

Об одной системе Фреге

Г. В. Боков

В работе рассматривается система Фреге в сигнатуре $\{\wedge, \vee, \neg\}$. Для данной системы доказывается нетривиальная нижняя оценка длины минимального вывода.

Ключевые слова: Системы Фреге, длина вывода, нижние оценки.

Основные понятия и результаты

Понятие формулы в сигнатуре Σ (или Σ -формулы) определяется стандартным образом. Обозначим через Fm множество всех формул в сигнатуре $\{\wedge, \vee, \neg\}$. Для $A \in \text{Fm}$ через $|A|$ будем обозначать суммарное число логических символов и символов переменных в формуле A . Подмножество всех тавтологий в Fm будем обозначать через Th .

Правилом Фреге будем называть конечный набор формул $\langle A_1, \dots, A_n; B \rangle$, удовлетворяющих условию

$$A_1, \dots, A_n \models B,$$

т.е. для любой подстановки σ формула $\sigma B \in \text{Th}$ всякий раз, когда $\sigma A_1, \dots, \sigma A_n \in \text{Th}$.

Пусть \mathcal{F} — это множество правил Фреге. Будем говорить, что формула $C \in \text{Fm}$ \mathcal{F} -выводима из множества формул $M = \{D_1, \dots, D_m\} \subseteq \text{Fm}$ и обозначать это как

$$D_1, \dots, D_m \vdash_{\mathcal{F}} C,$$

если существует конечная последовательность формул F_1, \dots, F_l , которую будем называть \mathcal{F} -выводом C из M , для которой $F_l = C$ и каждый ее элемент F_k либо принадлежит M , либо выводим из элементов $F_i, i < k$, с помощью некоторого правила из \mathcal{F} , т.е. существуют такое правило $\langle A_1, \dots, A_n; B \rangle$ из \mathcal{F} и такая подстановка σ , что $\sigma B = F_k$ и для каждого $i \leq n$ существует такое $j < k$, что $\sigma A_i = F_j$. При этом число l называется *длиной* \mathcal{F} -вывода F_1, \dots, F_l . \mathcal{F} -доказательством формулы A будем называть всякий \mathcal{F} -вывод A из пустого множества. При этом формулу, имеющую \mathcal{F} -доказательство, назовем *выводимой* или *доказуемой* в \mathcal{F} . Множество всех доказуемых в \mathcal{F} формул обозначим через $[\mathcal{F}]$. Из определения правил Фреге следует, что

$$A_1, \dots, A_n \vdash_{\mathcal{F}} B \implies A_1, \dots, A_n \models B.$$

Поэтому всякая доказуемая в \mathcal{F} формула является тавтологией, т.е. $[\mathcal{F}] \subseteq \text{Th}$. Конечное множество правил Фреге \mathcal{F} будем называть *системой Фреге*, если любая тавтология из Th имеет \mathcal{F} -доказательство, т.е. $[\mathcal{F}] = \text{Th}$. В теории сложности [3, 5, 6] важную роль играют системы Фреге, для которых выполнено условие

$$A_1, \dots, A_n \models B \implies A_1, \dots, A_n \vdash_{\mathcal{F}} B.$$

Такие системы Фреге называют *импликативно-полными*.

Введем меру сложности систем Фреге. Обозначим через $L_{\mathcal{F}}(A)$ длину наименьшего \mathcal{F} -доказательства формулы A и введем функцию Шеннона:

$$L_{\mathcal{F}}(n) = \max_{A \in \text{Th}: |A| \leq n} L_{\mathcal{F}}(A).$$

В настоящее время для импликативно-полных систем Фреге \mathcal{F} известна только линейная по n нижняя оценка для $L_{\mathcal{F}}(n)$ [4]. В данной работе будет показано, что без требования импликативной полноты может быть доказана экспоненциальная нижняя оценка.

