ՀԱՅԱՍՏԱՆԻ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИ
NATIONAL ACADEMY OF SCIENCES OF ARMENIA
ДОКЛАДЫ ԶԵԿՈՒՅՑՆԵՐ REPORTS

Հատոր Том Volume 113 2013 № 1

МАТЕМАТИКА

УДК 510.64

С. М. Саядян, Анаит А. Чубарян

О некоторых системах доказательств для интуиционистской и минимальной пропозициональных логик

(Представлено чл.-кор. НАН РА Г. Б. Маранджяном 19/ IX 2012)

Ключевые слова: *интуиционистская (минимальная) логика, интуиционистски (минимально) определяющий конъюнкт, интуиционистски (минимально) определяющая дизъюнктивная нормальная форма.*

1. **Исследования сложностных характеристик выводов** в исчислении высказываний, возникшие в связи с разработками автоматизаций доказательств и носившие до конца 70-х гг. XX в. лишь фрагментарный и изолированный характер, получили бурное развитие после известного результата Кука–Рехова [1], доказавших, что $NP \neq coNP$ в том и только в том случае, если не существует полиномиально ограниченной системы доказательств классических тавтологий, т.е. для любой системы доказательств классической логики высказываний (КЛВ) найдется последовательность таких формул, нижние оценки длин кратчайших выводов которых имеют суперполиномиальную зависимость от длин формул. Исследования развивались в двух направлениях: поиска новых систем доказательств (что, естественно, потребовало уточнения самого понятия "система доказательств") и поиска класса формул, трудно доказуемых в данной системе. Логические рассуждения при доказательстве тех или иных комбинаторных утверждений, претендующих на роль труднодоказуемых, зачастую носят конструктивный (интуиционистский) характер, а иногда ограничиваются рамками минимальной логики Иогансона [2]. В частности, логическое программирование основано на интуиционистской логике.

В связи с упомянутыми обстоятельствами не менее актуальными (а может быть, и более) оказываются разработки новых систем доказательств и исследования сложностей выводов в неклассических логиках. Ряд существенных отличий между классической и неклассическими логиками

делают нетривиальными эти разработки. В частности, многие системы доказательств для классических тавтологий основаны на импликативно эквивалентных им дизъюнктивных (конъюнктивных) нормальных формах этих тавтологий, но наличие таковых форм для интуиционистских тавтологий просто невозможно в силу того, что для выводимости формул вида $A \vee B$ в интуиционизме необходимо вывести или A или B, что невозможно для дизъюнктивной нормальной формы.

Тем не менее, для несколько необычного определения элементарного дизъюнкта, введенного Г. Минцем, в [3] построен аналог системы резолюций *RI* для интуиционистской логики высказываний (ИВЛ), однако на основе этого понятия дизъюнкта не представляется возможным построение интуиционистских аналогов таких обобщений системы резолюций для КЛВ, каковыми являются Res(k) (в которой могут подвергаться резолюции сразу k переменных [4]), R(lin) (оперирующей с дизъюнктами из линейных равенств [5]), и тем более арифметических систем "Cutting Planes" [6] (систем линейных неравенств) и "Nullstellensatz refutation" [7], оперирующей с системами линейных равенств, и в которых резко укорачиваются выводы многих известных "трудновыводимых" классических тавтологий.

Нами на основе *RI*-вывода произвольной интуиционистской тавтологии вводится понятие определяющего интуиционистского конъюнкта (литералами в котором являются пропозициональные переменные с одним или двумя отрицаниями) и строится соответствующая определяющая дизъюнктивная нормальная форма (ранее в [8] вторым из соавторов эти понятия были даны для классических тавтологий).

Очевидно, что сами эти дизъюнктивные нормальные формы не являются интуиционистскими тавтологиями, т.е. не могут быть выведены в интуиционистской системе доказательств, однако на их основе уже возможно построение интуиционистских аналогий для систем Res(k), R(lin), Cutting Planes. Все вышеизложенное для минимальной логики высказываний (МЛВ) Иогансона получается на основе системы *RM* (аналога *RI*), описанного в [9].

