\mathcal{E}$-вывод пустого конъюнкта из $\mathcal{D}_{\varphi}^{min}$ может быть трансформирован в $\mathcal{F}$-вывод, количество шагов которого не превышает $c \cdot s \cdot l$, где $s = S\left(\mathcal{D}_{\varphi}^{min}\right)$, $l = |\varphi|$ и c — некоторая константа, зависящая от выбора системы $\mathcal{F}$ (подробнее см. в [4]).

Заметим, что: а) исходя из метода моделирования $\mathcal{F}$-вывода на основе $\mathcal{E}$-вывода, можно утверждать, что длина построенного $\mathcal{F}$-вывода не превышает $c' \cdot s \cdot l^2$ для некоторой константы c'; и б) величина $S\left(\mathcal{D}_{\varphi}^{min}\right)$ может быть существенно меньше экспоненты от количества различных переменных твт φ.

Теорема 2.2. *Для достаточно большого n и каждого p $\left(1 \leqslant p \leqslant \left[\sqrt{n} \log_n 2\right]\right)$ существует последовательность формул φ_p^n таких, что $|\varphi_p^n| = \theta(n)$, и количество шагов $\mathcal{F}$-выводов φ_p^n не превышает $c_1 \cdot n^p$, а длина $\mathcal{F}$-вывода не превышает $c_2 \cdot n^{p+1}$ для некоторых констант c_1 и c_2.*

Доказательство основано на применении результатов теоремы 2.1 и замечания а) к вышеупомянутым формулам $\varphi_{k,\,m}$ при $m = 1, k, k^2, k^3, \ldots, k^{[\log_k(2^k - 1)]}$.

§ 3. О сложности выводов в системах Фреге с подстановкой

Здесь описана последовательность формул длины n, нижние и верхние оценки количества шагов и длины выводов которых имеют порядок n и n^2 соответственно и в $\mathcal{F}$ и в $S\mathcal{F}$. Доказано также, что при переходе от систем с правилом единичной подстановки к системам с правилом мультипликативной подстановки возможно экспоненциальное увеличение минимально необходимого количества шагов выводов.

Система Фреге с подстановкой — $S\mathcal{F}$ получается из $\mathcal{F}$ добавлением правила подстановки $\frac{A}{A\sigma}$, где σ — отображение, ставящее в соответствие каждой переменной формулы A некоторую формулу (в частности переменную), и $A\sigma$ — результат повсеместной замены каждой переменной в A на соответствующую формулу. Отметим, что это определение *мультипликативной подстановки.* Если позволяется лишь повсеместная замена одной переменной на соответствующую формулу, то мы имеем дело с *единичной подстановкой.* Басс в [5] делает предположение о возможности увеличения числа шагов выводов при переходе от единичной подстановки к мультипликативной, что подтверждается утверждением теоремы 3.3 настоящей

работы (если не оговорено иное, подстановка будет считаться мультипликативной).

Определение. Формулы φ и ψ назовем *сравнимыми*, если для некоторой неэлементарной формулы γ найдутся такие подстановки σ' и σ'', что $\varphi = \gamma\sigma'$ и $\psi = \varphi\sigma''$.

Через $Sf(F)$ обозначим множество всех неэлементарных подформул формулы F. Для каждой формулы F, каждой подформулы $\varphi \in Sf(F)$ и произвольной переменной p через $(F)^p_\varphi$ обозначим результат повсеместной замены в F подформулы φ на переменную p. При этом если $\varphi \notin Sf(F)$, то $(F)^p_\varphi = F$. Множество различных переменных формулы F обозначим через $Var(F)$.

Определение. Пусть F — некоторая твт, p — переменная такая, что $p \notin Var(F)$ и $\varphi \in Sf(F)$. Подформулу φ назовем *существенной* для F, если $(F)^p_\varphi$ не является твт.