Определим множество правил Фреге \mathcal{F}_0 , состоящее из следующих групп:

Группа Υ_1 :

$$\frac{}{x_1 \vee \neg x_1}, \quad \frac{}{x_1 \vee \neg x_1 \vee x_2};$$

Группа Υ_\wedge :

$$\frac{x_1, x_2}{x_1 \wedge x_2}, \quad \frac{x_1 \vee x_3, x_2 \vee x_3}{(x_1 \wedge x_2) \vee x_3};$$

Группа Υ_\vee :

$$\frac{x_1 \vee x_2}{x_2 \vee x_1}, \quad \frac{(x_1 \vee x_2) \vee x_3}{x_1 \vee (x_2 \vee x_3)}, \quad \frac{x_1 \vee (x_2 \vee x_3)}{(x_1 \vee x_2) \vee x_3};$$

Группа Υ_\neg :

$$\frac{\neg x_1 \vee \neg x_2}{\neg(x_1 \wedge x_2)}, \quad \frac{\neg x_1 \vee \neg x_2 \vee x_3}{\neg(x_1 \wedge x_2) \vee x_3},$$

$$\frac{\neg x_1, \neg x_2}{\neg(x_1 \vee x_2)}, \quad \frac{\neg x_1 \vee x_3, \neg x_2 \vee x_3}{\neg(x_1 \vee x_2) \vee x_3},$$

$$\frac{x_1}{\neg\neg x_1}, \quad \frac{x_1 \vee x_2}{\neg\neg x_1 \vee x_2}.$$

Главным результатом работы является следующая теорема.

Теорема 1. \mathcal{F}_0 является системой Фреге, для которой

$$L_{\mathcal{F}_0}(n) \geq 2^{\sqrt[3]{n}}$$

при $n \geq 2^7$.

Доказательство Теоремы 1

Для начала докажем, что множество \mathcal{F}_0 является системой Фреге.

Лемма 1. \mathcal{F}_0 является системой Фреге.

Доказательство. Для доказательства леммы достаточно показать, что для любой тавтологии A в сигнатуре $\{\wedge, \vee, \neg\}$ существует \mathcal{F}_0 -доказательство. Поскольку $\Upsilon_\vee \subseteq \mathcal{F}_0$, то без ограничения общности будем считать, что A имеет вид $A_1 \vee \dots \vee A_n$, где

A_i — это формула, не представляемая в виде $B \vee C$, для любого $1 \leq i \leq n$.

Доказательство будем проводить индукцией по суммарному взвешенному числу символов \neg , \wedge , \vee в формулах A_1, \dots, A_n , полагая вес \neg равным 1, а веса \wedge и \vee равными 2. Если $A_i = x$ и $A_j = \neg x$ для некоторой переменной x , то легко убедиться, что A выводима в \mathcal{F}_0 с помощью правил $\Upsilon_1 \cup \Upsilon_\vee$. В противном случае возможны следующие случаи:

1) $A_i = A_{i,1} \wedge A_{i,2}$. Тогда A выводима из тавтологий

$$B_j = A_1 \vee \dots \vee A_{i,j} \vee \dots \vee A_n, \quad j \in \{1, 2\},$$

с помощью правил $\Upsilon_\wedge \cup \Upsilon_\vee$;

2) $A_i = \neg(A_{i,1} \vee A_{i,2})$. Тогда A выводима из тавтологий

$$B_j = A_1 \vee \dots \vee \neg A_{i,j} \vee \dots \vee A_n, \quad j \in \{1, 2\},$$

с помощью правил $\Upsilon_\neg \cup \Upsilon_\vee$;

3) $A_i = \neg(A_{i,1} \wedge A_{i,2})$. Тогда A выводима из тавтологии

$$B_1 = A_1 \vee \dots \vee \neg A_{i,1} \vee \neg A_{i,2} \vee \dots \vee A_n$$

с помощью правил $\Upsilon_\neg \cup \Upsilon_\vee$;

4) $A_i = \neg\neg B_1$. Тогда A выводима из тавтологии B_1 с помощью правил $\Upsilon_\neg \cup \Upsilon_\vee$.

По индуктивному предположению формулы B_j имеют \mathcal{F}_0 -доказательства. Следовательно, A также имеет \mathcal{F}_0 -доказательство. \square

Литералом будем называть переменную либо ее отрицание. Каждой переменной x соответствуют два литерала x и $\neg x$, которые для краткости будем обозначать в виде:

$$x^a = \begin{cases} x, & a = 1; \\ \neg x, & a = 0. \end{cases}$$

Поскольку далее будут рассматривать только $\{\wedge, \vee\}$ -формулы над литералами, то условимся считать, что формула x^a не является подформулой в $x^{\bar{a}}$, где $a \in \{0, 1\}$ и

$$\bar{x} = \begin{cases} 1, & x = 0; \\ 0, & x = 1. \end{cases}$$

Для произвольного множества M обозначим через M^* множество всех слов конечной длины в алфавите M . Длину слова $\alpha \in M^*$ будем обозначать через $|\alpha|$. Также определим

$$M^n = \{\alpha \in M^* \mid |\alpha| = n\}, \quad M^{\leq n} = \{\alpha \in M^* \mid |\alpha| \leq n\}, \\ M^{< n} = \{\alpha \in M^* \mid |\alpha| < n\}.$$

Кроме того, для $\alpha, \beta \in M^*$ будем писать $\alpha \preceq \beta$ ($\alpha \prec \beta$), если α является (собственным) началом β , т.е. $\beta = \alpha\gamma$ для некоторого (непустого) $\gamma \in M^*$. Полагаем $\alpha \succeq \beta$ ($\alpha \succ \beta$), если $\beta \preceq \alpha$ ($\beta \prec \alpha$).

