Математические вопросы кибернетики и вычислительной техники 54, 138−146, 2020.

УДК 510.6

Об отношениях сложностей выводов в ряде систем исчисления высказываний

Акоп А. Тамазян и Анаит А. Чубарян

Ереванский государственный университет
e-mail: tam.hak27@gmail.com, achubaryan@ysu.am

Аннотация

Для некоторых семейств формул сравнены количества шагов линейных выводов в ряде систем исчисления высказываний: секвенциальной системе с правилом сечения **PK**, в той же системе без правила сечения **PK⁻,** в той же системе с добавлением правила подстановки **SPK,** в той же системе с добавлением кванторов **QPK.** Для одного из рассмотренных семейств формул Алессандрой Карбоне в [1] сравнены количества шагов выводов в *виде дерева* в тех же системах исчисления высказываний и выявлено отличительное свойство системы **QPK**, а именно доказано экспоненциальное ускорение по отношению к системам **SPK** и **PK,** которые,, в свою очередь,, имеют экспоненциальное ускорение по отношению к системе **PK⁻**. Этот результат послужил толчком для бурного интереса к исследованиям системы **QPK.** В настоящей работе для *линейных* выводов получены иные сотношения количества шагов в тех же системах: оказалось, что система **QPK** не имеет преимуществ по отношению к системе **SPK,** оказалось также, что для рассматриваемых семейств формул система **PK** не имеет преимуществ по отношению к системе **PK⁻,** которая, в свою очередь, не имеет преимуществ по отношению к более слабой монотонной системе **PMon.** Доказана также достоверность полученных результатов для ряда иных семейств формул и ряда других систем.

Ключевые слова: разновидности секвенциальных систем исчисления высказываний; разновидности систем Фреге; количество щагов вывода; экспоненциальное ускорение.

1. Введение

Теория сложностей выводов изучает количественные характеристики выводов, то есть насколько «просто» или «сложно» может быть доказана та или иная теорема. Толчком для бурного развития теории сложностей пропозициональных выводов явился известный результат Кука и Рекхау о неравенстве множеств NP и $coNP$ в том и только в том случае,

если не существует полиномиально ограниченной системы доказательств классических тавтологий [2]. За годы интенсивных исследований получено множество интересных оценок длины и количества шагов выводов в различных системах классического исчисления высказываний, на основе которых выстроена некая иерархия пропозициональных систем выводов. Некоторые из них с относительно простой стратегией поиска выводов, условно определены как «слабые» системы – системы, в которых для отдельных классов формул получены нижние экспоненциальные оценки длин выводов, а те системы, в которых ни для какого класса таковых оценок пока не найдено, считаются «сильными». К первому множеству относится, в частности, секвенциальная система без правила сечения **PK**$^{-}$, ко второму классу относятся наиболее естественные системы выводов – системы Фреге $\boldsymbol{\mathcal{F}}$, системы Фреге с правилом подстановки **S**$\boldsymbol{\mathcal{F}}$, секвенциальная система с правилом сечения **PK,** та же система с добавлением правила подстановки **SPK,** а также та же система с добавлением кванторов **QPK**. Добавление кванторов расширило множество пропозициональных тавтологий: в частности, формула $(p \supset \mathrm{q}) \supset ((\mathrm{p} \supset \mathrm{q})\&(r \supset q))$ не является тавтологией, но формула $\exists \mathrm{r}((p \supset \mathrm{q}) \supset \big((\mathrm{p} \supset \mathrm{q})\&(\mathrm{r} \supset \mathrm{q})\big))$ уже является тавтологией. Это обстоятельство вызвало особый интерес к изучению системы **QPK,** а результаты работы [1], в которой для одного из рассмотренных семейств формул выявлено отличительное свойство системы **QPK**, а именно доказано экспоненциальное ускорение по отношению к системам **SPK** и **PK,** которые, в свою очередь, имеют экспоненциальное ускорение по отношению к системе **PK**$^{-}$**,** послужили толчком для бурного интереса к исследованиям системы **QPK.** Как оказалось, эта система может быть полезной для решения одной из NP-полных задач – задачи «Выполнимости».

В настоящей работе исследованы соотношения количества шагов для *линейных* выводов (выводов, в которых формулы не повторяются) для тех же систем, которые рассмотрены в [1]. Оказалось, что для этих более естественных выводов система **QPK** не имеет преимуществ по отношению к системе **SPK,** оказалось также, что для рассматриваемых семейств формул система **PK** не имеет преимуществ по отношению к системе **PK**$^{-}$**.** Доказана также достоверность полученных результатов для ряда иных семейств формул и ряда других систем.