Множество существенных для твт F подформул обозначим через $\mathcal{E}ssf(F)$. Очевидно, что если F является минимальной твт, т. е. не может быть получена подстановкой из более короткой твт, то

$$\mathcal{E}ssf(F) = Sf(F).$$

Определение. Для каждого правила вывода $\frac{A_1 A_2 \ldots A_k}{B}$ $(k \geqslant 1)$ *характеризующей* назовем любую из существенных подформул формулы $A_1 \wedge (A_2 \wedge (\ldots \wedge (A_{k-1} \wedge A_k)\ldots)) \to B$, и их множество обозначим через $\mathcal{D}sf(A_1, A_2, \ldots, A_k, B)$.

Определение. Формулу φ назовем *важной* в $\mathcal{F}$-выводе ($S\mathcal{F}$-выводе), если φ или является существенной для некоторой аксиомы этого вывода, или является характеризующей для некоторого $\mathcal{F}$-правила, примененного в выводе (отметим, что важные в выводе формулы *активны* в смысле определения, введенного в [5]).

Лемма 3.1. 1) *Для каждого $\mathcal{F}$-правила* $\frac{A_1 A_2 \ldots A_k}{B}$ $(k \geqslant 1)$

$$\mathcal{E}ssf(B) \subset \left(\bigcup_{i=1}^{k} \mathcal{E}ssf(A_i) \right) \cup \mathcal{D}sf(A_1, A_2, \ldots, A_k, B).$$

2) *Для правила подстановки* $\frac{A}{A_\sigma}$

$$\mathcal{E}ssf(A\sigma) \subset \{\varphi\sigma \mid \varphi \in \mathcal{E}ssf(A)\}.$$

Доказательство. 1) Если некоторая подформула φ формулы B является существенной, то или φ будет существенной для формулы $A_1 \wedge (A_2 \wedge (\ldots \wedge (A_{k-1} \wedge A_k)\ldots)) \to B$, или для некоторой из формул A_i $(1 \leqslant i \leqslant k)$, откуда и следует первое утверждение.

2) Очевидно, что ни одна подформула ни одной формулы, подставленной вместо переменной формулы A не может быть существенной в $A\sigma$, если ни одно из ее иных вхождений в $A\sigma$ не является одновременно результатом подстановки в одну из существенных подформул формулы A.

Следствие. *Пусть F некоторая твт и $\varphi \in \mathcal{E}ssf(F)$, тогда*

1) *в каждом $\mathcal{F}$-выводе формулы F формула φ должна быть важной;*

2) *если правилами подстановки, использованными в некотором $S\mathcal{F}$-выводе формулы F являются* $\frac{A_1}{A_1\sigma_1}, \frac{A_2}{A_2\sigma_2}, \ldots, \frac{A_m}{A_m\sigma_m}$, *то φ должна быть или важной формулой этого вывода, или результатом последовательных подстановок $\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_s}$ для $1 \leqslant i_1, i_2, \ldots, i_s \leqslant m$ в одну из важных формул.*

Доказательство очевидным образом следует из утверждения леммы 3.1.

Теорема 3.1. *Для достаточно больших n, если F_n — такая твт, что $|F_n| = \theta(n)$ и для некоторого $l = \theta(n)$ существуют подформулы $\varphi_1, \varphi_2, \ldots, \varphi_l$ такие, что*

а) $\{\varphi_1, \varphi_2, \ldots, \varphi_l\} \subseteq \mathcal{E}ssf(F_n)$,

б) *для каждого фиксированного k $\left(1 \leqslant k \leqslant \left[\frac{l}{2}\right]\right)$ формулы φ_i и φ_{i+k} не сравнимы для всех i $(k \leqslant i \leqslant l-k)$,*

в) $|\varphi_1| < |\varphi_2| < \ldots < |\varphi_l|$ *и* $|\varphi_l| = \theta(n)$, *то количество шагов в любом $\mathcal{F}$-выводе ($S\mathcal{F}$-выводе) формулы F_n по порядку не менее, чем n, а длина любого $\mathcal{F}$-вывода ($S\mathcal{F}$-вывода) по порядку не менее n^2.*

Доказательство следует из вышеприведеных утверждений и того факта, что для заданной системы количество существенных подформул каждой аксиомы, и количество характеризующих подформул каждого $\mathcal{F}$-правила ограничено некоторой константой.