Определим семейство формул F_α для непустого $\alpha \in \{0, 1\}^*$. Если $\alpha = a \in \{0, 1\}$, то $F_\alpha = x_1^a$, в противном случае $\alpha = \beta a$ для некоторых $|\beta| > 0$ и $a \in \{0, 1\}$ и тогда

$$F_\alpha = F_\beta \wedge x_{1\beta}^a$$

при нечетном $|\alpha|$ и

$$F_\alpha = F_\beta \vee x_{1\beta}^a$$

при четном $|\alpha|$, где $x_{1\beta}$ — это переменная, двоичная запись номера которой совпадает со словом 1β .

Зафиксируем $k \geq 1$ и определим семейство формул G_α для $\alpha \in \{0, 1\}^{\leq 2k}$. Если $|\alpha| = 2k$, то $G_\alpha = F_\alpha$, в противном случае

$$G_\alpha = G_{\alpha 0} \wedge G_{\alpha 1}$$

при нечетном $|\alpha|$ и

$$G_\alpha = G_{\alpha 0} \vee G_{\alpha 1}$$

при четном $|\alpha|$. Нетрудно убедиться, что для непустого $\alpha \in \{0, 1\}^{\leq 2k}$ формулы F_α и G_α задают одну и ту же булеву функцию, а формула G_ε является тавтологией.

Формулу $A \in \text{Fm}$ будем называть *линейной*, если каждая переменная в A имеет единственное вхождение. Определим множество \mathcal{F}_1 , состоящее из правил Фреге вида

$$\frac{A_1(x, z_1, \dots, z_n), \quad A_2(y, z_1, \dots, z_n)}{B(x \wedge y, z_1, \dots, z_n)} \quad (1)$$

для любых линейных $\{\vee\}$ -формул A_1, A_2 и B от $n+1$ переменных и $0 \leq n \leq N$, а также правил вида

$$\frac{}{A(x, \neg x, z_1, \dots, z_n)} \quad (2)$$

для произвольной линейной $\{\vee\}$ -формулы A от $n+2$ переменных и произвольного $0 \leq n \leq N$, где N — число символов в формуле G_ε .

Лемма 2. $L_{\mathcal{F}_0}(G_\varepsilon) \geq L_{\mathcal{F}_1}(G_\varepsilon)$.

Доказательство. Рассмотрим произвольный минимальный вывод $\Gamma = A_1, \dots, A_n$ формулы G_ε в системе \mathcal{F}_0 .

Для начала докажем индукцией по s от n до 1, что всякое вхождение символа \neg в формулу A_s является вхождением литерала $\neg x$ для некоторой переменной x . Для $s = n$ это верно, т.к. $A_n = G_\varepsilon$. Пусть утверждение верно для всех $s' > s$, докажем его для s . Так как Γ является минимальным выводом, то существует такое $s' > s$, что $A_{s'}$ является результатом применения правила $\omega \in \Upsilon_\wedge \cup \Upsilon_\vee \cup \Upsilon_\neg$ к A_s и, возможно, другим элементам из Γ . По предположению индукции всякое вхождение символа \neg в формулу $A_{s'}$ является вхождением некоторого литерала, поэтому $\omega \notin \Upsilon_\neg$. Так как правила из $\Upsilon_\wedge \cup \Upsilon_\vee$ не нарушают этого свойства, то всякое вхождение символа \neg в формулу A_s также является вхождением некоторого литерала. Таким образом, правила Υ_\neg не участвуют в выводе Γ .

Теперь докажем индукцией по s от 1 до n , что существует подпоследовательность A_{i_1}, \dots, A_{i_m} в выводе Γ , которая является выводом A_s в системе \mathcal{F}_1 .