2. Предварительные понятия

Для представления основных результатов напомним некоторые понятия и обозначения. Мы пользуемся общепринятыми определениями пропозициональной формулы, пропозициональной формулы с кванторами, свободной переменной в формуле с кванторами, тавтологии в данной логике, секвенции, сукцедента, антецедента, главной формулы секвенции, секвенциальных систем без сечения, секвенциальных систем с правилом подстановки, секвенциальных систем с кванторами, сложностей выводов [2-6].

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, логические связки ¬, &, ∨, ⊃ и пару скобок (,). В некоторых системах будут использованы также знаки T «истина» и ⊥ «ложь».

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

2.1. Описание рассматриваемых систем. Напомним ряд определений. Секвенцией называется выражение $\Gamma \to \Delta$, где Γ (антецедент) и Δ (сукцедент) являются конечной (может быть пустой) последовательностью пропозициональных формул. Следуя [3,4], определим следующие системы.

Схемой аксиом для классической системы **РК** являются секвенции $p \to p$, $\to T$, где p - произвольная пропозициональная переменная.

Для произвольных формул A, B и последовательностей формул Γ и Δ логическими правилами вывода являются:

$$\supset\to \frac{\Gamma \to \Delta,\ A \qquad B,\ \Gamma \to \Delta}{A \supset B,\ \Gamma \to \Delta} \qquad \to\supset \frac{A,\ \Gamma \to \quad B,\ \Delta}{\Gamma \to A \supset B, \Delta}$$

$$\vee\to \frac{A,\ \Gamma \to \Delta \text{ и } B,\ \Gamma \to \Delta}{A \vee B,\ \Gamma \to \Delta} \qquad \to\vee \frac{\Gamma \to A,\ \Delta \text{ или } \Gamma \to B,\ \Delta}{\Gamma \to A \vee B,\ \Delta}$$

$$\& \to \frac{A,\ \Gamma \to \Delta \text{ или } B,\ \Gamma \to \Delta}{A\&B,\ \Gamma \to \Delta} \qquad \to \& \frac{\Gamma \to A, \Delta \text{ и } \Gamma \to B, \Delta}{\Gamma \to A\&B, \Delta}$$

$$\neg\to \frac{\Gamma\to \ A,\ \Delta}{\neg A,\ \Gamma\to\Delta} \qquad \to \neg \frac{A,\ \Gamma\to \ \Delta}{\Gamma\to\neg A,\ \Delta},$$

где формулы $A \supset B$, $A \vee B$, $A\&B$ и $\neg A$ являются главными формулами секвенции.

Правило сечения

$$\frac{\Gamma \to \Delta, A \quad A, \Gamma \to \Delta}{\Gamma \to \Delta}.$$

Система **РК⁻** получается из системы **РК** удалением правила сечения.

Система **SPK** получается из системы **РК** добавлением правила подстановки:

$$S_p^B \quad \frac{C(p), \Gamma \to \Delta, A(p)}{C(B), \Gamma \to \Delta, A(B)},$$

где переменная p не присутствует ни в Γ, ни в Δ, B – формула, подставляемая вместо всех вхождений переменной p.

Система **QPK** получается из системы **РК** добавлением правил:

$$\frac{A(q), \Gamma \ \to \ \Delta}{(\exists p)A(p), \Gamma \ \to \ \Delta}(\exists \to) \qquad \frac{\Gamma \ \to \ \Delta, A(B)}{\Gamma \ \to \ \Delta, (\exists p)A(p)}(\to \exists)$$

$$\frac{A(B)\Gamma \ \to \ \Delta}{(\forall p)A(p), \Gamma \ \to \ \Delta}(\forall\to) \qquad \frac{\Gamma \ \to \ \Delta, A(q)}{\Gamma \ \to \ \Delta, (\forall p)A(p)}(\to \forall),$$

где B - любая пропозициональная формула быть может с кванторами, а также выполнены следующие условия: в нижних секвенциях правил $(\exists \to)$ и $(\to \forall)$ не должно быть

свободных переменных, которые не свободны в верхних, и все вхождения переменной q в A(q) должны быть заменены переменной p, а в правилах (→ ∃) и (∀→) формула B не должна содержать переменные, находящиеся в области действия каких-либо кванторов.