Пример 3.1 Для обоснования корректности условий теоремы 3.1, построим формулу, удовлетворяющую этим условиям. Как известно в трехбуквенном алфавите $\{a, b, c\}$ для любого $n > 0$ можно построить слово длины n, ни одно из подслов которого дважды подряд не повторяется (см. [1]).

Пусть $\alpha_1\alpha_2 \ldots \alpha_n$ — одно из таких слов в алфавите $\{a, b, c\}$. Этому слову поставим в соответствие некоторую формулу F_n, построенную следующим образом.

При $n > 0$ возмем $\psi_{n+1,\,n} = (p_0 \to \neg\neg p_0)$. Пусть уже построена формула $\psi_{i+1,\,n}$, соответствующая подслову $\alpha_{i+1} \ldots \alpha_n$ $(1 \leqslant i \leqslant n)$, тогда:

1) если $\alpha_i = a$, то $\psi_{i,\,n} = (p_i \to p_i) \wedge \psi_{i+1,\,n}$;

2) если $\alpha_i = b$, то $\psi_{i,\,n} = (\neg p_i \vee p_i) \to \psi_{i+1,\,n}$;

3) если $\alpha_i = c$, то $\psi_{i,\,n} = (\neg p_i \wedge p_i) \vee \psi_{i+1,\,n}$.

Возьмем $F_n = \psi_{1,\,n}$ и $\varphi_i = \psi_{i,\,n}$ $(1 \leqslant i \leqslant n)$. Нетрудно убедиться, что для формулы F_n и ее существенных подформул φ_i $(1 \leqslant i \leqslant n)$ выполнены условия теоремы 3.1.

Отметим, что для формулы F_n нетрудно получить одинаковые верхние оценки сложностей $\mathcal{F}$-выводов и $S\mathcal{F}$-выводов, равные по порядку нижним для обоих критериев сложности, а значит верно следующее утверждение.

Теорема 3.2. *Для достаточно больших n существуют формулы F_n, длины порядка n, такие, что минимальные количества шагов их $\mathcal{F}$-выводов и $S\mathcal{F}$-выводов имеют порядок n, а минимальные длины их $\mathcal{F}$-выводов и $S\mathcal{F}$-выводов имеют порядок n^2.*

Пример 3.2 Нетрудно убедиться, что при единичной подстановке условия теоремы 3.1 выполняются также для формулы

$$\Phi_n = (p_1 \to p_1) \wedge \big((p_2 \to p_2) \wedge \big(\ldots \wedge \big((p_{n-1} \to p_{n-1}) \wedge (p_n \to p_n)\big) \ldots\big)\big)$$

и ее существенных подформул

$$\varphi_i = (p_{n-i} \to p_{n-i}) \wedge \big((p_{n-i+1} \to p_{n-i+1}) \wedge \big(\ldots \wedge \big((p_{n-1} \to p_{n-1}) \wedge (p_n \to p_n)\big) \ldots\big)\big) \quad (0 \leqslant i \leqslant n-1),$$

а значит, количество шагов любого вывода формулы Φ_n в системе с правилом единичной подстановки по порядку не менее, чем n.

Однако следует заметить, что при допущении мультипликативной подстановки формулу Φ_n можно вывести следующим образом.

Обозначим через $\gamma_{i,\,j}(q)$ формулу

$$(p_i \to p_i) \wedge \big((p_{i+1} \to p_{i+1}) \wedge \big(\ldots \wedge \big((p_j \to p_j) \wedge q\big) \ldots\big)\big)$$

для некоторой переменной q, а через β_k — формулу $q \to \gamma_{1,\,k}(q)$. Пусть формула β_1 выводится в системе $S\mathcal{F}$ за c шагов. Предположим уже выведена формула β_k. Подстановкой вместо переменной q можно за один шаг вывести $\gamma_{k+1,\,2k}(q) \to \gamma_{1,\,k}(\gamma_{k+1,\,2k}(q))$, т. е. формулу $\gamma_{k+1,\,2k}(q) \to \gamma_{1,\,2k}(q))$. Подставляя в β_k вместо каждой переменной p_i переменную p_{i+k} $(1 \leqslant i \leqslant k)$, еще за один шаг получим $q \to \gamma_{k+1,\,2k}(q)$. Применив далее правило силлогизма (транзитивность импликации), которое в любой системе $S\mathcal{F}$ может быть получено за конечное число шагов, выведем β_{2k}.