Если $k = 1$, то A_1 есть результат применения правила из $\Upsilon_1 \subseteq \mathcal{F}_1$. Поэтому для $i_1 = 1$ утверждение верно. Пусть $k > 1$. Возможны два случая:

1) A_s получена с помощью правила группы Υ_{\wedge} из формул A_i и A_j для некоторых $1 \leq i, j < s$. По индуктивному предположению мы можем объединить выводы A_i и A_j в системе \mathcal{F}_1 в одну последовательность A_{i_1}, \dots, A_{i_m} . Так как $\Upsilon_{\wedge} \subseteq \mathcal{F}_1$, то последовательность $A_{i_1}, \dots, A_{i_m} A_s$ является выводом формулы A_s в \mathcal{F}_1 .

2) A_s получена с помощью правила группы Υ_{\vee} из формулы A_i для некоторого $1 \leq i < s$. По предположению индукции существует подпоследовательность A_{i_1}, \dots, A_{i_m} , которая является выводом A_i в \mathcal{F}_1 . Нетрудно убедиться, что данная подпоследовательность также является выводом формулы A_s в \mathcal{F}_1 .

Таким образом, в системе \mathcal{F}_1 существует вывод формулы G_{ε} , длина которого не превосходит n . Так как Γ является минимальным выводом формулы G_{ε} в \mathcal{F}_0 , то $L_{\mathcal{F}_0}(G_{\varepsilon}) \geq L_{\mathcal{F}_1}(G_{\varepsilon})$. \square

Конфигурацией веса $k \geq 1$ будем называть пару $\mathfrak{r} = \langle R, \varphi \rangle$, где R — непустое подмножество $\{0, 1\}^{<2^k}$ и $\varphi: R \setminus \{\varepsilon\} \rightarrow \{0, 1\}$, удовлетворяющую следующим условиям:

- 1) если $\alpha a \in R$, то $\alpha \in R$;
- 2) если $\alpha a \in R$ и $|\alpha| \geq k$, то $a = 0$;
- 3) если $\alpha \beta \in R$ и $|\alpha| = k + 1$, то $\varphi(\alpha \gamma) = 0$ для любого $\gamma \prec \beta$.

Обозначим через \mathfrak{R}_k множество всех конфигураций веса k и определим *мощность* конфигурации $|\mathfrak{r}| = |R|$. Заметим, что множество \mathfrak{R}_k конечно для любого $k \geq 1$.

Пусть $\mathfrak{r} = \langle R, \varphi \rangle \in \mathfrak{R}_k$ — некоторая конфигурация. *Терминалом* конфигурации \mathfrak{r} будем называть всякое $\alpha \in R$ такое, что $\alpha i \notin R$ для некоторого $i \in \{0, 1\}$. Далее мы каждому терминалу α конфигурации \mathfrak{r} , сопоставим формулу $\psi_{\alpha}^{\mathfrak{r}}$ и множество формул $\rho_{\alpha}^{\mathfrak{r}}$. Возможны два случая:

1) Если $\alpha = \beta 0^{k-s}$, где $1 \leq s \leq k$, $\beta = a_1 a_3 \dots a_{2k-1}$ и $\varphi(a_1 a_3 \dots a_{2i-1}) = a_{2i}$ для всех $i \in \{1, \dots, k\}$, то определим

$$\psi_{\alpha}^{\mathfrak{r}} = F_{a_1, \dots, a_{2s-1}} \vee x_{1a_1 \dots a_{2s-1}}^{a_{2s}} \vee x_{1a_1 \dots a_{2s+1}}^{a_{2s+2}} \vee \dots \vee x_{1a_1 \dots a_{2k-1}}^{a_{2k}},$$

$$\rho_{\alpha}^{\mathfrak{r}} = \left\{ x_{1a_1 \dots a_{2s-1}}^{a_{2s}} \vee x_{1a_1 \dots a_{2s+1}}^{a_{2s+2}} \vee \dots \vee x_{1a_1 \dots a_{2k-1}}^{a_{2k}} \right\}$$

если $\varphi(\alpha) = 0$ либо $s = k$ и

$$\begin{aligned}\psi_\alpha^r &= x_{1a_1 \dots a_{2s}}^{a_{2s+1}} \vee x_{1a_1 \dots a_{2s+1}}^{a_{2s+2}} \vee \dots \vee x_{1a_1 \dots a_{2k-1}}^{a_{2k}}, \\ \rho_\alpha^r &= \left\{ x_{1a_1 \dots a_{2s}}^{a_{2s+1}} \vee x_{1a_1 \dots a_{2s+1}}^{a_{2s+2}} \vee \dots \vee x_{1a_1 \dots a_{2k-1}}^{a_{2k}} \right\}\end{aligned}$$

иначе.

