СЛОЖНОСТЬ ВЫВОДОВ В ОДНОЙ СИСТЕМЕ КЛАССИЧЕСКОГО ИСЧИСЛЕНИЯ ВЫСКАЗЫВАНИЙ

А. А. Чубарян

Известия Национальной Академии Наук Армении. Математика, том 34, № 5, 1999

На основе метода Кальмара выводимости тавтологий в классическом исчислении высказываний мы строим полную аксиоматическую систему $\mathcal{C}$ со следующими свойствами : 1) каждую тавтологию φ можно вывести в $\mathcal{C}$ не более, чем за $c_1 2^m l$ шагов, где $m = |M\varphi|$, $M\varphi$ – характеристическое множество подформул φ, l – длина φ, а c_1 – некоторая постоянная; 2) существует класс тавтологий такой, что количество шагов выводов в $\mathcal{C}$ больше, чем $c_2 2^m$, где c_2 – некоторая постоянная.

§1. ВВЕДЕНИЕ

В недавних обзорных работах [1] – [3], относящихся к сложности выводов в различных модификациях классического исчисления высказываний, указывалось на экспоненциальные нижние оценки сложностей выводов, полученные лишь в системах с резолюциями, а в системах Фреге наилучшие нижние оценки разве лишь квадратические.

В настоящей статье для произвольной тавтологии φ определяется некоторое характеристическое подмножество $M\varphi$ подформул. На основе метода Кальмара [4] установления выводимости произвольной тавтологии в классическом исчислении высказываний, мы определяем систему аксиом $\mathcal{C}$ типа Фреге со следующими свойствами (через $TAUT$ обозначим множество всех тавтологий) :

a) система аксиом $\mathcal{C}$ полна ;

b) каждую $\varphi \in TAUT$ можно вывести в $\mathcal{C}$ не более, чем за $c_1 2^m l$ шагов, где $m = |M\varphi|$, l не превышает длины φ, а c_1 – константа ;

c) существует $\varphi \in TAUT$ с минимальным количеством шагов выводов в $\mathcal{C}$, превышающих $c_2 2^m$, где c_2 – константа.

Перечисленные свойства позволяют указать $\varphi \in TAUT$ длину n и верхнюю (нижнюю) оценку числа шагов выводов n^{p+1} (n^p), где $1 \le p \le [\sqrt{n}\log_n 2]$ для достаточно большого n, $[\cdot]$ обозначает целую часть.

В заключительной части работы обсуждаются соотношения между сложностями выводов в $C-$ и Фреге системах.

§1. ОСНОВНЫЕ ПОНЯТИЯ, ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ

Согласно общепринятому понятию, пропозициональная формула является словом, составленным по следующим правилам

1) пропозициональные переменные x_i, $i \ge 1$;
2) логические связки $\vee$, $\wedge$, $\rightarrow$, $\neg$;
3) скобки (,).

В дальнейшем под символом $*$ мы будем понимать $\vee$, $\wedge$, $\rightarrow$ или $\neg$. Символ $\rightleftharpoons$ означает графическое равенство слов.

Известно, что каждой формуле φ можно сопоставить некоторое дерево с корнем : каждой подформуле ставится по одно-однозначному соответствию некая вершина ; если подформула имеет вид $\alpha * \beta$, то вершины, которым приписаны формулы $\alpha * \beta$, соединяются ребрами с вершинами α и β ; если подформула имеет вид $\neg\alpha$, то вершина $\neg\alpha$ связана с α. Корнем считается вершина, которой приписана формула φ. Дерево с корнем, соответствующее формуле φ, назовем **φ-деревом**, а корень **φ-корнем**. Естественно, что каждой подформуле α в φ соответствует α-дерево с α-корнем в φ-дереве. Каждой висячей вершине φ-дерева соответствует некоторая элементарная подформула формулы φ.

