Сибирский математический журнал
Март—апрель, 2009. Том 50, № 2

УДК 510.64

О ПОЛИНОМИАЛЬНЫХ ОГРАНИЧЕНИЯХ СЛОЖНОСТЕЙ ВЫВОДОВ В СИСТЕМАХ ФРЕГЕ

С. Р. Алексанян, А. А. Чубарян

Аннотация. Ранее одним из авторов было введено понятие определяющего множества переменных пропозициональной формулы, позволившее выделить множество *трудноопределяемых* тавтологий, сложности выводов которых в ряде систем доказательств классического исчисления высказываний (секвенциальной системе без правила сечения, системе резолюций, системе, основанной на методе расщепления, системе неравенств «Cutting planes», ограниченных системах Фреге) оцениваются снизу экспонентой от длины выводимой формулы. В настоящей работе доказывается, что для получения суперполиномиальной нижней оценки шагов (длины) выводов в системах Фреге наличия свойства трудноопределяемости недостаточно: приводится пример последовательности трудноопределяемых формул, имеющих полиномиально ограниченные сложности выводов в любой системе Фреге.

Ключевые слова: сложность вывода, система Фреге, определяющий конъюнкт, определяющее множество переменных пропозициональной формулы, трудноопределяемая формула.

1. Введение

Общеизвестно, что исследования сложностей выводов в пропозициональных системах важны в связи с их тесной связью с основной проблемой теории сложности: $P \stackrel{?}{=} NP$. В частности, Кук и Рехов доказали, что $NP = \mathrm{co}\,NP$ в том и только том случае, если существует система доказательств классических тавтологий, в которой длины выводов полиномиально ограничены [1]. Известны примеры формул (PHP_n, представляющих принцип «ящиков Дирихле» или «$\mathrm{Clique}_{n,k}$», описывающих связь хроматического числа графа с количеством вершин его максимального полного подграфа), для которых с применением разных интересных технических средств получены показательные нижние оценки сложностей их выводов в ряде систем доказательств классического исчисления высказываний (КИВ) [2]. Однако длины выводов этих формул в наиболее традиционных системах доказательств пропозициональной логики — системах Фреге — оказались полиномиально ограниченными [3, 4], поэтому исследование сложностей выводов именно в системах Фреге представляет большой интерес.

В работе [5] А. А. Чубарян введены понятия определяющего конъюнкта и определяющего множества переменных пропозициональной формулы и предложено оценивать сложностные характеристики выводов не только в зависимости от длины выводимой формулы, но и на основе двух параметров: длины формулы и количества переменных в определяющем ее множестве. Последнее обстоятельство позволило:

а) для достаточно широких классов формул существенно понизить верхние оценки сложностей выводов практически во всех известных системах доказательств КИВ [5–7];

б) сформулировать условие трудноопределяемости формулы, достаточное для наличия нижней показательной оценки сложностей выводов тавтологий в ряде систем доказательств КИВ [5, 7].

Были приведены также примеры формул, удовлетворяющих этому условию. Естественно, было интересно исследовать сложности выводов именно этих формул в системах Фреге, так как вышеупомянутые формулы PHP_n и «$\mathrm{Clique}_{n,k}$» указанному свойству не удовлетворяют (оно достаточное, но не необходимое).

В настоящей работе доказывается, что построенные примеры трудноопределяемых формул также имеют полиномиально ограниченные сложности выводов в системах Фреге.

Проблема $NP = \mathrm{co}\,NP$ была бы решена, если бы удалось доказать, что для всех формул с указанным свойством длины выводов в системах Фреге могут быть полиномиально ограничены.

Результаты настоящей работы доложены на двух международных конференциях и представлены в сборниках докладов [8, 9].

2. Предварительные понятия и результаты

Для доказательства основного результата напомним некоторые понятия и обозначения.

Мы будем пользоваться общепринятыми понятиями единичного n-мерного булева куба (E^n), пропозициональной формулы, тавтологии, системы доказательства КИВ, сложности выводов.