2) Если $\alpha = a_1 a_3 \dots a_{2s-1}$, $s < k$ и $\varphi(a_1 a_3 \dots a_{2i-1}) = a_{2i}$ для всех $i \in \{1, \dots, s\}$, то определим

$$\begin{aligned}\psi_\alpha^r &= G_{a_1 \dots a_{2s}}, \\ \rho_\alpha^r &= \left\{ x_{1a_1 \dots a_{2s} b_{2s+1} \dots b_{2k-1}}^{b_{2k}} \mid b_{2s+1}, \dots, b_{2k} \in \{0, 1\} \right\}.\end{aligned}$$

Если $\alpha_1, \dots, \alpha_t$ — это все терминалы конфигурации τ в лексикографическом порядке, то через ψ^r будем обозначать формулу

$$\psi_{\alpha_1}^r \vee \dots \vee \psi_{\alpha_t}^r.$$

При этом t назовем *терминальным числом* конфигурации τ и обозначим через τ_r .

Будем говорить, что две формулы A и B \vee -эквивалентны и записывать это как $A \sim_\vee B$, если одну из них можно получить через другую с помощью правил Υ_\vee . Для вывода Γ и формулы $A \in \Gamma$ обозначим через Γ_A минимальную подпоследовательность в Γ , которая является выводом A .

Лемма 3. Если Γ — вывод G_ε в \mathcal{F}_1 , то для любого $A \in \Gamma$ существует такая конфигурация $\tau \in \mathfrak{R}_k$, что

- 1) $A \sim_\vee \psi^r$,
- 2) B содержит хотя бы одну формулу из ρ_α^r

для любого терминала α конфигурации τ и любой формулы $B \in \Gamma_A$.

Доказательство. Пусть $\Gamma = A_1, \dots, A_n$. Докажем пункт 1 индукцией по i от n до 1. Если $i = n$, то $A_n = G_\varepsilon \sim_\vee \psi^{\tau_n}$ для $\tau_n = \langle \{\varepsilon\}, \varphi_\emptyset \rangle$, где φ_\emptyset — отображение с пустой областью определения.

Пусть $A_i \sim_{\vee} \psi^{\tau_i}$ для $\tau_i = \langle R_i, \varphi_i \rangle$ и A_i есть результат применения правила (1) к формулам A_{i_0} и A_{i_1} для некоторых $1 \leq i_0, i_1 < i$. Тогда $A_{i_0} \sim_{\vee} B_0 \vee C$, $A_{i_1} \sim_{\vee} B_1 \vee C$ и $A_i \sim_{\vee} (B_0 \wedge B_1) \vee C$ для некоторых формул B_0, B_1, C .

Так как $B_0 \wedge B_1$ является слагаемым в ψ^{τ_i} , то $B_0 \wedge B_1$ является слагаемым в $\psi_{\alpha}^{\tau_i}$ для некоторого терминала α . Из определения формулы $\psi_{\alpha}^{\tau_i}$ следует, что существует $a \in \{0, 1\}$, для которого B_i является слагаемым в $\psi_{\alpha a}^{\tau_{i_j}}$, где $\tau_{i_j} = \langle R_i \cup \{\alpha a\}, \varphi_{i_j} \rangle$ и

$$\varphi_{i_j}(x) = \begin{cases} j, & x = \alpha a; \\ \varphi_i(x), & \text{иначе.} \end{cases}$$

для $j \in \{0, 1\}$. Очевидно, что $A_{i_j} \sim_{\vee} \psi^{\tau_{i_j}}$ для $j \in \{0, 1\}$. Это завершает доказательство пункта 1.

Теперь докажем пункт 2 индукцией по i от 1 до n . Если A_i является результатом применения правила (2), то $\Gamma_{A_i} = A_i$ и утверждение верно.

