

Подход Колмогорова и Гёделя к интуиционистской логике и работы последнего десятилетия в этом направлении.

С.Н.Артёмов *

УМН т.59 вып.2(356), март - апрель, 2004

УДК: 510.23, 510.24, 510.25, 510.642, 510.648, 510.652.

Аннотация

Интуиционистская математика была создана Брауэром на основе конструктивных способов рассуждений, при которых критерием истинности является наличие доказательства. В работах Колмогорова и Гёделя была предложена идея интерпретации интуиционистской логики на основе классических понятий задачи и ее решения и понятия доказуемости. В 1933 году Гедель сделал первое существенное продвижение в этом направлении. Несмотря на большие успехи в исследовании интуиционизма, точной модели интуиционистской логики на основе этого подхода не было построено вплоть до работы автора 1995 года. В настоящей работе мы расскажем о работах последнего десятилетия, полученных в русле этого подхода.

1 Введение

Согласно Брауэру, в интуиционистской математике истинность означает не что иное, как доказуемость. Вот выдержка (в переводе автора) из двухтомника А. Трулстры и Д. ван Далена *Конструктивизм в математике* ([82], стр. 4), в которой коротко формулируются принципы интуиционистской семантики по Брауэру:

“Не имеет смысла говорить об истинности или ложности математического утверждения вне зависимости от нашего знания, касающегося этого утверждения. Данное утверждение *истинно*, если у нас есть его доказательство, и *ложно*, если мы можем показать, что предположение о том, что это утверждение имеет доказательство, ведет к противоречию.”

*Graduate Center CUNY, 356 Fifth Avenue, New York, NY 10016, U.S.A.; Московский Государственный Университет, Механико - математический факультет, Москва 119992, Россия. E-mail: SArtemov@gc.cuny.edu; URL: <http://www.cs.gc.cuny.edu/~sartemov/>

Система аксиом для интуиционистской логики была предложена Гейтингом в 1930 году на основе неформальной семантики Брауэра; за точными формулировками мы отсылаем читателя к фундаментальным монографиям [5, 82]. Через **Int** мы будем обозначать исчисление Гейтинга для пропозициональной интуиционистской логики, известное также под именем **IPC**. Гейтинг и Колмогоров в 1931-34 годах сформулировали набор неформальных условий, которым должна удовлетворять семантика интуиционистской логики [4, 6, 49, 50]. Эти условия, получившие название *семантики Брауэра-Гейтинга-Колмогорова (ВНК)*, предполагают, что истинность формулы означает наличие ее доказательства. В свою очередь, доказательство сложного утверждения выражается через доказательства составных его частей таким образом, что

- доказательство $A \wedge B$ состоит из доказательства утверждения A и доказательства утверждения B ,
- доказательство $A \vee B$ дается предъявлением доказательства A или доказательства B ,
- доказательством $A \rightarrow B$ является конструкция, которая по каждому доказательству A находит какое-либо доказательство B ,
- тождественно ложное высказывание \perp — это утверждение, не имеющее доказательства, $\neg A$ есть $A \rightarrow \perp$.

Семантика *ВНК* предложила совершенно новый взгляд на логические операции. В частности, импликация $A \rightarrow B$, которая в обычной классической логике не имеет самостоятельного смысла а выражается через остальные связки, в семантике *ВНК* задает тотальную функцию из множества доказательств A в множество доказательств B .

Следует отметить, что А.Н. Колмогоров в [6] говорит о *логике решения задач*. В заметке 1985 года [7] А.Н. Колмогоров пишет

“Работа [6] писалась в надежде на то, что логика решения задач сделается со временем постоянным разделом курса логики. Предполагалось создание единого логического аппарата, имеющего дело с объектами двух типов - высказываниями и задачами.”

Работа А.Н. Колмогорова [6] написана неформально, что оставляло возможность рассматривать разные математические модели “решения задач”. Однако, с 1980х годов стало общепринятым **доказуемое** понимание колмогоровского “решения задач” (см. [39, 82, 83]). Причины этого довольно естественны. В математической логике моделью понятия математической задачи и ее решения являются формулы в языке подходящей логико-математической теории (например, в арифметике Пеано, теории множеств Цермело-Френкеля, и т.п.) и их формальные доказательства в данной теории. Именно поэтому теория множеств сейчас трактуется как “теория Цермело-Френкеля **ZF**”, элементарная теория чисел как “формальная арифметика первого порядка (арифметика Пеано **PA**)”, “задача” и “решение задачи” как “формула в данном формальном языке” и “доказательство формулы в подходящей формальной теории”.