2.2. Некоторые характеристики тавтологий и логических систем выводов. Здесь мы исследуем некоторые свойства тавтологий различных логик и вышеприведенных систем выводов на основе одной из сложностных характеристик выводов – *t*-сложности, определяемой как количество различных секвенций в выводе. Пусть ϕ является некоторой секвенциальной системой выводов фиксированной логики, а φ – некоторая тавтология данной логики. Через $\boldsymbol{t}^{\phi}(\varphi)$ обозначим минимально возможное значение *t*-сложности всевозможных выводов соответствующей секвенции → φ в системе ϕ.

Далее будут получены верхние и нижние оценки *t*-сложностей выводов и для их записи будут использованы следующие общепринятые обозначения:
если $\exists c_1 \exists k_1 \forall x > k_1 |f(x)| \geq c_1 |g(x)|$, то мы будем писать $f(x) = \Omega(g(x))$,
если $\exists c_2 \exists k_2 \forall x > k_2 |f(x)| \leq c_2 |g(x)|$, то мы будем писать $f(x) = O(g(x))$.
При выполнении этих обоих условий будем писать $f(x) = \theta(g(x))$.

Если для двух систем ϕ_1 и ϕ_2 для одних и тех же последовательностей формул ϕ_n имеет место $t^{\phi_1}(\varphi_n) = \Omega(2^{t^{\phi_2}(\varphi_n)})$, то считают, что для последовательности формул ϕ_n система ϕ_2 имеет ***экспоненциальное ускорение*** по отношению к системе ϕ_1.

2.3. Результаты А.Карбоне. В [1] дано определение некоторого класса тавтологий длины $O(2^{2^n})$, для которых исследованы количество шагов выводов в виде дерева во всех вышеперечисленных системах.

Для пропозициональной переменной p формула p^m определяется по индукции следующим образом: $p^1 \equiv p$ и $p^{i+1} \equiv (p^i \& p^i)$ для $i \geq 1$. Нетрудно проверить, что формула p^m содержит ровно 2^m вхождений пропозициональной переменной p и m различных подформул.

Теорема (Карбоне): *Если для достаточно больших n F_n является секвенцией* $\rightarrow p \supset p^{2^n}$, *то*

*1. существует вывод в виде дерева секвенции F_n в системе **QPK** с количеством шагов $O(n)$;*
*2. количество шагов любого вывода в виде дерева секвенции F_n в системе **SPK** является $\Omega(2^n)$;*
*3. количество шагов любого вывода в виде дерева секвенции F_n в системе **PK** является $\Omega(2^n)$;*
*4. количество шагов любого вывода в виде дерева секвенции F_n в системе **PK**⁻ является $\Omega(2^{2^n})$.*

Нам полезен вывод секвенции $\rightarrow p \supset p^{2^n}$ в системе **QPK** с количеством шагов O(n).

Сначала рассматривается вывод секвенции $\forall q(q \supset q^k) \rightarrow \forall q(q \supset q^{2k})$, где k произвольное натуральное число и $q^{2k} = (q^k)^k$. Вывод этой секвенции не зависит от k и может быть получен за конечное число шагов следующим образом:

$$\frac{p \rightarrow p \quad p^k \rightarrow p^k}{p \supset p^k, p \rightarrow p^k}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\forall q(q \supset q^k), p \to p^k \quad p^{2k} \to p^{2k}}{\forall q(q \supset q^k), p^k \supset p^{2k}, p \to p^{2k}}}{\forall q(q \supset q^k), p^k \supset p^{2k} \to p \supset p^{2k}}}{\forall q(q \supset q^k), \forall q(q \supset q^k) \to p \supset p^{2k}}}{\forall q(q \supset q^k) \to p \supset p^{2k}}}{\forall q(q \supset q^k) \to \forall q(q \supset q^{2k})}$$

Следует отметить, что в этом выводе нет повторяющихся секвенций, а значит этот вывод линейный. Повторяя этот вывод n раз можно получить вывод секвенции

$$\forall q(q \supset q^2) \to \forall q\left(q \supset q^{2^n}\right),$$

а так как $\forall q(q \supset q^2)$ выводится за конечное число шагов, то $\forall q(q \supset q^{2^n})$, а следовательно и $\to p \supset p^{2^n}$ выводится за $O(n)$ шагов.

3. Основные результаты

Для того же класса формул, но для линейных выводов доказана

Теорема 1: *Если для достаточно больших n F_n является секвенцией $\to p \supset p^{2^n}$, то*

*1. существует линейный вывод секвенции F_n в системе **QPK** с количеством шагов $O(n)$;*
*2. существует линейный вывод секвенции F_n в системе **SPK** с количеством шагов $O(n)$;*
*3. количество шагов линейного вывода секвенции F_n в системе **PK** является $\theta(2^n)$;*
*4. количество шагов линейного вывода секвенции F_n в системе **PK**$^-$ является $\theta\left(2^n\right)$.*

Доказательство:

Доказательство пункта 1. совпадает с доказательством Карбоне с учетом замечания о линейности рассмотренного вывода.