Пусть A_i есть результат применения правила (1) к формулам A_{i_0} и A_{i_1} для некоторых $1 \leq i_0, i_1 < i$ и утверждение верно для A_{i_0} и A_{i_1} . Рассмотрим конфигурации $\tau_i, \tau_{i_0}, \tau_{i_1}$ из первой части доказательства и произвольную формулу $B \in \Gamma_{A_i}$, тогда $B \in \Gamma_{A_{i_j}}$ для некоторого $j \in \{0, 1\}$. По предположению индукции B содержит хотя бы одну формулу из $\rho_{\alpha}^{\tau_{i_j}}$ для каждого терминала α из τ_{i_j} и, следовательно, B также содержит хотя бы одну формулу из $\rho_{\alpha}^{\tau_i}$ согласно определению множества $\rho_{\alpha}^{\tau_i}$. Это завершает доказательство пункта 2. \square

Определим отношение эквивалентности \sim на множестве \mathfrak{R}_k . Две конфигурации $\tau_1 = \langle R, \varphi_1 \rangle$ и $\tau_2 = \langle R, \varphi_2 \rangle$ из \mathfrak{R}_k будем называть *эквивалентными* и обозначать это через $\tau_1 \sim \tau_2$, если $\varphi_1(\alpha) = \varphi_2(\alpha)$ для любого $\alpha \in R$ такого, что $|\alpha| > k$. Класс эквивалентности конфигурации $\tau \in \mathfrak{R}_k$ будем обозначать через $[\tau]$.

Лемма 4. *Если $\tau_1 \sim \tau_2$ — различные конфигурации, то $\rho_{\alpha}^{\tau_1} \cap \rho_{\alpha}^{\tau_2} = \emptyset$ для некоторого терминала α .*

Доказательство. Пусть $\tau_i = \langle R, \varphi_i \rangle$ для $i \in \{1, 2\}$. Так как τ_1 и τ_2 различны, то существует $\beta \in R$, для которого $\varphi_1(\beta) \neq \varphi_2(\beta)$. Непосредственной проверкой можно убедиться, что $\rho_\alpha^{\tau_1} \cap \rho_\alpha^{\tau_2} = \emptyset$ для любого терминала $\alpha \succeq \beta$. \square

Конфигурацию $\tau = \langle R, \varphi \rangle \in \mathfrak{R}_k$ будем называть *терминальной*, если найдутся такие терминалы $\alpha_0, \alpha_1 \in R$, что $\varphi(\alpha_0) = \varphi(\alpha_1) = a$, $|\alpha_0| = |\alpha_1| = 2k - \max(s, 1)$ и $\alpha_0 \prec \alpha_1$ для $|\alpha| = s$ и $a \leq s \leq a(k-1)$.

Лемма 5. *Конфигурация $\tau \in \mathfrak{R}_k$ является терминальной тогда и только тогда, когда формула ψ^τ является результатом применения правила (2).*

Доказательство. Если $\tau = \langle R, \varphi \rangle$ — терминальная конфигурация, то найдутся такие терминалы $\alpha_0, \alpha_1 \in R$, что $\varphi(\alpha_0) = \varphi(\alpha_1) = a$, $|\alpha_0| = |\alpha_1| = 2k - \max(s, 1)$ и $\alpha_0 \prec \alpha_1$ для $|\alpha| = s$ и $a \leq s \leq a(k-1)$. По определению, если $\alpha = a_1 a_3 \dots a_{2s-1}$ и $\varphi(a_1 a_3 \dots a_{2i-1}) = a_{2i}$ для $1 \leq i \leq s$, то

$$\psi_{\alpha_0}^\tau = \neg x_{1a_1 \dots a_{2s}} \vee A, \quad \psi_{\alpha_1}^\tau = x_{1a_1 \dots a_{2s}} \vee A$$

для некоторого формулы A . Следовательно, ψ^τ является результатом применения правила (2).

Обратно, пусть ψ^τ является результатом применения правила (2), тогда ψ^τ содержит слагаемые $\neg x_{1\beta}$ и $x_{1\beta}$ для некоторого слова $\beta \in \{0, 1\}^{\leq 2k}$. Ясно, что $\beta = a_1 \dots a_{2s}$ для некоторого $0 \leq s \leq k$. По определению ψ^τ литералы $\neg x_{1\beta}$ и $x_{1\beta}$ являются слагаемыми в $\psi_{\alpha_0}^\tau$ и $\psi_{\alpha_1}^\tau$, для некоторых терминалов α_0 и α_1 в τ таких, что $|\alpha_0| = |\alpha_1| = 2k - \max(s, 1)$ и $\alpha_0 \prec \alpha_1$ для $\alpha = a_1 a_3 \dots a_{2s-1}$. Ясно, что $\varphi(\alpha_0) = \varphi(\alpha_1) = 0$ при $s = 0$ и $\varphi(\alpha_0) = \varphi(\alpha_1) = 1$ иначе. Следовательно, τ является терминальной конфигурацией. \square

Теперь докажем ключевую лемму.