2. **φ-определяющий конъюнкт, φ-определяющая дизъюнктивная нормальная форма для КЛВ.** Напомним некоторые понятия из [8]. Пропозициональную формулу в дизъюнктивной нормальной форме (ДНФ) мы рассматриваем как множество конъюнктов $\{К_1, К_2,..., К_г\}$, а конъюнкт К – как множество литералов (литерал – это переменная или переменная с отрицанием) . При этом ни в один конъюнкт не входит переменная и та же переменная с отрицанием. Переменные p и $\bar{p}$ называются контрарными.

Обозначим единичный m-мерный куб через E^m. Для КЛВ в [8] введены следующие определения.

Пусть φ – пропозициональная формула и $\{p_1,...,p_n\}$ – множество ее различных переменных. Для некоторого набора $\sigma = (\sigma_1, \ldots, \sigma_m) \in E^m$

конъюнкт $K = \left\{ p_{i_1}^{\sigma_1}, p_{i_2}^{\sigma_2}, \ldots p_{i_m}^{\sigma_m} \right\}$ $(1 \le m \le n)$ назовем ***φ-определяющим***, если, придавая каждой переменной p_{i_j} значения σ_i, можно определить значение формулы φ вне зависимости от значений остальных переменных. ДНФ $D = \{K_1, K_2, \ldots, K_r\}$ назовем φ-определяющей для тавтологии φ, если каждый конъюнкт из D является φ-определяющим и $\varphi = D$.

В [8] приведен *K*-алгоритм построения φ-определяющей ДНФ для произвольной классической тавтологии φ с использованием опровержения $\neg\varphi$ в общеизвестной системе резолюций R для КЛВ. Однако те же построения неприемлемы для неклассических логик высказываний, так как:

1) интуиционистская (минимальная) тавтологичность определяется как выводимость в некой интуиционистской (минимальной) системе доказательств,

2) литерал $\overline{\overline{p}}\left(\left(p \supset \bot\right) \supset \bot\right)$ не эквивалентен литералу p в ИЛВ (МЛВ), что предполагает в φ-определяюших конъюнктах для неклассических логик присутствие не только литералов p и $\bar{p}$, но и $\overline{\overline{p}}$ для ИЛВ $\left(p, p \supset \bot\right.$ и $\left(p \supset \bot\right) \supset \bot$ для МЛВ).

В настоящей работе описаны аналоги *K*-алгоритма для ИЛВ и МЛВ.

3. **Система резолюций *RI (RM).*** Описанная в [3] система *RI* является секвенциальной системой. Мы будем пользоваться общепринятыми понятиями цедента, антецедента, сукцедента, положительного и отрицательного вхождения подформул в формулу, глубины формулы, собственной подформулы, элементарной подформулы.

Модифицируя описанный Г. Цейтином метод сведения любой тавтологии к противоречивой системе формул глубины ≤ 2, в [3] заменой каждой неэлементарной подформулы новой переменной сопоставляем каждой формуле секвенцию $D_1, \ldots, D_n \to p$, где каждая из D_i имеет один из видов

$$p \supset (q \vee r);\ \left(p \supset q^*\right) \supset r;\ \ p \supset \left(q \supset r^*\right);\ \ \ p \supset q; p^*, \tag{1}$$

где p^* – или p, или $\bot$.

Для каждой формулы D_i одного из видов (1) введем соответствующую секвенцию $\overline{D_i}$ вида

$$p \to (q \vee r);\ p \supset q^* \to r;\ p, q \to r^*;\ p \to q;\ p^*.$$

Следуя [3], опишем систему *RI*.

Аксиомы системы: $p \to p$, $\bot \to p$

Правила вывода:

$$\left(\supset \overline{\ }_{1R}\right)\frac{p \supset q \to r; \sum p \to \bot}{\sum \to r} \qquad\qquad \left(\supset \overline{\ }_{2R}\right)\frac{p \supset q \to r; \sum p \to q}{\sum \to r}$$

$$\left(\supset\overline{{}_{3R}}\right)\frac{p\supset q\to r;\sum\to q}{\sum\to r}\qquad\left(\supset\overline{{}_{4R}}\right)\frac{p\supset\bot\to r;\sum p\to\bot}{\sum\to r}$$

