

*Математика*

УДК 621.39.1:519.24

А.А. ЧУБАРЯН

О НЕКОТОРОЙ СИСТЕМЕ КЛАССИЧЕСКОГО ИСЧИСЛЕНИЯ  
ВЫСКАЗЫВАНИЙ

В работе на основе введенных автором обобщенных правил *modus ponens* строится некоторая система классического исчисления высказываний, к которой полиномиально сводимы по обоим критериям сложности (количество шагов выводов и длина выводов) и системы Фреге и системы Фреге с подстановками.

**Введение.** В ряде обзоров по результатам о сложностях логических выводов в системах исчисления высказываний [1–3] указывается на особую роль систем Фреге с правилом подстановки, в частности – на существование ряда формул, выводимых в системах с подстановками за  $n$  шагов, в то время как для их выводов в системах без подстановок требуется как минимум  $2^n$  шагов. В то же время установлено, что если в качестве критерия сложности брать сумму длин всех формул вывода, то для вышеуказанных формул рост длины вывода оказывается разве что квадратическим [1,4]. В [5] описана конструкция вывода для систем с подстановками, которая по количеству шагов дает максимально возможный рост (экспоненциальный) при переходе к системам без подстановок, но по длине выводов рост ограничен полиномом. В общем случае установление оценки роста длины вывода при указанном переходе является открытой проблемой [1,2], причем авторами этих обзоров отмечается, что, видимо, эта оценка будет также экспоненциальной.\*

В связи с этим открытой является и проблема существования системы исчисления высказываний типа Фреге, при переходе к которой от систем с подстановками наблюдался бы лишь полиномиальный рост как длины вывода, так и числа шагов выводов.

В настоящей работе вводятся два правила вывода, являющиеся обобщением правила *modus ponens*, на основе которых строится некоторая система классического исчисления высказываний  $\mathcal{F}^m$ , обладающая следующими свойствами: любой вывод произвольной формулы, построенный как в системах Фреге, так и в системах Фреге с подстановками, моделируется в вывод в системе  $\mathcal{F}^m$  с не более, чем полиномиальным увеличением длины вывода.

\* Автор настоящей статьи в силу результатов работы [5] склоняется к гипотезе о разнице между полиномиальным ростом длин выводов при указанном переходе.

**Основные понятия и определения.** Напомним общепринятые понятия систем Фреге, выводов в них и сложностных характеристик вывода.

Каждая система Фреге  $\mathcal{F}$  использует некоторое конечное, функционально полное множество пропозициональных связок.  $\mathcal{F}$  определяется конечным множеством схематически заданных правил вывода  $\frac{A_1 A_2 \dots A_k}{B}$

(при  $k = 0$  соответствующее правило определяет схему аксиом).  $\mathcal{F}$  непротиворечива, т. е. для каждого правила вывода, если при некотором истинностном значении переменных все  $A_i (1 \leq i \leq k)$  принимают значение "истина", и  $B$  принимает значение "истина".  $\mathcal{F}$  полна, т.е. всякая тавтология выводима в  $\mathcal{F}$ . Система Фреге с подстановкой  $S\mathcal{F}$  получается из  $\mathcal{F}$  добавлением правила подстановки  $\frac{A}{A\sigma}$ , где  $\sigma$  – 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.

Подстановку, являющуюся отображением, ставящим в соответствие каждой переменной формулы  $A$  некоторую переменную, будем называть, следуя [1], переименованием и будем обозначать через  $r$ , а результат этого переименования переменных формулы  $A$  – через  $Ar$ . Через  $R\mathcal{F}$  будем обозначать систему, получающуюся из  $\mathcal{F}$  добавлением правила переименования  $\frac{A}{Ar}$ , и будем называть системой Фреге с переименованием.

Мы будем пользоваться общепринятым определением вывода в данной системе в виде последовательности формул, каждая из которых является аксиомой данной системы или получается из предыдущих по одному из правил вывода данной системы. Вывод в системе  $\Phi$  назовем  $\Phi$ -выводом.

В качестве сложности вывода зафиксируем два понятия: количество различных формул (шагов) в выводе ( $T$ -сложность) и суммарную длину всех формул вывода ( $L$ -сложность).

Принято считать, что система  $\Phi_1$  полиномиально сводима в смысле  $T$ -или  $L$ -сложности к системе  $\Phi_2$ , если можно указать такой полином  $p(\ )$ , что каждая формула, выводимая в  $\Phi_1$  со сложностью ( $T$  или  $L$ ), не превышающей  $n$ , выводима в  $\Phi_2$  с соответствующей сложностью, не превышающей  $p(n)$ .