Лемма 6. $L_{\mathcal{F}_1}(G_\varepsilon) \geq 2^{2^k}$.

Доказательство. Для начала, индукцией по $m \geq 1$, будем строить нетерминальную конфигурацию $\tau \in \mathfrak{R}_k$ мощности m

и минимальный вывод Γ формулы G_ε в системе \mathcal{F}_1 такие, что для любого $\mathbf{r}' \in [\mathbf{r}]$ формула $\psi_{\mathbf{r}'}$ принадлежит Γ .

Если $m = 1$, то $\mathbf{r} = \langle \{\varepsilon\}, \varphi_\emptyset \rangle$ и Γ — произвольный минимальный вывод G_ε в \mathcal{F}_1 .

Пусть уже построена нетерминальная конфигурация \mathbf{r} мощности m и минимальный вывод Γ с данными свойствами. Если $\tau_{\mathbf{r}} = n$, то $[\mathbf{r}] = \{\mathbf{r}_1, \dots, \mathbf{r}_n\}$ и формулы $\psi_{\mathbf{r}_1}, \dots, \psi_{\mathbf{r}_n}$ принадлежат Γ .

Для каждого i , $1 \leq i \leq n$, обозначим через Γ_i минимальную подпоследовательность в Γ , которая является выводом формулы $\psi_{\mathbf{r}_i}$, и пусть $\mathbf{r}_i = \langle R, \varphi_i \rangle$. Заметим, что, с одной стороны, последовательности Γ_i и Γ_j не пересекаются при $i \neq j$ согласно Леммам 3 и 4, с другой стороны, формулы $\psi^{\mathbf{r}_i}$ и $\psi^{\mathbf{r}_j}$ совпадают с точностью до переименования литералов. Поэтому будем считать, что выводы $\Gamma_1, \dots, \Gamma_n$ также совпадают с точностью до переименования литералов, т.к. иначе всегда можно создать n копий минимального из выводов Γ_i и переименовать литералы соответствующим образом. Ясно, что полученный при этом вывод также будет минимальным.

Рассмотрим произвольное $i \in \{1, \dots, n\}$. Поскольку конфигурация \mathbf{r} является нетерминальной, то по Лемме 5 формула $\psi^{\mathbf{r}_i}$ является результатом применения правила (1) к некоторым формулам A_0 и A_1 из Γ . Из доказательства Леммы 3 следует, что существует такой терминал $\alpha \in R$, $|\alpha| < 2k - 1$, и такое $a \in \{0, 1\}$, что $\alpha a \notin R$ и $A_j \sim_{\vee} \psi_{\alpha a}^{\mathbf{r}_{i,j}}$, где $\mathbf{r}_{i,j} = \langle R \cup \{\alpha a\}, \varphi_{i,j} \rangle$ и

$$\varphi_{i,j}(x) = \begin{cases} j, & x = \alpha a; \\ \varphi_i(x), & \text{иначе.} \end{cases}$$

для $j \in \{0, 1\}$.

Теперь определим конфигурацию \mathbf{r}' мощности $m + 1$. Если $\alpha = \beta a \gamma 0^{k-s}$, где $1 \leq s < k$, $|\beta| = s - 1$, $|\gamma| = k - s$ и не существует $\gamma' \in \{0, 1\}^{k-s}$, для которого $\beta \bar{a} \gamma' 0^{k-s+1} \in R$, то положим $\mathbf{r}' = \mathbf{r}_{i,1}$. В противном случае, $\mathbf{r}' = \mathbf{r}_{i,0}$.

Если конфигурация $\mathbf{r}' = \langle R', \varphi' \rangle$ является нетерминальной, то продолжаем построение для \mathbf{r}' . В противном случае найдутся такие терминалы $\alpha_0, \alpha_1 \in R'$, что $\varphi'(\alpha_0) = \varphi'(\alpha_1) = b$, $|\alpha_0| =$

$|\alpha_1| = 2k - \max(s, 1)$ и $\alpha 0 \prec \alpha_0$, $\alpha 1 \prec \alpha_1$ для $|\alpha| = s$ и $b \leq s \leq b(k-1)$. Поскольку конфигурация \mathfrak{r} является нетерминальной, то $\alpha a = \alpha_i$ для некоторого $i \in \{0, 1\}$. По построению $\varphi'(\alpha a) = \varphi_{i,0}(\alpha a) = 0$ и, следовательно, $\varphi'(\alpha_0) = \varphi'(\alpha_1) = 0$, $|\alpha_0| = |\alpha_1| = 2k - 1$ и $|\alpha| = 0$. Покажем, что это возможно только при $n = 2^k$.