$$\left(V_{\overline{R}}\right)\frac{p\to q\vee r;\ \Gamma\to p;\sum q\to s^{*};\prod r\to s^{**}}{\Gamma\sum\prod\to r}$$

$$\left(C_{1R}\right)\frac{pq\to r^{*};\Gamma\to p;\sum\to q}{\Gamma\sum\to r^{*}}\qquad\left(C_{2R}\right)\frac{p\to q;\Gamma\to p}{\Gamma\to q}$$

$$\left(\bot_{R}\right)\frac{\to\bot}{\to p},$$

где $\Gamma,\sum,\prod$ – цеденты, *p,q,r* – пропозициональные переменные. $\neg A$ вводится как $A\supset\bot$. Система резолюции для МЛВ *(RM)* определяется по аналогии с системой *RI*, при помощи удаления правил вывода $\left(\supset\overline{{}_{1R}}\right)$ и $\left(\bot_{R}\right)$.

В [3] доказано, что для произвольной формулы φ, если *s* – переменная, которой заменена сама формула φ, в *RI* с использованием в качестве дополнительных аксиом построенные для φ и называемые дизъюнктами вышеописанные секвенции D_i выводима секвенция $\to s$ тогда и только тогда, когда секвенция $\to\varphi$ выводима в системе натурального вывода для ИВЛ, т.е. является интуиционистской тавтологией.

4. **I-алгоритм построения φ-определяющей ДНФ в *RI*.** Прежде чем перейти к описанию алгоритма, введем некоторые понятия, используемые в данном построении.

Основными переменными формулы φ, представленной секвенциями в *RI*, назовем переменные, которые входят в формулу φ и

(1) при построении вывода формулы φ данная переменная не участвует в правиле $\dfrac{p\supset q\to r;\sum p\to\bot}{\sum\to r}\left(\supset\overline{{}_{1R}}\right)$ в качестве переменной *q*,

(2) при построении вывода формулы φ данная переменная не участвует в правиле $\dfrac{p\supset q\to r;\sum\to q}{\sum\to r}\left(\supset\overline{{}_{3R}}\right)$ в качестве переменной *p*.

Секвенцию $\Gamma\to\Delta$ назовем основной, если она содержит хотя бы одно вхождение основной переменной и не является собственной аксиомой *RI*.

I-алгоритм заключается в следующем.

1) Для данного вывода $\to s$ в *RI* построим соответствующее дерево-вывод. Отметим в нем пути, которые удовлетворяют следующим условиям:

а) ведут от вершины, которым приписаны основные секвенции, к вершине, которой приписана секвенция $\to s$,

б) ни одна из основных переменных не имеет одновременно положительного и отрицательного вхождения в секвенции данного пути,

в) множество различных секвенций этого пути не содержится в множестве различных секвенций, приписанных вершинам некоего иного пути, удовлетворяющего пунктам а) и б) .

2) Для каждого из отмеченных путей поступим следующим образом. Поставим данной ветви в соответствие некоторый пустой конъюнкт K_i. Двигаясь от вершины, которой приписана секвенция $\to s$, вверх по этому пути включим в конъюнкт K_i все основные переменные из формул секвенции, приписанной данной вершине. При этом пополнение K_i происходит следующим образом:

а) если какая-либо секвенция на ветви содержит основную переменную p_j в сукцеденте, добавим $\overline{p}_j$ в K_i,

б) если какая-либо секвенция на ветви содержит основную переменную p_j в качестве формулы антецедента, добавим $\overline{p}_j$ в K_i,

в) если секвенция имеет вид $p_j \supset x \to y$, где p_j - основная переменная, добавляем $\overline{\overline{p}}$ в K_i,

г) если секвенция имеет вид $p_j \supset p_n \to x$, где p_j и p_n основные переменные, т. е. подформула $p_j \supset p_n$ имела положительное вхождение, то берем дополнительный конъюнкт K_l, равный K_i, и добавляем $\overline{\overline{p}}_j$ в K_l, а p_n в K_i.

Процесс включения переменных в K_i прекращается на начальной вершине (аксиоме) этого пути.

Проделав вышеописанный процесс для всех отмеченных путей дерева, получим множество $D = \{K_1, K_2, \ldots, K_m\}$, где m не превышает двукратное количество отмеченных путей.