Единичный m-мерный булев куб обозначается через E^m. Для каждого множества $X = \{x_1, ..., x_m\}$ и для любого $\sigma = (\sigma_1, ..., \sigma_m) \in E^m$ введем обозначение $X^\sigma = \{x_1^{\sigma_1}, ..., x_m^{\sigma_m}\}$, где

$$x^{\sigma_i} = \begin{cases} x & \text{для} \quad \sigma_i = 1, \\ \neg x & \text{для} \quad \sigma_i = 0, \end{cases} \qquad i = 1, ..., m.$$

Мы назовем $\varphi \in TAUT$ **минимальной тавтологией**, если φ не получается подстановкой из более короткой тавтологии. Пусть φ – минимальная тавтология, $X = \{x_1, ..., x_m\}$ – множество различных переменных формулы φ, α – подформула формулы φ. Пусть далее $X_p = \{x_{i_1}, ..., x_{i_p}\} \subset X$ и $\sigma = (\sigma_{i_1}, ..., \sigma_{i_p}) \in E^p$.

Определение 1. Множество формул X_p^σ назовем **α-определяющим**, если приписывая значения σ_{i_j} каждой вершине x_{i_j}, $1 \le j \le p$ мы индуцируем значение каждой вершины любого изолированного поддерева α-дерева, которое содержит α-корень и только те висячие вершины, маркированные переменными x_{i_j}.

Определение 2. α-определяющее множество X_p^σ назовем **тупиковым**, если ни одно собственное подмножество не является α-определяющим. α-определяющее множество X_p^σ называется **$\alpha - \varepsilon$-определяющим**, если $\alpha(\sigma_{i_1}, ..., \sigma_{i_p}) = \varepsilon$, $\varepsilon \in \{0, 1\}$.

Определение 3. Множество переменных X_p назовем **важным** для формулы φ, если для любого $\sigma \in E^p$ множество X_p^σ является φ-определяющим.

Вообще говоря, важное множество переменных можно выбирать различными способами, причем число его переменных может быть гораздо меньше числа различных переменных формулы φ.

Пример 1. Для формулы

$$\varphi_k = x_1 \to (x_2 \to \cdots \to (x_k \to (\overline{x}_k \to x_1)\cdots), \quad k \geq 2$$

каждое непустое подмножество множества $\{x_1, x_k\}$ является важным.

Определение 4. Минимальное по мощности важное множество переменных минимальной тавтологии φ назовем **характеристическим множеством** для φ и будем обозначать через $M\varphi$.

Отметим, что если $M\varphi = \{x_{i_1}, ..., x_{i_m}\}$, то переименованием переменных можно добиться, чтобы $M\varphi = \{x_1, ..., x_m\}$. Из Определения 4 следует, что если $M\varphi = \{x_1, ..., x_m\}$, то для произвольного $\sigma = (\sigma_1, ..., \sigma_m) \in E^m$ формулу φ можно вывести из посылок $x_1^{\sigma_1}, ..., x_m^{\sigma_m}$, пошаговым построением подформул (или их отрицаний) соответствующего поддерева, содержащего φ-корень. Итак, метод Кальмара [4] можно применить не ко всем вершинам формулы φ, а для переменных характеристического множества минимальной тавтологии φ. Тогда φ выводится пошаговым исключением формул с помощью 2^m различных посылок (согласно теореме о полноте классического исчисления высказываний [4]). Однако, для вывода минимальной тавтологии φ, не обязательно использовать все 2^m φ-множества.

Пусть для минимальной тавтологии φ, $M\varphi = \{x_1, ..., x_m\}$, и пусть для некоторого $\sigma = (\sigma_{i_1}, ..., \sigma_{i_r}) \in E^r$, $r \leq m$ множество $X_r^\sigma = \{x_{i_1}^{\sigma_1}, ..., x_{i_m}^{\sigma_m}\}$ имеет минимальную мощность среди всех тупиковых φ-определяющих подмножеств множества $M^\sigma\varphi$ для всех $\sigma \in E^m$. Очевидно, что φ можно вывести, исключая предпосылки из X_r^σ и φ-определяющих множеств, получающиеся из $X_r^{\sigma'}$, $\sigma' \in E^r \setminus \{\sigma\}$ добавлением максимум всех остальных $m-r$ переменных степени σ'' для всех $\sigma'' \in E^{m-r}$, т.е. не более чем $1 + (2^r - 1)2^{m-r}$ наборов посылок.