Для этого докажем индукцией по h , $1 \leq h \leq k$, что для любого $\xi \in \{0, 1\}^h$ существует такое $\zeta \in \{0, 1\}^{k-h}$, что $\xi\zeta 0^{k-h} \in R'$ и $\varphi'(\xi\zeta 0^{k-h}) = 0$ при $h < k$. Для $h = 1$ утверждение верно. Пусть оно верно для $h < k$, докажем его для $h + 1$. Рассмотрим произвольное $\xi \in \{0, 1\}^h$. По предположению индукции найдутся такие $a \in \{0, 1\}$ и $\zeta \in \{0, 1\}^{k-h-1}$, что $\xi a \zeta 0^{k-h} \in R'$ и $\varphi'(\xi a \zeta 0^{k-h}) = 0$. Тогда по построению $\xi \bar{a} \zeta' 0^{k-h} \in R'$ для некоторого $\zeta' \in \{0, 1\}^{k-h-1}$ и, следовательно, $\varphi'(\xi a \zeta 0^{k-h-1}) = \varphi'(\xi \bar{a} \zeta' 0^{k-h-1}) = 0$ при $h+1 < k$ по определению конфигурации. Поэтому для любого $\xi \in \{0, 1\}^{h+1}$ существует такое $\zeta \in \{0, 1\}^{k-h-1}$, что $\xi\zeta 0^{k-h-1} \in R'$ и $\varphi'(\xi\zeta 0^{k-h-1}) = 0$ при $h+1 < k$.

Из доказанного следует, что для любого $\xi \in \{0, 1\}^k$ в R' существует терминал $\alpha \succeq \xi$. Поэтому $n = 2^k$.

Поскольку множество \mathfrak{R}_k конечно, то процесс построения нетерминальной конфигурации \mathfrak{r} и минимального вывода формулы G_ε в \mathcal{F}_1 с указанными свойствами обязательно оборвется. Из доказанного выше следует, что он оборвется на конфигурации \mathfrak{r} , терминальное число которой равно 2^k . Так как при этом $|\mathfrak{r}| = 2^{2^k}$, то тем самым доказана оценка снизу $L_{\mathcal{F}_1}(G_\varepsilon) \geq 2^{2^k}$. \square

Теперь докажем Теорему 1. Согласно Лемме 1 множество правил \mathcal{F}_0 является системой Фреге. Непосредственной проверкой можно убедиться, что

$$|G_\varepsilon| = 5k2^{2^k} - 1.$$

Пусть $k = \frac{1}{2}(\log n - \log \log n - 2)$. Так как $n \geq 2^7$, то $k \geq 1$ и, следовательно, k всегда найдется. Для данного k имеем $|G_\varepsilon| < n$. Объединив Леммы 2 и 6, получим

$$L_{\mathcal{F}_0}(n) \geq L_{\mathcal{F}_0}(G_\varepsilon) \geq L_{\mathcal{F}_1}(G_\varepsilon) \geq 2^{2^k} \geq 2^{\sqrt[3]{n}}.$$

Теорема 1 доказана.

Список литературы

- [1] *Боков Г. В.* Об алгоритмической неразрешимости некоторых проблем распознавания для пропозициональных исчислений. // Интеллектуальные системы, т. 18, вып. 4, 2014, с. 207-214.
- [2] *Боков Г. В.* О некоторых свойствах решетки пропозициональных исчислений. // Интеллектуальные системы, т. 19, вып. 2, 2015, с. 47-64.
- [3] *Arora S. and Barak B.* Computational Complexity: A Modern Approach // Cambridge University Press, 2009.
- [4] *Buss S. R.* Some remarks on lengths of propositional proofs // Archive for Mathematical Logic, vol. 34 (6), 1995, p. 377–394.
- [5] *Stephen A. Cook and Robert A. Reckhow* The relative efficiency of propositional proof systems, J. Symbolic Logic, Vol. 44, 1979, p. 36–50.
- [6] *Krajíček J.* On Frege and Extended Frege Proof Systems // Feasible Mathematics II, Series “Progress in Computer Science and Applied Logic”, vol. 13, 1995, p. 284-319.

On some Frege system

G. V. Bokov

In this article, we consider a Frege system over the signature $\{\wedge, \vee, \neg\}$. For this system, we prove a nontrivial lower bound to the length of proofs.

Keywords: Frege systems, length of proof, lower bounds.