Конкретный выбор языка для представления пропозициональной формулы (а значит, и системы доказательств) не имеет значения для наших рассмотрений, однако из технических соображений мы предполагаем, что он содержит пропозициональные переменные p_i $(i \geq 1)$ и (или) p_{ij} $(i \geq 1,\ j \geq 1)$, логические связки $\neg$, $\&$, $\vee$, $\supset$ и пару скобок (,). В ряде случаев в целях упрощения записи формул некоторые скобки могут быть опущены согласно общепринятым правилам.

Длина формулы φ, определяемая как количество всех вхождений в нее логических связок, обозначается через $|\varphi|$. Очевидно, что линейной функцией от $|\varphi|$ оцениваются и полная длина формулы, понимаемая как количество всех символов, и количество вхождений переменных.

Тавтология φ называется *минимальной*, если она не может быть получена подстановкой из более короткой тавтологии.

Следуя общепринятой терминологии, *литералом* будем называть переменную или ее отрицание. Конъюнкт K может быть представлен как множество литералов, причем это множество не может содержать переменную и ее отрицание одновременно.

В работе [5] введены следующие понятия.

Для произвольной пропозициональной формулы ψ следующие тривиальные эквивалентности назовем *правилами замещения*:

$$
\begin{aligned}
&0\&\psi=0,\ \ \psi\&0=0,\ \ 1\&\psi=\psi,\ \ \psi\&1=\psi,\ \ \psi\&\psi=\psi,\ \ \psi\&\bar{\psi}=0,\ \ \bar{\psi}\&\psi=0,\\
&0\vee\psi=\psi,\ \psi\vee 0=\psi,\ 1\vee\psi=1,\ \psi\vee 1=1,\ \psi\vee\psi=\psi,\ \psi\vee\bar{\psi}=1,\ \bar{\psi}\vee\psi=1,\\
&0\supset\psi=1,\ \psi\supset 0=\bar{\psi},\ 1\supset\psi=\psi,\ \psi\supset 1=1,\ \psi\supset\psi=1,\ \psi\supset\bar{\psi}=\bar{\psi},\ \bar{\psi}\supset\psi=\psi,\\
&\bar{0}=1,\qquad \bar{1}=0,\qquad \bar{\bar{\psi}}=\psi.
\end{aligned}
$$

Применение правил замещения к некоторому слову заключается в замене какого-либо его подслова, имеющего вид левой части одного из указанных эквивалентностей, правой частью.

Пусть φ — пропозициональная формула, $P=\{p_1,p_2,\dots,p_n\}$ — множество ее различных переменных, а $P'=\{p_{i_1},p_{i_2},\dots,p_{i_m}\}$ $(1\le m\le n)$ — некоторое подмножество P.

Определение 1. Для некоторого $\sigma=\{\sigma_1,\dots,\sigma_m\}\in E^m$ конъюнкт $K^\sigma=\{p_{i_1}^{\sigma_1},p_{i_2}^{\sigma_2},\dots,p_{i_m}^{\sigma_m}\}$[1)] называется *$\varphi$-определяющим*, если, подставляя в φ вместо каждой переменной p_{i_j} значение σ_j $(1\le j\le m)$ и последовательно применяя правила замещения, получаем значение формулы φ (0 или 1) вне зависимости от значений остальных переменных.

Примеры. 1. Для формул $p_1\supset(p_2\supset(\dots\supset(p_{k-1}\supset p_k)\dots))$ $(k\ge 3)$ определяющими являются, в частности, конъюнкты $\{p_k\}$, $\{\bar{p}_1\}$, $\{\bar{p}_{k-1}\}$, $\{p_{k-1},p_k\}$, $\{p_1,p_2,\dots,p_k\}$.

2. Для известных тавтологий

$$PHP_n=\mathop{\&}_{i=1}^{n+1}\bigvee_{j=1}^{n}p_{ij}\supset\bigvee_{1\le i<k\le n+1}\ \bigvee_{1\le j\le n}(p_{ij}\,\&\,p_{kj})\quad(n\ge 1),$$

выражающих принцип «ящиков Дирихле», определяющими являются, в частности, конъюнкты $\{p_{11},p_{21}\}$, $\{\bar{p}_{11},\bar{p}_{12},\dots,\bar{p}_{1n}\}$.