Конвертацией вхождения переменной p формулы φ назовем изменения ее вхождения с отрицательного на положительное и наоборот.

Отметим, что при переходе от формулы φ к соответствующей системе дизъюнктов-аксиом единожды происходит конвертация вхождений основных переменных, следовательно, после построения конъюнкта K_i введем конъюнкт $\tilde{K}_i$, который содержит все литералы K_i с отрицанием. Если в K_i был литерал p_i, то в $\tilde{K}_i$ он будет преобразован в $\overline{p}_i$, если в $K_i - \overline{p}_i$, то в $\tilde{K}_i - \overline{\overline{p}}_i$, если в $K_i - \overline{\overline{p}}_i$, то в $\tilde{K}_i - \overline{p}_i$ (так как в ИЛВ $\overline{\overline{p}}_i \sim \overline{p}_i$) .

Утверждение. Для произвольной интуиционистской тавтологии φ каждый построенный по *I*-алгоритму конъюнкт $\tilde{K}_i$ представляет собой φ-определяющий конъюнкт, а множество $\tilde{D} = \{\tilde{K}_1, \tilde{K}_2, \ldots, \tilde{K}_m\}$ φ-определяющую ДНФ.

Доказательство получается по аналогии с приведенным в [8] доказательством.

Отметим, что каждый φ-определяющий конъюнкт, построенный по *I*-алгоритму, содержит только два типа литералов: $\overline{p}$ или $\overline{\overline{p}}$ (ранее предполагаемое присутствие литерала *p* отпало).

Определяющие конъюнкты и определяющая ДНФ для тавталогий МЛВ строятся аналогичным образом, на основе RM–выводов.

Отметим также, что так как каждая тавтология ИЛВ (МЛВ) является классической тавтологией, то заменой $\overline{\overline{p_i}}$ на p_i $(p_i \supset \bot) \supset \bot$ на p_i) для всех переменных произвольной тавтологии ИЛВ (МЛВ) получаем из I-определяющей (*M*-определяющей) ДНФ определяющую для КЛВ. Обратное, естественно, не верно.

5. **Новые системы доказательств для ИЛВ (МЛВ).** Естественно, что уже на основе построенных для ИЛВ (МЛВ) определяющих ДНФ можно для этих логик построить аналоги Res(k), R(lin), Cutting Planes (CP), Nullstellensatz refutation (NR).

Продемонстрируем построение ICP (CP для ИЛВ) на основе CP.

Приведем формальное определение системы CP, следуя [6].

Сначала определим класс выражений $CP(\xi)$. Если $\alpha \in Z$ и $i \in N$, то $\alpha \in \xi$ и $(\alpha \cdot x) \in \xi$. Если $E, F \in \xi$ и $\alpha \in Z$, то $\alpha \cdot E$ и $E + F$ принадлежат ξ. Скажем, что положительное целое число c делит выражение $E = \sum a_i \cdot E_i$, принадлежащее ξ, и обозначим c|E, если для всех i верно c|a_i. Частным является $E' = \sum b_i \cdot E_i$, где $b_i = a_1 / c$.

Формулами CP являются выражения вида $E \geq F$, где $E, F \in \xi$.

Собственными аксиомами системы CP являются неравенства

$$x \geq 0, \ -x \geq -1$$

для произвольной арифметической переменной x.

Правилами вывода системы CP являются следующие пять правил:

1) транзитивности $\dfrac{E \geq F \ F \geq G}{E \geq G}$,

2) обычных арифметических упрощений неравенства: коммутативность и ассоциативность суммы и произведения, дистрибутивность произведения относительно сложения, вынесения выражений за скобки, перенос членов с одной стороны неравенства в другую сторону с изменением знака коэффициента, вычисление сумм и произведений целых чисел, подстановка выражения 0 вместо $0 \cdot E$ и т.д.,

3) суммирования: $\dfrac{E \geq F \ F \geq H}{E + G \geq F + H}$,

4) умножения на натуральное число c: $\dfrac{E \geq F}{c \cdot E \geq c \cdot F}$,

5) деления: если $c \in N,\ c > 0,\ b \in Z$, то $\dfrac{E \geq b}{E' \geq [b/c]}$ где E' частное от деления E на c.