Определение 5. Множество переменных минимальной тавтологии φ, которые имеют минимальную мощность среди тупиковых φ-определяющих подмножеств множества $M^\sigma\varphi$, $\sigma \in E^m$ называется **ядром насыщения характеристического множества** $M\varphi$ и будет обозначаться через $kM\varphi$. Если $M\varphi = kM\varphi$, то характеристическое множество $M\varphi$ называется **насыщенным**.

Пример 2. Для $\varphi_m = \bigvee_{\sigma\in E^m} (\bigwedge_{i=1}^m x_i^{\sigma_i})$, $\quad m \geq 1$ имеем $M\varphi_m = \{x_1, ..., x_m\}$ и оно является насыщенным.

Пример 3. Для

$$\varphi_l = (x_1 \to x_2) \to \Big((x_2 \to x_3) \to \cdots \to \Big((x_{l-1} \to x_l) \to (x_1 \to x_l)\Big)\cdots\Big), \quad l \geq 3$$

имеем $M\varphi_l = \{x_1, ..., x_m\}$ и $kM\varphi_l = \{x_1\}$ или $kM\varphi_l = \{x_l\}$, т.е. $M\varphi_l$ не является насыщенным. φ_l-определяюшие множества, которые используются в методе Кальмара для вывода φ имеют вид

$$\begin{array}{llllll}
x_1^0 & & & & & \\
x_1^1 & x_2^0 & & & & \\
x_1^1 & x_2^1 & x_3^0 & & & \\
\cdots & \cdots & \cdots & \ddots & & \\
x_1^1 & x_2^1 & x_3^1 & \cdots & x_{l-1}^1 & x_l^0 \\
x_1^1 & x_2^1 & x_3^1 & \cdots & x_{l-1}^1 & x_l^1
\end{array}
\qquad \text{или} \qquad
\begin{array}{llllll}
 & & & & & x_l^1 \\
 & & & & x_{l-1}^1 & x_l^0 \\
 & & & x_{l-2}^1 & x_{l-1}^0 & x_l^0 \\
 & & \cdots & \cdots & \cdots & \cdots \\
x_1^1 & x_2^0 & \cdots & x_{l-2}^0 & x_{l-1}^0 & x_l^0 \\
x_1^0 & x_2^0 & \cdots & x_{l-2}^0 & x_{l-1}^0 & x_l^0
\end{array}$$

Пример 4.

$$\varphi_{k,m} = \bigvee_{\sigma\in E^k} \bigwedge_{j=1}^{m} \left(\bigvee_{i=1}^{k} x_{ij}^{\sigma_i} \right), \quad k \geq 1, \quad 1 \leq m \leq 2^k - 1. \tag{1.1}$$

Формула $\varphi_{k,m}$ утверждает, что в каждой 0-1-матрице порядка $k \times m$, где $m \leq 2^k - 1$, строки можно выбрать так, чтобы записав 0 вместо 1, а 1 вместо 0, получаем матрицу, в каждом столбце которой было бы по крайней мере одна 1. Множество $M\varphi_{k,m}$ для $m = 2^k - 1$ содержит все km переменные, но не для $m < 2^k - 1$. Оно не является насыщенным, но каждое $\varphi_{k,m}$-определяющее множество содержит по крайней мере m формул (по одному из каждого дизъюнкта некоторой конъюкции). Следовательно $|kM\varphi_{k,m}| = m$.