Несмотря на значительный интерес к этому вопросу, найти точную семантику доказательств для интуиционистской логики не удавалось в течение более 60-ти лет.

Общая идея понимания логических связей как операций над объектами, являющимися обоснованиями истинности, оказалась чрезвычайно плодотворной. Клини в [52] предложил рассматривать в качестве “обоснований истинности” вычислимые функции, а не доказательства, как в семантике *ВНК*, открыв при этом *вычислительную интерпретацию* интуиционистской логики. Стало понятно, что конструктивный (интуиционистский) логический вывод — это одновременно и вычислительная программа, и доказательство корректности этой программы. Этот подход породил целый класс так называемых “семантик реализуемости” для конструктивных логико-математических теорий; в [81] можно найти обзор основных идей и достижений в этой области.

Ни реализуемость Клини, ни ее разновидности не решили проблему нахождения семантики *ВНК*. Сам Клини протестовал против попыток отождествить его реализуемость с *ВНК*. Поведение вычислительных программ как “обоснований истинности” существенно отличается от поведения математических доказательств. Доказательства в норме допускают алгоритмическую проверку корректности, в то время, как вычислительные программы подобных алгоритмов проверки корректности иметь не могут. В результате, предикат

p есть доказательство *F*

разрешим, в то время как предикат

r реализует *F*

не может быть разрешимым в силу теоремы Райса. Говоря неформально, реализуемая семантика допускает слишком много “свидетельств истинности” и слишком много логических формул являются реализуемыми, больше чем имеется интуиционистских теорем. Согласно результату Плиско [11], множество реализуемых формул первого порядка не является рекурсивно аксиоматизируемым. До сих пор остается открытым вопрос об аксиоматизируемости (рекурсивной перечислимости) множества реализуемых пропозициональных формул.

Еще один “канонический” пример вычислительной семантики для интуиционистской логики — *изоморфизм Карри-Ховарда* интуиционистских выводов (т.е. доказуемых объектов) и элементарных прототипов вычислительных программ в форме *λ-термов* (см., например [44, 83]). С точки зрения оснований математики, значение изоморфизма Карри-Ховарда ограничено рамками вычислительной семантики. Он не является семантикой *ВНК*, поскольку *λ-термы* как доказательства есть не что иное, как выводы в том самом исчислении Гейтинга (в форме натурального вывода), обоснованием которого и должна стать *ВНК*. Таким образом, доказуемое прочтение изоморфизма Карри-Ховарда являет собой замкнутый круг

типа “формула F доказуема в **Int** тогда, и только тогда, когда формула F доказуема в **Int**” и, следовательно, не дает семантики независимой от изначального исчисления Гейтинга. Обзоры [13, 38, 82] служат хорошими источниками по вычислительной семантике интуиционистской логики.

Известен также ряд попыток построения *ad hoc* семантики *ВНК*, где в качестве “доказательств” фигурировали вычислительные программы специального вида или абстрактные объекты, не связанные с общепринятыми математическими моделями доказательств. Так в [9, 62, 74] и многих других работах изучались абстрактные математические модели (для справок см. также [28, 29, 81]). В частности, в [9] “задача” определяется непустым конечным множеством решений, в котором выделено некоторое подмножество фактических решений, импликация $A \rightarrow B$ определяется отображениями из A в B . Логика финитных задач не совпадает с интуиционистским исчислением. Неизвестно также, является ли эта логика разрешимой (см. [13, 84] для более подробного анализа этого подхода). В [62] была рассмотрена реализуемость интуиционистской логики абстрактными, не обязательно вычислимыми функционалами. Попытка формализации семантики *ВНК* была предпринята Крайзелем в [53, 54, 55] в его “теории конструкций”, первоначальный вариант которой оказался противоречивым. Последующее исправление, сделанное Гудманом в [48], привело к потере связи с *ВНК*, поскольку “доказательство” импликации $A \rightarrow B$ перестало быть применимым ко всем “доказательствам” A (см. также [85] для полного анализа теории Крайзеля-Гудмана).