3. В дальнейших рассмотрениях важную роль играют тавтологии

$$\Pi M_{n,m}=\bigvee_{(\sigma_1,\dots,\sigma_n)\in E^n}\ \mathop{\&}_{j=1}^{m}\bigvee_{i=1}^{n}p_{ij}^{\sigma_i}\quad(n\ge 1,\ 1\le m\le 2^n-1),$$

которые при каждых фиксированных $n\ge 1$ и m из указанных интервалов «выражают» следующее истинное утверждение: в каждой $0,1$-матрице размера $n\times m$ можно так «перевернуть» строки (заменить 0 на 1 и 1 на 0), чтобы в каждом столбце была по крайней мере одна единица. В силу структуры $\Pi M_{n,m}$ очевидно, что каждый $\Pi M_{n,m}$-определяющий конъюнкт содержит по крайней мере m литералов.

Как видно из примеров, каждая формула φ может иметь много φ-определяющих конъюнктов, отличающихся как по количеству, так и по составу литералов.

Определение 2. Минимально возможное количество переменных в φ-определяющем конъюнкте назовем *определяющей длиной формулы* φ и будем обозначать через $d(\varphi)$.

[1)] Для пропозициональной переменной p и $\sigma\in E^1$ через p^σ, как принято, обозначена функция $p^\sigma=\begin{cases}p, & \text{если } \sigma=1,\\ \bar{p}, & \text{если } \sigma=0.\end{cases}$

Очевидно, для произвольной формулы φ будет $d(\varphi) < |\varphi|$, и чем меньше разность между этими величинами, тем более «трудной» можно считать формулу φ.

Определение 3. Пусть φ_n $(n \geq 1)$ — последовательность минимальных тавтологий. Если для некоторого n_0 можно указать такую константу c, что

$$\forall n \geq n_0 \quad n \cdot (d(\varphi_n))^c \leq |\varphi_n| < n \cdot (d(\varphi_n))^{c+1},$$

то формулы $\varphi_{n_0}, \varphi_{n_0+1}, \varphi_{n_0+2}, \ldots$ назовем *трудноопределяемыми.*

Утверждение 1. *Пусть $\varphi_n = \Pi M_{n,2^n-1}$ для каждого $n \geq 1$. Тогда формулы $\varphi_3, \varphi_4, \ldots$ трудноопределяемы.*

Действительно, во-первых, нетрудно убедиться, что каждая из формул φ_n является минимальной тавтологией, и, во-вторых, так как $d(\varphi_n) = 2^n - 1$ и $|\varphi_n| = n(2^n-1) \cdot 2^n + n \cdot 2^{n-1} = n(2^{2n} - 2^{n-1})$, то $n(2^n-1)^2 \leq n(2^{2n} - 2^{n-1})$ для каждого $n \geq 1$ и $n(2^{2n} - 2^{n-1}) < n(2^n-1)^3$ для $n \geq 3$, следовательно, при $n_0 = 3$ и $c = 2$ удовлетворено условие трудноопределяемости. □

Отметим также, что формулы PHP_n и «$\mathrm{Clique}_{n,k}$» не являются трудноопределяемыми ни для одного из значений параметров n, так как $d(PHP_n) = 2$ и $d($«$\mathrm{Clique}_{n,k}$»$) = 3$.

В теории сложности выводов принято рассматривать две основные характеристики выводов: t-сложность, определяемую как количество шагов вывода, и ℓ-сложность, определяемую как общее количество символов вывода.

В [5, 7] доказано, что в некоторых системах доказательств КИВ (системах с правилом резолюции, секвенциальных системах без правила сечения, системах, основанных на правиле расщепления, ограниченных системах Фреге и ряде других) наименьшая t-сложность (и тем более наименьшая ℓ-сложность) произвольной минимальной тавтологии φ не менее $2^{d(\varphi)}$, в силу чего трудноопределяемость тавтологии является условием, при наличии которого сложностные характеристики выводов φ в указанных системах оцениваются снизу экспонентой от длины φ.

В настоящей работе исследованы сложностные характеристики выводов трудноопределяемых формул в системах Фреге, для которых до настоящего времени не выявлено тавтологий с суперполиномиальной нижней оценкой сложностей выводов.