Если $\varphi \in TAUT$ не минимальна, то выбирается некоторая минимальная тавтология ψ такая, что φ получается из ψ подстановкой. Если $M\psi = \{x_1, ..., x_m\}$ и φ получается из ψ некоторой заменой переменных $x_1, ..., x_m$ соответственно формулами $\alpha_1, ..., \alpha_m$, то множество $M\varphi = \{\alpha_1, ..., \alpha_m\}$ называется **характеристическим множеством** формулы φ.

При различных выборах формул ψ, $M\varphi$ могут быть разными (даже по мощности). Ниже мы будем использовать этот факт при выборе ψ и следовательно $M\varphi$. Если $M\varphi = \{\alpha_1, ..., \alpha_m\}$ для любого $\varphi \in TAUT$, то метод Кальмара приложим и для множества $\{\alpha_1, ..., \alpha_m\}$. Эти замечания позволяют нам применять метод Кальмара, используя :

1) не все переменные формулы φ,

2) не все наборы посылок,

3) некоторые подформулы или их отрицания вместо переменных или их отрицаний.

Ниже определяется некоторая специальная аксиоматическая система C, в которой получаются относительно близкие верхние и нижние оценки числа шагов выводов тавтологий. Ниже мы также будем использовать несколько понятий, см. [6]. Главный логический знак формулы φ (если он существует) будем обозначать через $R(\varphi)$. Сама формула φ нумеруется последовательностью (1). Если некоторая подформула $\alpha = \alpha' * \alpha''$ ($\alpha = \neg\alpha$) занумерована последовательностью $(\sigma_1, ..., \sigma_n) \in E^n$, то α' нумеруется последовательностью $(\sigma_1, ..., \sigma_n, 0)$, а α'' последовательностью $(\sigma_1, ..., \sigma_n, 1)$ (α' нумеруется последовательностью $(\sigma_1, ..., \sigma_n, 1)$). Число логических вхождений в φ, кроме отрицаний над переменными, называется **логической длиной** (или просто длиной) формулы φ и будем обозначать через $l\varphi$. Для каждой формулы $\alpha_1, ..., \alpha_m$, если $K = \alpha_1^{\sigma_1} \wedge ... \wedge \alpha_m^{\sigma_m}$, $\sigma = (\sigma_1, ..., \sigma_m) \in E^m$, то множество $\{\alpha_1^{\sigma_1}, ..., \alpha_m^{\sigma_m}\}$ будем обозначать через K^σ, а множество $\{\alpha_1, ..., \alpha_m\}$ через $\widetilde{K}$.

Ниже будем использовать общепринятое понятие вывода в системах Фреге. Вывод формулы в некотором исчислении назовем **кратчайшим**, если он имеет минимальное число формул среди всех выводов формулы φ. Число формул в кратчайшем выводе формулы φ в системе C будем обозначать через T_φ^C.

Вывод называется **тупиковым**, если после вычеркивания из него любой формулы, кроме последней, он не является выводом. Очевидно, что кратчайший вывод необходимо тупиковый.

§2. СИСТЕМА КЛАССИЧЕСКОГО ИСЧИСЛЕНИЯ ВЫСКАЗЫВАНИЙ C

Аксиомами системы C являются формулы, задаваемые следующими схемами :

I $\quad \alpha_1 \wedge (\alpha_2 \wedge ... \wedge (\alpha_{m-1} \wedge \alpha_m)...) \to \alpha_i, \quad m \geq 1,\ 1 \leq i \leq m,$

II 1. $(K \to \alpha) \to ((K \to \neg\beta) \to ((K \to \neg(\alpha \to \beta))),$

2. $(K \to \neg\alpha) \to (K \to (\alpha \to \beta)),$

3. $(K \to \beta) \to (K \to (\alpha \to \beta)),$

4. $(K \to \alpha) \to ((K \to \beta) \to (K \to \alpha \wedge \beta)),$

5. $(K \to \neg\alpha) \to (K \to \neg(\alpha \wedge \beta)),$

6. $(K \to \neg\beta) \to (K \to \neg(\alpha \wedge \beta)),$

7. $(K \to \neg\alpha) \to ((K \to \neg\beta) \to (K \to \neg(\alpha \vee \beta))),$