Известно, что полиномиально сводимы друг к другу для обоих критериев сложности:

- 1) каждая пара систем Фреге  $\mathcal{F}_1$  и  $\mathcal{F}_2$  [1, 2],
- 2) каждая пара систем Фреге с подстановкой  $S\mathcal{F}_1$  и  $S\mathcal{F}_2$  [1, 2],
- 3) каждая система Фреге к любой системе Фреге с подстановкой [1–3].

Каждая система Фреге с подстановкой сводима к некоторой системе Фреге с переименованием по длине вывода [2].

Как уже было сказано в введении, для  $T$ -сложности  $S\mathcal{F}$  не сводима к  $\mathcal{F}$ , для  $L$ -сложности вводимость  $S\mathcal{F}$  к  $\mathcal{F}$  – открытая проблема.

Нами на основе системы Фреге  $\mathcal{F}$  будет определена новая система, та-

кая, что каждая система Фреге с переименованием, а следовательно, и каждая система Фреге и система Фреге с подстановкой сводимы к этой новой системе.

**Определение системы  $\mathcal{GF}^{mp}$ .** В нижеприведенном определении системы  $\mathcal{GF}^{mp}$  существенную роль играет правило *modus ponens* (m. p.), которое постулирует выводимость формулы  $B$  при наличии выводимости формул  $A$  (малой посылки m. p.) и  $A \rightarrow B$  (большой посылки m. p.).

Определим две модификации правила m. p., которые мы будем называть соответственно *generalized modus ponens 1* (g.m.p.1) и *generalized modus ponens 2* (g. m. p. 2).

1. Если выводимы формулы  $A$  и  $B \rightarrow C$  и для некоторого переименования  $r$   $A = Br$ , то выводима формула  $Cr$  (g. m. p. 1):

$$\frac{A, B \rightarrow C, \exists r(A = Br)}{Cr}$$

2. Если выводимы формулы  $A$  и  $B \rightarrow C$  и для некоторого переименования  $r$   $B = Ar$ , то выводима формула  $C$  (g. m. p. 2):

$$\frac{A, B \rightarrow C, \exists r(B = Ar)}{C}$$

*Замечание 1.*

1) Если  $A$  и  $B \rightarrow C$  – тавтологии, то  $(B \rightarrow C)r$  также будет тавтологией, а т. к.  $(B \rightarrow C)r = Br \rightarrow Cr$  и  $A = Br$  – тавтология, то и  $Cr$  будет тавтологией.

2) Если  $A$  и  $B \rightarrow C$  – тавтологии, то  $Ar$  – также тавтология, а значит и  $B = Ar$  – тавтология, а следовательно, и  $C$  будет тавтологией.

*Замечание 2.* Правило m. p. является частным случаем и g. m. p. 1, и g. m. p. 2 при тождественном переименовании  $r$ .

Зафиксируем некоторую систему Фреге, единственным правилом вывода которой (кроме аксиом) является *modus ponens*, и впредь будем обозначать ее через  $\mathcal{F}^{mp}$ . Через  $\mathcal{GF}^{mp}$  обозначим систему, полученную из  $\mathcal{F}^{mp}$  заменой правила m. p. на правила g. m. p. 1 и g. m. p. 2. В силу вышеприведенных замечаний 1 и 2 система  $\mathcal{GF}^{mp}$  полна и непротиворечива.

**Теорема.** Каждая система Фреге сводима к  $\mathcal{GF}^{mp}$  для обоих критериев сложности, и каждая система Фреге с подстановкой сводима к  $\mathcal{GF}^{mp}$  по длине вывода.

Доказательство основано на следующем утверждении:

**Лемма.** Пусть  $\mathcal{RF}^{mp}$  – система, полученная из  $\mathcal{F}^{mp}$  добавлением правила переименования  $\frac{A}{Ar}$ , тогда любая формула, выводимая в  $\mathcal{RF}^{mp}$  с  $T$ -сложностью ( $L$ -сложностью), не превышающей  $t(l)$ , выводима в  $\mathcal{GF}^{mp}$  с  $T$ -сложностью ( $L$ -сложностью), не превышающей  $t(l)$ .

*Доказательство.* Пусть  $F_1, F_2, \dots, F_l$  является кратчайшим по сложности ( $T$  или  $L$ ) выводом формулы  $F_l$  в системе  $\mathcal{RF}^{mp}$ , и  $\sum_{i=1}^l |F_i| = l$ . Процесс