3. Сложности выводов трудноопределяемых формул в системах Фреге

Напомним общепринятые понятия системы Фреге (см. например, [2]).

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

Не нарушая общности, предположим, что $\mathscr{F}$ такая система Фреге, которая содержит в своем языке связки $\neg$, $\&$, $\vee$, $\supset$, быть может, наряду с другими, и правило Modus ponens является одним из ее правил вывода.

Минимально возможное значение t-сложности (ℓ-сложности) вывода в системе $\mathscr{F}$ ($\mathscr{F}$-выводе) тавтологии φ обозначим через $t_{\varphi}^{\mathscr{F}}$ $\left(\ell_{\varphi}^{\mathscr{F}}\right)$.

Определение 4. Выводы тавтологий множества Φ назовем *t-полиномиально* (*ℓ-полиномиально*) *ограниченными*, если существует такой полином $\mathbf{p}(\,)$, что $t_{\varphi}^{\mathscr{F}} \leq \mathbf{p}(|\varphi|)$ $(\ell_{\varphi}^{\mathscr{F}} \leq \mathbf{p}(|\varphi|))$ для каждой тавтологии φ из множества Φ.

Поскольку величина $d(\varphi)$ для ряда систем доказательств КИВ играет важную роль в оценке сложностей выводов формулы φ, интересно исследовать взаимосвязь между $t_{\varphi}^{\mathscr{F}}$, $\ell_{\varphi}^{\mathscr{F}}$ и $d(\varphi)$.

Утверждение 2. (а) *Для любой минимальной тавтологии φ справедливы неравенства $d(\varphi) \leq \ell_{\varphi}^{\mathscr{F}}$ и $d(\varphi) \leq c \cdot t_{\varphi}^{\mathscr{F}}$ для некоторой константы c.*

(б) *Существуют такие трудноопределяемые формулы φ_n, что $t_{\varphi_n}^{\mathscr{F}} \leq \ell_{\varphi_n}^{\mathscr{F}} \leq \mathbf{p}(d(\varphi_n))$ для некоторого полинома $\mathbf{p}(\,)$.*

Первое неравенство п. (а) тривиально. Для доказательства второго воспользуемся понятием существенной подформулы тавтологии, введенным в [6]. Напомним, что подформула ψ тавтологии φ называется *существенной*, если результат повсеместной замены в φ подформулы ψ переменной, не содержащейся в φ, не является тавтологией. Очевидно, что каждая неэлементарная подформула минимальной тавтологии существенна.

В [6] доказано, что количество существенных подформул тавтологии φ не превышает $ct_{\varphi}^{\mathscr{F}}$ для произвольной системы Фреге $\mathscr{F}$ и константы c, зависящей только от выбора системы, но тогда количество пропозициональных переменных формулы φ, а значит, и $d(\varphi)$ не больше, чем $ct_{\varphi}^{\mathscr{F}}$. $\square$

Доказательство п. (б) будет получено в качестве следствия из теоремы, которая приводится далее. В частности, будет доказано, что трудноопределяемость формулы не является достаточным условием для получения нижней экспоненциальной оценки сложностных характеристик выводов в системах Фреге, т. е. свойство трудноопределяемости формулы может быть «достигнуто» в системах Фреге с полиномиально ограниченной сложностью вывода.

Теорема. *$\mathscr{F}$-выводы тавтологий*

$$\Pi M_{n,m} = \bigvee_{(\sigma_1,\dots,\sigma_n)\in E^n} \mathop{\&}_{j=1}^{m} \bigvee_{i=1}^{n} p_{ij}^{\sigma_i} \quad n \geq 1,\ 1 \leq m \leq 2^n - 1,$$

t-полиномиально (ℓ-полиномиально) ограничены.

Для доказательства этого утверждения будет показано, что для всех n и m из указанных интервалов $\mathscr{F}$-выводы формул $\Pi M_{n,m}$ могут быть «полиномиально сведены» к $\mathscr{F}$-выводам уже упоминаемых формул PHP_m, а в [3] доказано, что $\mathscr{F}$-выводы формул PHP_m ℓ-полиномиально (а следовательно, и t-полиномиально) ограничены.