8. $(K \to \alpha) \to (K \to \alpha \vee \beta),$

9. $(K \to \beta) \to (K \to \alpha \vee \beta),$

10. $(K \to \alpha) \to (K \to \neg\neg\alpha),$

III 1. $(\delta \wedge K \to \varphi) \to ((\overline{\delta} \wedge K \to \varphi) \to (K \to \varphi)),$

2. $(\gamma \to \varphi) \to ((\overline{\gamma} \to \varphi) \to \varphi),$

где

1) α, β, α_i, $1 \le i \le m$ некоторые формулы. $\alpha_m \notin TAUT$ и $\overline{\alpha}_m \notin TAUT$.

2) $K \rightleftharpoons \beta_1 \wedge \ldots \wedge \beta_p$, $p \ge 1$ для любых формул β_i, $1 \le i \le p$. $\beta_p \notin TAUT$, причем $\overline{\beta}_p \notin TAUT$.

3) для каждой подформулы вида $K \to \psi$, в аксиомах группы II, множество K^σ является ψ – 1–определяюшим.

4) в аксиомах 1. группы III $\delta \notin \widetilde{K}$. $\{\delta\} \cup \widetilde{K} \subset M\varphi$, и множество K^σ не является φ-определяющим.

5) в аксиомах 2. группы III формула φ не имеет вид $\varphi_1 \to \varphi_2$ для некоторой $\varphi_2 \in TAUT$.

6) в аксиомах 2. группы III, если все формулы $M\varphi$ формулы φ суть тавтологии, то $\gamma \rightleftharpoons x_1$. в противном случае γ принадлежит $M\varphi$, $\gamma \notin TAUT$ и $\overline{\gamma} \notin TAUT$. Правилами вывода являются **modus ponens** : $\dfrac{A \quad A \to B}{B}$ (где A называется малой, а $A \to B$ большой посылкой), а также

$$\frac{A \quad B}{A \wedge B}, \quad \frac{A}{A \vee B}, \quad \frac{B}{A \vee B}, \quad \frac{B}{A \to B}, \quad \frac{\overline{A}}{A \to B}.$$

Ниже, если не оговорено иное, все выводы рассматриваются в системе C.

Теорема 1. Система C полна.

Доказательство : Пусть $\varphi \in TAUT$. $M\varphi = \{\alpha_1, \ldots, \alpha_m\}$. Если существует целое i. $1 \le i \le m$ такое, что $\alpha_i \notin TAUT$, то "аксиоматическое моделирование" выводимости тавтологии методом Кальмара прилагается к $\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_m, \alpha_i$

по схеме, описанной в [5]. Если $\alpha_1, ..., \alpha_m \in TAUT$, то аналогичная схема прилагается к $\alpha_1, ..., \alpha_m, x_1$. Теорема 1 доказана.

Теорема 2. **Для каждого $\varphi \in TAUT$ имеем $T_\varphi^C \leq c_1 2^m l$, где $m = |M\varphi|$, $l = l\varphi$, а c_1 –постоянная.**

Доказательство : аналогично доказательству Теоремы 2 в [5].

Определение 6. Формула φ называется правильной, если

a) φ – минимальная тавтология,

b) для каждой аксиомы A системы C имеем $\varphi \neq A_{(1)}$, $\varphi \neq A_{(11)}$, а для аксиом 1., 4., 7. группы II, или для аксиомы 1. группы III имеет место $\varphi \neq A_{(111)}$,

c) φ не имеет ни вида $\varphi_1 \wedge \varphi_2$, ни вида $\varphi_1 \vee \varphi_2$, где $\varphi_1 \in TAUT$ или $\varphi_2 \in TAUT$, или вида $\varphi_1 \to \varphi_2$, где $\neg\varphi_1 \in TAUT$ и $\varphi_2 \in TAUT$.