Под конъюнктивной нормальной формой (КНФ) K понимается семейство дизъюнктов $\{D_1, D_2 \ldots, D_l\}$, а каждый дизъюнкт $D_i = \left\{ p_{i_1}^{\sigma_{i_1}}, p_{i_2}^{\sigma_{i_2}}, \ldots, p_{i_s}^{\sigma_{i_s}} \right\}$ понимается как множество литералов, причем ни в один дизъюнкт не входят переменная и ее отрицание одновременно.

Каждому дизъюнкту $D_i = \left\{ p_{i_1}^{\sigma_{i_1}}, p_{i_2}^{\sigma_{i_2}}, \ldots, p_{i_s}^{\sigma_{i_s}} \right\}$ сопоставляется неравенство

$$\sum\nolimits_{j=1} \alpha_{ij}\left(p_{ij}, \sigma_{ij}\right) \geq 1, \text{ где } \alpha_{ij}\left(p_{ij}, \sigma_{ij}\right) = \begin{cases} x_{ij}, & \text{åñëè } \sigma_{ij} = 1 \\ 1 - x_{ij}, & \text{åñëè } \sigma_{ij} = 0 \end{cases},$$

а x_{ij} – арифметическая переменная.

Для каждой КНФ $K = \{D_1, D_2 \ldots, D_l\}$ в качестве аксиом системы СР фиксируется множество неравенств, сопоставленных каждому дизъюнкту $D_i \ (1 \leq i \leq l)$.

Скажем, что КНФ $K = \{D_1, D_2 \ldots, D_l\}$ СР–опровержима, если существует такая последовательность неравенств $E_1, E_2, \ldots E_m$, что каждое $E_i \ (1 \leq i \leq m)$ либо является собственной аксиомой, либо аксиомой системы CP, соответствующей КНФ K, либо выводится из предыдущих неравенств в последовательности по одному из правил вывода, и E_m является неравенством вида $0 \geq 1$. $E_1, E_2, \ldots E_m$ будем называть опровержением КНФ K.

Скажем, что формула A СР -выводима, если КНФ K, соответствующая формуле $\neg A$ СР-опровержима. Опровержение K будем называть выводом формулы A.

Система ICP полностью совпадает с СР, но КНФ, построенная как отрицание определяющей ДНФ для произвольной интуиционистской тавтологии, понимается как семейство дизъюнктов, каждый из которых состоит из литералов p^{σ}, где $p^0 = \overline{p}$, а $p^1 = \overline{\overline{p}}$, но арифметическое неравенство, сопоставляемое дизъюнкту, полностью совпадает с вышеописанным.

Те же изменения лишь при определении дизъюнктов имеют место при определении систем Res(k), R(lin), NR для ИЛВ (МЛВ).

6. **Основополагающими для сравнения эффективности различных систем** доказательств и классической логики и неклассических логик являются следующие понятия:

***l* -сложность (длина) вывода**, определяемая как сумма длин всех формул (или всех их представлений) вывода**, *t*-сложность** – как количество шагов вывода;

***l*-сложность (*t*-сложность) формулы φ** в системе Ф, определяемая

как минимальное значение среди l-сложностей (t-сложностей) Ф-выводов формулы φ и обозначаемая через $l_\varphi^\Phi\left(t_\varphi^\Phi\right)$.

Пусть Φ_1 и Φ_2 суть пропозициональные системы выводов. Следуя [1] , напомним понятие полиномиальной сводимости.

Определение 1. Φ_1 p-l-сводится к Φ_2 (Φ_1 I $_l$ Φ_2), если существует такой полином p( ), что для любой формулы φ, выводимой и в Φ_1 и в Φ_2 , $l_\varphi^{\Phi_2} \le p\left(l_\varphi^{\Phi_1}\right)$.

Определение 2. Φ_1 p-l-эквивалентна Φ_2 ($\Phi_1 \sim_l \Phi_2$), если (Φ_1 I $_l$ Φ_2) и (Φ_2 I $_l$ Ф1).

Аналогично вводятся понятия p-t-сводимости и p-t-эквивалентности, на основе t-сложности выводов.