Таким образом β_{2k} выводится из β_k за c_1+3 шага, а следовательно, для произвольного $k \geqslant 2$ β_k может быть выведена за $O(\log_2 k)$ шага. Наконец, подставив вместо q формулу $p_{k+1} \to p_{k+1}$, и выведя ее саму за конечное число шагов, выведем формулу

$$(p_1 \to p_1) \wedge \big((p_2 \to p_2) \wedge \big(\ldots \wedge \big((p_k \to p_k) \wedge (p_{k+1} \to p_{k+1})\big) \ldots\big)\big) .$$

Таким образом, для любого достаточно большого n Φ_n может быть выведена за не более, чем $O(\log_2 n)$ шагов, а следовательно, верно следующее утверждение.

Теорема 3.3. *Для достаточно большого n существует последовательность твт длины $\theta(n)$ таких, что количество шагов их кратчайших выводов в системе с единичной подстановкой по подядку не менее n, а в системе с мультипликативной подстановкой — не более, чем* $\log_2 n$.

Таким образом, экспоненциальное увеличение количества шагов выводов может иметь место не только при переходе от систем без подстановок к системам с подстановками, что впервые было установлено автором настоящей работы в 1969 г. [2] и подтверждено рядом других авторов в 1989 г., но и при переходе от систем с единичными подстановками к системам с мультипликативной подстановкой, т. е. подтверждается предположение С. Басса, высказанное в [5].

В заключение считаю необходимым высказать благодарность С. Бассу, а также участникам семинара ИПИА НАН РА за полезные советы и замечания.

СПИСОК ЛИТЕРАТУРЫ

1. Адян С. И. Проблемы Бернсайда и тождества в группах. — М.: Наука, 1975.
2. Цейтин Г. С., Чубарян А. А. О некоторых оценках длин логических выводов в классическом исчислении высказываний // Матем. вопросы кибернетики и вычисл. техники. — Ереван, И-во АН Арм. ССР. — 1975. — С. 57–64.
3. Чубарян А. А. О сложности выводов в различных системах исчисления высказываний // Прикладная математика. — ЕрГУ. — 1. — 1981. — С. 81–89.
4. Чубарян А. А. Сложность выводов в некоторой системе классического исчисления высказываний // Известия НАН РА, Математика. — Т. 34, № 5. — 1999. — С. 16–26.
5. Buss S. R. Some remarks on lengths of propositional proofs // Arch. Math. Logic. — 1995. — 34. — P. 377–394.
6. Chubaryan A. A. On the Complexity of proofs in a Frege system // Colloquium Logicum, Annals of the Kurt-Gödel-Sosiety. — V. 4. — Vienna. — 2001. — P. 69, and Bulletin of Symbolic Logic. — V. 8, № 1. — March 2002. — P. 128.
7. Chubaryan An. A., Chubaryan Arm. A. On the proofs complexity in CPL // Logic Colloquium-2002. — Muenster, Germany. — P. 30, and Bulletin of Symbolic Logic. — V. 9, № 1. — March 2003. — P. 90.
8. Pudlak P. The Lengths of Proofs // Handbook of proof theory. — North-Holland. — 1998. — P. 547–637.
9. Urquhart A. The complexity of propositional proofs // The Bulletin of Symbolic Logic. — V. 1, № 4. — Dec. 1995. — P. 425–467.
10. Urquhart A. The number of lines in Frege proofs with substitution // Arch. Math. Logic. — 1997. — 37. — P. 15–19.

Поступило в редакцию 12 III 2005