Очевидно, что для правильной тавтологии φ по крайней мере одна из формул множества $M\varphi$ не является тавтологией, также как отрицание этой формулы не является тавтологией.

Теорема 3. **Для любой правильной тавтологии φ имеем $T_\varphi^C > c_2 2^r$, где $r = |kM\varphi|$, а c_2 - некоторая постоянная.**

Доказательство : следует из нижеследующих лемм.

Лемма 1. **Каждая аксиома группы I может служить только малой посылкой modus ponens.**

Доказательство : Из ограничения 1) следует, что $\alpha_1 \wedge ... \wedge \alpha_m \notin TAUT$.

Лемма 2. **Если формулы φ_i, $0 \leq i \leq k$ и**

$$\psi_j = \varphi_j \to (\varphi_{j-1} \to ... \to (\varphi_1 \to \varphi_0)...), \quad 1 \leq j \leq k$$

выводятся по $\varphi \in TAUT$, и ψ_k – аксиома, то $k \leq 2$.

Доказательство : Предположим противное : $k \geq 3$. Формулы φ_i, $0 \leq i \leq k$ и ψ_j, $1 \leq j \leq k$ выводятся по $\varphi \in TAUT$, а ψ_k – аксиома. По Лемме 1 она не может быть аксиомой группы I. Она не может быть и аксиомой группы II или аксиомой 1. группы III потому, что по ограничению 2), φ_{k-1} (φ_{k-2} соответственно) не может быть конъюнкцией. Она не может быть и аксиомой 2. группы III (что следует из ограничения 5)). Лемма 2 доказана.

Лемма 3. **В тупиковом выводе произвольной правильной формулы φ, содержащей вывод $\gamma \to \varphi$ и $\overline{\gamma} \to \varphi$ для некоторого $\gamma \in M\varphi$, которая не является тавтологией и $\overline{\gamma} \notin TAUT$.**

Доказательство : Рассмотрим всевозможные концовочные фрагменты вывода правильной формулы φ. Так как φ – правильна, то по ограничению b) она не может быть аксиомой, а φ должна быть выведена только по modus ponens из некоторых формул ψ_1 и $\psi_1 \to \varphi$ (что следует из ограничения c)). Из ограничения b) формула $\psi_1 \to \varphi$ не может быть аксиомой, и не может быть выведена по правилу $\dfrac{\varphi}{\psi_1 \to \varphi}$ (противоречит тупиковости), или по правилу $\dfrac{\overline{\psi}_1}{\psi_1 \to \varphi}$ (ввиду выводимости ψ_1) и следовательно, должна быть выведена из некоторых выводимых формул ψ_2 и $\psi_2 \to (\psi_1 \to \varphi)$ по modus ponens. Из Леммы 2 следует, что формула $\psi_2 \to (\psi_1 \to \varphi)$ является аксиомой. Она не может быть

– аксиомой группы I (по Лемме 1),

– аксиомой группы II (по ограничениям 2) и b)),

– аксиомой 1 группа III (по ограничению b)).

Следовательно, $\psi_2 \to (\psi_1 \to \varphi)$ должна быть аксиомой 2 группы III. Поэтому $\psi_2 \rightleftharpoons \gamma \to \varphi$, $\quad \psi_1 \rightleftharpoons \overline{\gamma} \to \varphi$, для некоторого $\gamma \in M\varphi$, где $\gamma \notin TAUT$ и $\overline{\gamma} \notin TAUT$. Лемма 3 доказана.

Лемма 4. Пусть формула $K \to \varphi$ выведена в некотором тупиковом выводе правильной формулы φ. Если K – конъюкция формул таких, что $\widetilde{K} \subset M\varphi$, но K^σ не является φ-определяющим, то необходимо вывести и $\delta \wedge K \to \varphi$ и $\overline{\delta} \wedge K \to \varphi$, где $\delta \in M\varphi \setminus \widetilde{K}$.