Для доказательства пункта 2. рассмотрим:

Вывод в SPK		Количество шагов
$p \to p$	аксиома	1
$p\&p \to p\&p$	$S_p^{p^2}$	2
$p \to p\&p$	сечение	3
$p^2 \to p^3$	$S_p^{p^2}$	4
$p \to p^3$	сечение	5
$p^3 \to p^5$	$S_p^{p^3}$	6
$p \to p^5$	сечение	7
. . .	. . .	. . .

$p \to p^{2^{n-1}+1}$	сечение	$2(n-1)+3$
$p^{2^{n-1}+1} \to p^{2^n+1}$	$S_p^{p^{2^{n-1}+1}}$	$2(n-1)+4$
$p \to p^{2^n+1}$	сечение	$2n+3$

Таким образом доказан пункт 2.

Для доказательства пункта 3. верхнюю оценку порядка 2^n получим на основе вывода в **РК:**

$p \to p$	аксиома	1
$p \to p\&p$	$\to \&$	2
$p \to (p\&p)\&(p\&p)$	$\to \&$	3
$p \to p^4$	$\to \&$	4
$p \to p^5$	$\to \&$	5
...	...	...
$p \to p^{2^n-1}$	$\to \&$	2^n-1
$p \to p^{2^n}$	$\to \&$	2^n

Для получения нижней оценки напомним понятие существенной подформулы тавтологии: подформула φ тавтологии A называется сушественной, если результат ее повсеместной замены на переменную, не входящую в A, не является тавтологией. В [5] было доказано, что формулы, имеющие k штук существенных подформул, требуют как минимум k шагов выводов в системах Фреге, а значит вывод секвенции → A в системе **РК** также содержит как минимум k различных секвенций. В формуле F_n 2^n+1 штук сушественных подформул: сама формула и различные подформулы формулы p^{2^n}.

Для доказательства пункта 4. достаточно заметить, что в приведенном выше выводе в системе **РК** не применено правило сечения, а значит результаты, полученные для системы **РК** верны и для системы **РК⁻**. Теорема полностью доказана.

Таким образом, для линейных выводов той же последовательности формул нет экспоненциального ускорения системы **QPK** по отношению к системам **SPK** и **PK,** и последняя не имеет экспоненциального ускорения по отношению к системе **РК⁻**.

Замечание 1. Утверждения нашей теоремы и теоремы Карбоне верны не только для рассмотренного семейства формул F_n. Нетрудно убедиться, что если в F_n все знаки конъюкции заменить на дизъюнкции, а применения правила → & заменить на применения правила →∨, то все утверждения обеих теорем будут верны и для нового семейства. Интересно исследовать как велико множество семейств формул, для которых верны вышеприведенные утверждения, или может будут иные соотношения между сложностями выводов в тех же системах.

Замечание 2. Если в качестве сложности выводов рассматривать вторую из основных характеристик – длину вывода, определяемую как сумму длин всех формул вывода, то нетрудно убедиться, что во всех рассмотренных выводах длины практически те же или один из них является квадратом другого, но экспоненциальный рост не наблюдается. Однако получение нижних оценок требует дополнительного изучения.

Замечание 3. Отметим также, что результаты пунктов 4. обеих теорем верны для монотонного исчисления высказываний, описанного в [6], так как сами семейства секвенций $p \to p^{2^n}$ и для конъюнкций и для дизъюнкций монотонны и в монотонном исчислении высказываний имеются те же правила → & и →∨.

4. Заключение

На основе сравнения шагов выводов некоторых множеств формул в ряде пропозициональных систем обосновано существенное различие между выводами в виде дерева и линейными выводами, что, в свою очередь, указало на «равносильность» системы с кванторами и системы с правилом подстановки для линейных выводов.

Литература

[1] A. Carbone, “Quantified propositional logic and the number of lines of tree-like proofs”, *Studia Logica*, vol.. 64, pp. 315-321, 2000.

[2] S. Cook and R. Reckhow, “The relative efficiency of propositional proof systems”, *Journal of Symbolic Logic*, vol. 44, pp. 36-50, 1979.

[3] P. Pudlák, *The Lengths of Proofs*, in S. Buss (ed.), handbook of proof Theory, North Holland, pp. 547-637, 1998.