преобразования этого вывода в  $\mathcal{G}\mathcal{F}^m$  - вывод заключается в удалении из последовательности  $F_1, F_2, \dots, F_t$  всех формул  $F_i (3 \leq i \leq t-1)$ , которые получаются по правилу переименования. Действительно, если формула  $F_i$  получена из  $F_{i-1}$  переименованием переменных, то ни одна из последующих формул не может быть получена из  $F_i$  по правилу переименования, так как последовательное применение правила подстановки более одного раза противоречит тому, что был взят кратчайший вывод, ибо результат последовательного применения нескольких подстановок может быть получен одной "унифицированной" подстановкой. Если  $F_k (i < k \leq t)$  получена из  $F_i$  и некоторой формулы  $F_j (j < k)$ , не являющейся результатом подстановки, по правилу м. р. (отметим, что ни  $F_{i-1}$ , ни какая-либо другая формула, полученная из  $F_{i-1}$  переименованием, не могут быть в роли  $F_j$  в силу специфики правил переименования и м. р.), и  $F_j$  является малой посылкой м. р., а  $F_i$  – большой посылкой м. р., то  $F_k$  получится из  $F_j$  и  $F_{i-1}$  по г. м. р. 1, если же  $F_j$  является большой посылкой м. р., а  $F_i$  – малой посылкой, то  $F_k$  является результатом применения к  $F_{i-1}$  и  $F_j$  правила г. м. р. 2. Если же  $F_j$  также получена переименованием из некоторой формулы  $F_l (l < j)$ , то  $F_k$  получится из  $F_{i-1}$  и  $F_l$  или по г. м. р. 1 или по г. м. р. 2 в зависимости от того, которая из них является малой (большой) посылкой м. р. В силу сказанного, удаление из последовательности  $F_1, F_2, \dots, F_t$  формулы  $F_i$  не отражается на выведении остальных формул в системе  $\mathcal{G}\mathcal{F}^m$ . Если же  $F_i$  получена из  $F_{i-1}$  по правилу переименования, то повторяем "прореженный" вывод  $F_{i-1}$ , произведя переименование во всех его формулах. Очевидно, что полученный таким образом вывод является  $\mathcal{G}\mathcal{F}^m$ -выводом и его  $T$ -сложность ( $L$ -сложность) не выше соответствующей сложности заданного  $\mathcal{R}\mathcal{F}^m$ -вывода.

Лемма доказана.

Доказательство теоремы следует из утверждения леммы и перечисленных выше известных фактов сведения одних систем к другим.

Отметим, что переход к системе  $\mathcal{G}\mathcal{F}^m$  через систему  $\mathcal{R}\mathcal{F}^m$  не необходим. Он лишь упрощает вид обобщенных правил м. р., а следовательно, упрощает их применение. Если переход к  $\mathcal{G}\mathcal{F}^m$  осуществлять непосредственно из  $\mathcal{S}\mathcal{F}$ , то 1) в определениях правил г. м. р. 1 и г. м. р. 2 будет фигурировать не переименование  $\tau$ , а подстановка  $\sigma$  и 2) необходимо добавить новое правило – self modus ponens (s. м. р.), формулируемое следующим образом:

$$\frac{A \rightarrow B, \exists \sigma ((A \rightarrow B) = A \sigma)}{B \sigma}.$$

Далее, система  $\mathcal{G}\mathcal{F}^m$  получается из  $\mathcal{F}^m$  заменой

правила м. р. на три правила г. м. р. 1, г. м. р. 2 и s. м. р.

## ЛИТЕРАТУРА

1. Pudlak P. The Lengths of Proofs, Handbook of proof theory. North-Holland, 1998, p. 547–637.
2. Buss S.R. – Arch. Math. Logic, 1995, v. 34, p. 377–394.
3. Цейтин Г.С., Чубарян А.А. Матем. вопросы киберн. и вычисл. техники. Ер., Изд-во АН Арм. ССР, 1975.
4. Բոլիբեկյան Հ., Չոբարյան Ա. Արտածումների որոշ բարդությունների հետազոտում. Եր., ԵՊՀ հրատ., 2000:
5. Чубарян А.А. – Изв. НАН РА , 2000, т. 35, № 5.

Ա.Ա. ՉՈՒԲԱՐՅԱՆ

ԱՍՈՒՅԹԱՅԻՆ ԴԱՍԱԿԱՆ ՀԱՇՎԻ ՄԵԿ ՀԱՄԱԿԱՐԳԻ ՎԵՐԱԲԵՐՅԱԼ

Ա մ փ ո փ ո մ

Հոդվածում սահմանվում են "modus ponens" կանոնի ընդհանրացումներ, որոնց հիման վրա կառուցվում է ասույթային դասական հաշվի մեկ համակարգ, որին բազմանդամայնորեն հանգեցվում են ինչպես Ֆրեգեի համակարգերը, այնպես էլ տեղադրման կանոնով Ֆրեգեի համակարգերը:

A.A. CHUBARIAN

ON SOME SYSTEM OF PROPOSITIONAL LOGICS CALCULUS

Summary

In this paper generalizations of "modus ponens" rules are defined on the basis of which a certain system of propositional logics calculus is constructed to which both the Frege systems and the Frege systems with substitutions are polynomially brought.