Доказательство : Рассмотрим всевозможные концовочные фрагменты подвывода $K \to \varphi$. Так как φ является правильной формулой, то по ограничению b), формула $K \to \varphi$ не может быть аксиомой. $K \to \varphi$ не может быть выведен по правилу $\dfrac{\varphi}{K \to \varphi}$ (ввиду тупиковости вывода) или по правилу $\dfrac{\overline{K}}{K \to \varphi}$ (из ограничения 2) следует, что K не является выводимой). Следовательно, $K \to \varphi$ должен быть выведен из некоторых выводимых формул ψ_1 и $\psi_1 \to (K \to \varphi)$ по modus ponens. Формула $\psi_1 \to (K \to \varphi)$ не может быть

– аксиомой группы I (по Лемме 1),

– одной из аксиом 1., 4., 7. группы II (по ограничению 3)),

– одной из оставшихся аксиом группы II или аксиомой группы III (если A является одной из упомянутых аксиом, то $R(A_{(110)}) \rightleftharpoons \to$, но $R(K) \rightleftharpoons \wedge$).

Формула $\psi_1 \to (K \to \varphi)$ может быть выведена по правилу $\dfrac{K \to \varphi}{\psi_1 \to (K \to \varphi)}$ (ввиду тупиковости вывода), или по правилу $\dfrac{\overline{\psi}_1}{\psi_1 \to (K \to \varphi)}$ (ввиду выводимости ψ_1). Следовательно, она должна быть выведена из некоторых выводимых формул ψ_2

и

$$\psi_2 \to (\psi_1 \to (K \to \varphi)) \tag{2.1}$$

по modus ponens. По Лемме 2 формула (2.1) является аксиомой. Она не может быть аксиомой группы I или II (в силу рассуждений, аналогичных приведенным выше), или аксиомой 2 группы III (по ограничению 5)). Следовательно, формула (2.1) может быть только аксиомой 1 группы III. Поэтому $\psi_2 \Rightarrow \delta \wedge K \to \varphi$, $\psi_1 \Rightarrow \overline{\delta} \wedge K \to \varphi$, для некоторого $\delta \in M\varphi \setminus \bar{K}$. Лемма 4 доказана.

Следствие 1. Пусть φ – правильная формула и $kM\varphi = \{x_{i_1}, \dots, x_{i_r}\}$. Тогда для любого $\sigma \in E^r$ по крайней мере формулы

$$x_{i_1}^{\sigma_{i_1}} \wedge \dots \wedge x_{i_r}^{\sigma_{i_r}} \to \varphi, \quad \sigma = (\sigma_1, \dots, \sigma_r) \in E^r,$$

должны быть выведены в кратчайшем выводе формулы φ.

Доказательство : следует из Леммы 4 и ограничений 3) и 4).

Отметим, что если φ представима в виде $\varphi \Rightarrow \varphi_1 * \dots * \varphi_t$, где $\varphi_i \in TAUT$ и $|M\varphi_i| = m_i$, $i = 1, \dots, t$, то $T\varphi$ имеет порядок $O\left(\sum_{i=1}^{t} 2^{m_i} l\varphi\right)$. Эта оценка может быть существенно лучше известных верхних оценок.

§3. ИЕРАРХИЯ ФОРМУЛ ПО СЛОЖНОСТИ ВЫВОДОВ В СИСТЕМЕ C

Результаты Теорем 2 и 3 позволяют указать на некоторую иерархию по сложности выводов формул в C. Обозначим через Φ_n^p классы последовательностей $\varphi_n^p \in TAUT$ таких, что $\log_2 l\varphi_n^p = O(n)$ и $O(n^p) \le \log_2 T_{\varphi_n^p}^C \le O(n^{p+1})$.

Теорема 4. Для любого p, $1 \le p \le [n \log_n 2]$ и достаточно больших n, классы Φ_n^p не пусты.