Будут использованы следующие два вспомогательных утверждения.

Лемма 1. *$\mathscr{F}$-выводы следующего множества тавтологий:*
1) $\alpha \vee \bar{\alpha}$,
2) $\alpha \supset \alpha \vee \beta$,
3) $(\alpha \supset \beta) \supset ((\beta \supset \gamma) \supset (\alpha \supset \gamma))$,
4) $(\bar{\beta} \supset \alpha) \supset (\bar{\alpha} \supset \beta)$,
5) $\alpha_1 \supset (\alpha_2 \supset (\ldots \supset (\alpha_k \supset \alpha_1 \,\&\, \alpha_2 \,\&\, \ldots \,\&\, \alpha_k) \ldots))$ $(k \geq 2)$,

6) $\alpha \vee \bar{\alpha} \supset \beta_1 \vee \ldots \vee \beta_k \vee \alpha \vee \beta_{k+1} \vee \ldots \vee \beta_{k+r} \vee \bar{\alpha} \vee \beta_{k+r+1} \vee \ldots \vee \beta_{k+r+t}$ $(k \geq 1, r \geq 1, t \geq 1)$,

7) $\neg \left(\bigvee_{i=1}^{k} \mathop{\&}_{i=1}^{m} \alpha_{ij} \right) \supset \mathop{\&}_{i=1}^{k} \bigvee_{j=1}^{m} \bar{\alpha}_{ij}$ $(k \geq 1, m \geq 1)$

8) $\mathop{\&}_{i=1}^{k} (\beta_{1i} \vee \beta_{2i}) \supset \neg \left(\bigvee_{i=1}^{k} (\bar{\beta}_{1i} \,\&\, \bar{\beta}_{2i}) \right)$ $(k \geq 1)$,

где α, β, γ, α_i, β_i, α_{ij}, β_{ij} — произвольные формулы, t-полиномиально (ℓ-полиномиально) ограничены.

Доказательство очевидно. □

Для $1 \leq i \leq 2^n$ и $1 \leq j \leq m$ положим $q_{i,j} = p_{1j}^{\sigma_{i1}} \vee p_{2j}^{\sigma_{i2}} \vee \ldots \vee p_{nj}^{\sigma_{in}}$, где $\sigma_{i1}, \sigma_{i2}, \ldots, \sigma_{in}$ — двоичное представление числа $2^n - i$.

Лемма 2. *$\mathscr{F}$-выводы формул $q_{i,j} \vee q_{k,j}$ $(1 \leq j \leq m, 1 \leq i < k \leq 2^n)$ t- (ℓ-) полиномиально ограничены.*

Доказательство следует из факта существования такого s $(1 \leq s \leq n)$, что q_{ij} содержит p_{sj}, а q_{kj} содержит $\bar{p}_{sj}$, и из утверждений пп. 1, 6 леммы 1. □

Используя обозначение q_{ij}, формулу $\Pi M_{n,m}$ можно представить в виде

$$\Pi M_{n,m} = \bigvee_{i=1}^{2^n} \mathop{\&}_{j=1}^{m} q_{i,j}.$$

Пусть $\psi_{n,m}$ — следующая подформула формулы $\Pi M_{n,m}$:

$$\psi_{n,m} = \bigvee_{i=1}^{m+1} \mathop{\&}_{j=1}^{m} q_{i,j}.$$

Из п. 7 леммы 1 вытекает

Свойство 1. *$\mathscr{F}$-выводы формул $\bar{\psi}_{n,m} \supset \mathop{\&}_{i=1}^{m+1} \bigvee_{j=1}^{m} \bar{q}_{i,j}$ t- (ℓ-) полиномиально ограничены.*

Пусть

$$PHP'_m = \mathop{\&}_{i=1}^{m+1} \bigvee_{j=1}^{m} \bar{q}_{i,j} \supset \bigvee_{1 \leq i < k \leq m+1} \bigvee_{1 \leq j \leq m} (\bar{q}_{i,j} \,\&\, \bar{q}_{k,j}). \tag{1}$$