Определение 3. Φ_1 имеет экспоненциальное l-ускорение (t-ускорение) относительно Φ_2, если Φ_2I $_l$$\Phi_1$ (Φ_2I $_t$$\Phi_1$) и существует последовательность выводимых и в Φ_1, и в Φ_2 формул таких, что $l_{\varphi_n}^{\Phi_2} > 2^{\theta\left(l_{\varphi_n}^{\Phi_1}\right)}\left(t_{\varphi_n}^{\Phi_2} > 2^{\theta\left(l_{\varphi_n}^{\Phi_1}\right)}\right)$.

Теорема.

1. *ICP, IRes(k), IR(lin), INR имеют экспоненциальное l-ускорение (t-ускореие) относительно RI;*
2. *MCP, MRes(k), MR(lin), MNR имеют экспоненциальное l-ускорение (t-ускорение) относительно RM.*

Доказательство основано на аналогичных доказательствах для соответствующих пар систем КЛВ с рассмотрением в качестве “плохих примеров“ последовательностей формул $\neg\neg\varphi_n$ для ИЛВ $((\varphi_n \supset \bot) \supset \bot$ для МЛВ) для последовательностей φ_n , рассматриваемых для каждой из четырех пар указанных систем выводов в КЛВ.

Работа выполнена в рамках гранта 11-1b023 ГКН РА.

Ереванский государственный университет
E-mails: sayadyans@yahoo.com, achubaryan@ysu.am

С. М. Саядян, Анаит А. Чубарян

О некоторых системах доказательств для интуиционистской и минимальной пропозициональных логик

Введены понятия определяющего конъюнкта и определяющей дизъюнктивной нормальной формы для пропозициональных формул, являющихся интуиционистскими (минимальными) тавтологиями. Описаны алгоритмы построения упомянутых дизъюнктивных нормальных форм для обеих неклассических пропозициональных логик. Продемонстрирован способ построения

на основе описанных дизъюнктивных нормальных форм более эффективных систем доказательств для указанных логик.

Ս. Մ. Սայադյան, Անահիտ Ա. Չուբարյան

Ինտուիցիոնիստական և մինիմալ ասույթային տրամաբանությունների որոշ արտածման համակարգերի վերաբերյալ

Ներմուծվել են որոշիչ կոնյունկտի և որոշիչ դիզյունկտիվ նորմալ ձևի գաղափարները ասույթային հաշվի այն բանաձևերի համար, որոնք ինտուիցիոնիստական և մինիմալ նույնաբանություններ են: Նկարագրված են նշված դիզյունկտիվ նորմալ ձևերի կառուցման ալգորիթմները երկու վերոհիշյալ տրամաբանությունների համար: Ցուցադրված է նաև այդ տրամաբանությունների համար նկարագրված դիզյունկտիվ նորմալ ձևերի հիման վրա առավել արդյունավետ արտածման համակարգերի կառուցման եղանակը:

S. M. Sayadyan, Anahit A. Chubaryan

On Some Proof Systems for Intuitionistic and Minimal Propositional Logics

The notions of determinative conjunct and determinative disjunctive normal form for propositional formulae, which are intuitionistic (minimal) tautologies are introduced. Some algorithms for construction of mentioned disjunctive normal forms for both non-classical propositional logics are described. The way of construction based on the described disjunctive normal forms of more effective proof systems for the mentioned logics is shown.

Литература

1. *Cook S. A., Reckhow A. R.* - The Journal of Symbolic Logic . 1979. V. 44. P.36-50.
2. *Kleene S. C.* - Introduction to metamathematics. 1952.
3. *Минц Г. Е.* - Семиотика и информатика. 1985. В. 25. С. 120-135
4. *Krajicek J.*- Journal Fund. Math. 2001.V. 170. P. 123-140.
5. *Raz R., Tzameret I.* - Ann. Pure Appl. Logic. 2008. V. 155. N 3. P.194-224.
6. Buss S.R. Handbook of Proof Theory. 1998
7. *Pudlak P.*- Set and proofs in Logic Coll. 1999. V. 97. P. 197-218.
8. *Чубарян А. А.* – Изв. НАН РА. 2003. Т. 35. N5. С. 71-84.
9. *Bolibekyan H., Chubaryan A.* Logic Colloquium, 2003. P 56.