Доказательство : Рассмотрим формулы (1.1) Примера 4. Имеем $|M\varphi_{n,m}| \le nm$, $|kM\varphi_{n,m}| = m$ и $l\varphi_{n,m} = 2^n(m(n-1) + m - 1) + 2^n - 1 = 2^n mn - 1$,

$$c_2 2^m \le T_{\varphi_{n,m}}^C \le c_1 2^{nm} 2^n mn = c_1 2^{n(m+1)} mn,$$

где c_1, c_2 – постоянные. Для $m = n^p$ получаем

$$\log_2 l\varphi_{n,n^p} = O(\log_2(n^p 2^n n)) = O(n + (p+1)\log_2 n) = O(n),$$

$$\log_2 T_{\varphi_{n,n^p}}^C \le O\left(\log_2(n^p 2^{n(n^p+1)} n)\right) = O(n^{p+1} + n + (p+1)\log_2 n) = O(n^{p+1}),$$

$$\log_2 T_{\varphi_{n,n^p}}^C \ge O\left(\log_2 2^{n^p}\right) = O(n^p),$$

Следовательно, $\varphi_{n,n^p} \in \Phi_n^p$. Теорема 4 доказана.

§4. РЕЗУЛЬТАТЫ ДЛЯ СИСТЕМ ФРЕГЕ

Обозначим через $\mathcal{C}'$ систему, получающуюся из $\mathcal{C}$ снятием ограничения 5). Пусть $\mathcal{F}$ – система Фреге с логическими символами $\vee$, $\wedge$, $\to$ и $\neg$.

Теорема 5. a) Если для тавтологии φ имеем $T_\varphi^{\mathcal{F}} \le n$, то $T_\varphi^{\mathcal{C}'} \le c_3 n$, где c_3 – константа.

b) Если $T_\varphi^{\mathcal{C}} \le n$, то $T_\varphi^{\mathcal{F}} \le c_4 n$, где c_4 – константа, зависящая только от мощности множества $M\varphi$.

Доказательство : а) следует из существования константы, ограниченной мощностью множества M_A для любой аксиомы Фреге A. Доказательство пункта b) очевидно.

Следствие 2. С точностью до линейного слагаемого, верхние оценки числа шагов выводов в системе $\mathcal{C}$ выполняются для любой системы Фреге с теми же логическими символами.

Автор выражает благодарность участникам семинара под руководством И. Д. Заславского за ряд полезных советов.

ABSTRACT. Basing on Kalmar's prrof of the deductibility of tautologies inside classical propositional logic, we construct a complete axiom system $\mathcal{C}$ with properties : 1) every tautology φ can be deduced inside $\mathcal{C}$ in less than $c_1 2^m l$ steps, where $m = |M\varphi|$, $M\varphi$ is the characteristic set of subformulas of φ, l is the length of φ and c_1 is a constant ; 2) there exists a class of tautologies, such that the number of deduction steps in $\mathcal{C}$ is at least $c_2 2^m$, where c_2 is a constant.

ЛИТЕРАТУРА

1. A. Urquhart, "The complexity of propositional proofs", Bull. of Symbolic Logic, vol. 1, no. 4, pp. 425 – 467, 1995.
2. S. Buss, Propositional Proofs Complexity, an Introduction. Handbook of Proof Theory, North Holland, 1997.
3. P. Pudlak, "The lengths of proofs", Handbook of Proof Theory, North Holland, pp. 547 – 637, 1998.
4. Э. Мендельсон, Введение в Математическую Логику, Наука, Москва, 1971.
5. А. А. Чубарян, "О некоторой нормальной форме и сложностных характеристиках выводов в классическом исчислении высказываний", Изв. АН. Арм.ССР, серия Математика, том 10, № 5, стр. 398 – 409, 1975.
6. А. С. Аникеев, "О некоторой классификации выводимых пропорциональных формул", Матем. Заметки, том 2, № 2, стр. 165 – 174, 1972.

3 июля 1999 Ереванский государственный университет