Формулы (1) получены соответствующими подстановками из PHP_m. Отсюда вытекает

Свойство 2. *$\mathscr{F}$-выводы формул (1) t- (ℓ-) полиномиально ограничены.*

Пусть

$$A_{n,m} = \bigvee_{1 \leq i < k \leq m+1} \bigvee_{1 \leq j \leq n} (\bar{q}_{i,j} \,\&\, \bar{q}_{k,j}).$$

Используя свойства (1), (2) и п. 3. леммы 1, получим

Свойство 3. *$\mathscr{F}$-выводы формул $\bar{\psi}_{n,m} \supset A_{n,m}$ t- (ℓ-) полиномиально ограничены.*

Из утверждения леммы 2 и п. 5 леммы 1 вытекает

Свойство 4. *$\mathscr{F}$-выводы формул*

$$B_{n,m} = \mathop{\&}_{1\le i<k\le m+1} \mathop{\&}_{1\le j\le n} (q_{i,j} \vee q_{k,j})$$

t- (ℓ-) полиномиально ограничены, и из утверждения п. 8 *леммы* 1 *следует, что $\mathscr{F}$-выводы формулы $\neg A_{n,m}$ также t- (ℓ-) полиномиально ограничены.*

Из свойств (3), (4) и п. 4 леммы 1 вытекает t- (ℓ-) полиномиальная ограниченность $\mathscr{F}$-выводов $\psi_{n,m}$, и, наконец, из п. 2 леммы 1 — доказательство теоремы. □

Учитывая трудноопределяемость формул φ_n из утверждения 1, получим

Следствие. *Существуют трудноопределяемые формулы, $\mathscr{F}$-выводы которых t- (ℓ-) полиномиально ограничены.*

Используя введенные в этой работе понятия, результаты § 2 работы [5] о сложностях выводов в системах Фреге и полиномиальную эквивалентность различных систем Фреге [2], можно перефразировать вышеупомянутый результат Кука и Рехова: $NP = \mathrm{co}\, NP$ тогда и только тогда, когда в некоторой системе Фреге длины выводов всех трудноопределяемых формул полиномиально ограничены.

Авторы выражают признательность анонимному рецензенту, критические замечания которого позволили существенно улучшить изложение всей работы.

ЛИТЕРАТУРА

1. *Cook S. A., Reckhow A. R.* The relative efficiency of propositional proof systems // J. Symbol. Logic. 1979. V. 44. P. 36–50.
2. *Pudlak P.* The lengths of proofs // Handbook of proof theory. Amsterdam: North-Holland, 1998. P. 547–637.
3. *Buss S. R.* Polynomial size proofs of the propositional pigeonhole principle // J. Symbol. Logic. 1987. V. 52. P. 916-927.
4. *Razborov A.* Lower bounds for propositional proofs and independence results in Bounded Arithmetic // Proc. of the 23-rd ICALP, 1099. New York; Berlin: Springer-Verl., 1996. P. 48–62.
5. *Chubaryan A. A.* On the proof complexity in some system of classical propositional logic // Izv. NAN Armenii, Mathematika. 1999. V. 37, N 5. P. 16–26.
6. *Чубарян А. А.* О сложности выводов в некоторых системах классического исчисления высказываний // Мат. вопросы кибернетики. 2005. № 14. С. 49–56.
7. *Chubaryan A. A.* Relative efficiency of a proof system in classical propositional logic // Izv. NAN Armenii. Mathematika. 2002. V. 37, N 5. P. 71–84.
8. *Aleksanyan S., Chubaryan A.* On some properties of Frege proofs // CSIT-2005, Yerevan, P. 45–46.
9. *Aleksanyan S., Chubaryan An.* On determinative complexity of Frege proofs // XIV Intern. conf. on LPAP: Proc. of the short papers session, 2007, Yerevan, P. 5–11.

Статья поступила 2 февраля 2008 г., окончательный вариант — 8 октября 2008 г.

Алексанян Сона Рафиковна
факультет прикладной математики ГИУА,
ул. Терьяна, 105, Ереван 375075, Армения
`sonush@rambler.ru`

Чубарян Анаит Арташесовна
факультет информатики и прикладной математики ЕГУ,
ул. А. Манукяна, 1, Ереван 375049, Армения
`achubaryan@ysu.am`