[4] S. C. Kleene , *Introduction to Metamathemics*. D.VanNostrand Company, INC, 1952.

[5] Г. Цейтин и Ан.Чубарян, “Некоторые оценки длин логических выводов в классическом исчислении высказываний”, *ДАН Арм. ССР*, т. LV, N 1, 10-12, 1972.

[6] A. Atserias, N. Galesi and R. Gavalda, “Monotone proofs of the pigeon-hole principle”, *Mathematical logic quarterly*, vol. 47, no. 4, pp. 461-474, 2001.

Ասույթային հաշվի մի շարք համակարգերում արտածումների բարդության հարաբերությունների մասին

Հակոբ Ա. Թամազյան և Անահիտ Ա. Չուբարյան

Երևանի պետական համալսարան

e-mail: tam.hak27@gmail.com, achubaryan@ysu.am

Ամփոփում

Բանաձևերի մի քանի ընտանիքների համար համեմատված է *գծային արտածումների* քայլերի քանակը ասույթային հաշվի մի քանի համակարգերում՝ հատույթի կանոնով սեկվենցիալ համակարգում – **PK,** առանց հատույթի կանոնի նույն համակարգում - **PK⁻,** տեղադրման կանոնով նույն համակարգում - **SPK,** ծավալիչների ավելացմամբ նույն համակարգում - **QPK.** Մեր կողմից դիտարկված բանաձևերի մեկ ընտանիքի համար Ալեսսանդրա Կարբոնեի կողմից [1]-ում համեմատված են *ծառատիպ արտածումների* քայլերի քանակը հիշատակված համակարգերում և հայտնաբերված է **QPK** համակարգի գերակայությունը՝ ապացուցված է, որ այն ունի էքսպոնենցիալ արագացում **SPK** և **PK** համակարգերի նկատմամբ, իսկ վերջինները, իրենց հերթին, ունեն էքսպոնենցիալ արագացում **PK⁻** համակարգի նկատմամբ: Այս արդյունքը առիթ հանդիսացավ **QPK** համակարգի հանդեպ հետազոտումների բուռն հետաքրքրությունների համար: Սույն աշխատությունում այդ նույն համակարգերի համար ստացվել են գծային արտածումների քայլերի բոլորովին այլ հարաբերություններ՝ պարզվել է, որ **QPK** համակարգը չունի որևէ առավելություն **SPK** համակարգի նկատմամբ, պարզվել է նաև, որ բանաձևերի դիտարկվող ընտանիքների համար **PK** համակարգը ևս չունի առավելություն **PK⁻** համակարգի նկատմամբ, որն իր հերթին չունի որևէ առավելություն առավել թույլ, մոնոտոն **PMon** համակարգի նկատմամբ: Ապացուցված է նաև ստացված արդյունքների իսկությունը բանաձևերի այլ ընտանիքների, ինչպես նաև այլ համակարգերի համար:

Բանալի բառեր՝ ասույթային հաշվի սեկվենցիալ համակարգերի տարատեսակներ, Ֆրեգեի համակարգի տարատեսակներ, արտածման քայլերի քանակ, էկսպոնենցիալ արագացում:

On Proof Complexities Relations in Some Systems of Propositional Calculus

Hakob A. Tamazyan and Anahit A. Chubaryan

Yerevan State University
e-mail: tam.hak27@gmail.com, achubaryan@ysu.am

Abstract

The number of *linear proofs* steps for some sets of formulas is compared in the folowing systems of propositional calculus: **PK** – seguent system with cut rule, **PK⁻** - the same system without cut rule, **SPK** – the same system with substitution rule**, QPK** – the same system with quantifier rules**.** The number of steps of *tree-like proofs* in the same systems for some considered set of formulas is compared from Alessandra Carbone in [1] and some distinctive property of the system **QPK** is revealed: **QPK** has an exponential speed-up over the systems **SPK** and **PK,** which, in their turn, have an exponential speed-up over the system P**K⁻**. This result drew the heavy interest for the study of the system **QPK.** In this work for linear proofs steps in the same systems the other relations are received: it is showed that the system **QPK** has no preference over the system **SPK,** it is showed also that for the considered formula sets the system **PK** has no preference over the system **PK⁻,** which, in its turn, has no preference over the monotone system **PMon.** It is proved also, that the same results are reliable for some other sets of formulas and for other systems as well.

Keywords: the varieties of propositional sequent systems; the varieties of Frege systems; the number of proof steps; exponential speed-up.

Submitted 20.08.20, accepted 24.11.20.