Семантика Кузнецова-Муравицкого-Голдблатта-Булоса ([8, 32, 33, 47]) для **Int** была уже связана с реальной математической моделью доказуемости — гёделевским предикатом доказуемости в арифметике. Однако, эта семантика не содержит ни индивидуальных доказательств, ни операций над ними. Она в сильной степени неконструктивна, т.к. реализуемость в этой модели имеет гиперарифметическую сложность, и, таким образом, далека от семантики *ВНК*.

Определенный итог попыткам построить *ad hoc* семантику *ВНК* был подведен в 1983 году в [85]:

“Интерпретация интуиционистских теорий в терминах доказательств и конструкций . . . пока не получила точной формулировки.”

В обзоре 1986 года [38] мы читаем:

“Искомая интерпретация интуиционистской логики по Гейтингу [имеется ввиду семантика *ВНК*, С.А.] . . . упорно ускользает.”

2 Подход Колмогорова - Гёделя

Как мы видели выше, подход Колмогорова 1932 года (см. [6, 7]) состоял в том, чтобы построить объединенную логику высказываний и доказательств

в обычной **классической математике**, и в ее рамках интерпретировать интуиционистскую логику, не опираясь на специфические интуиционистские основания. Того же рода подход можно найти и у Гёделя. В его работе 1933 года ([45]) был сделан первый шаг в построении точной семантики интуиционизма на основе классической доказуемости. Гёдель рассмотрел классическую модальную логику **S4** как исчисление, задающее свойства доказуемости в классической математике, и построил сведение интуиционистской пропозициональной логики **Int** к **S4**. Разумеется, цель Гёделя не могла быть достигнута прежде, чем новый логический оператор модальности получил точную интерпретацию через классическую математическую модель доказуемости.

Работа Гёделя [45] свела **Int** к **S4**, что оказалось составной частью окончательного решения, найденного в 1995 году (см. ниже). Вот Гёделевская формулировка модального исчисления классической доказуемости **S4** ([45]):

1. *Аксиомы и правила классической логики*
2. $\Box(F \rightarrow G) \rightarrow (\Box F \rightarrow \Box G)$
3. $\Box F \rightarrow F$
4. $\Box F \rightarrow \Box \Box F$
5. *Правило:*

$$\frac{\vdash F}{\vdash \Box F}$$

Согласно Гёделю, логика **S4** выражает свойства доказуемости как логического (модального) оператора.

Формализуя брауэровское понимание логической истинности как доказуемости, Гёдель определяет перевод $tr(F)$ пропозициональной формулы F с интуиционистского языка на язык классической логики с модальностью \Box : $tr(F)$ получена путем проставления \Box перед каждой подформулой формулы F . Говоря неформально, обычная процедура определения классической истинности формулы по дереву построения формулы при анализе $tr(F)$ будет проверять каждую новую подформулу F не на истинность, а на доказуемость, как и положено “по Брауэру”. Оказалось ([45, 64]), что такой перевод дает точное вложение интуиционистской логики **Int** в **S4**, т.е. в классическую логику, пополненную оператором доказуемости.

$$\mathbf{Int} \text{ доказывает } F \Leftrightarrow \mathbf{S4} \text{ доказывает } tr(F)$$

Однако изначальная задача определения **Int** через классическую доказуемость не была решена, поскольку сама логика **S4** осталась без точной доказуемостной модели. Как сразу же заметил сам Гёдель, напрашивающаяся интерпретация модальности $\Box F$ как утверждения F *доказуема в данной формальной системе* противоречит второй теореме Гёделя о неполноте. В самом деле, формула $\Box(\Box F \rightarrow F)$ легко выводится в **S4** из аксиомы рефлексивности $\Box F \rightarrow F$ по правилу (5). С другой стороны, при интерпретации модальности \Box как предиката $Provable_T(\cdot)$ формальной доказуемости

в теории T эта формула становится ложным утверждением о том, что рефлексия для теории T доказуема в самой теории T :

$$\text{Provable}_T(\text{Provable}_T(F) \rightarrow F).$$

Следуя Гёделю, мы исходим из того, что математической моделью доказуемости является гёделевский предикат доказательств $\text{Proof}_T(x, y)$, обозначающий

x есть код доказательства в T формулы с кодом y

а также гёделевский предикат доказуемости $\exists x \text{Proof}_T(x, y)$, означающий

формула с кодом y доказуема в T

(см. [32, 33, 79]).

Ситуацию после работы Гёделя [45] можно условно изобразить следующей схемой, где “ \leftrightarrow ” означает точное вложение:

$$\text{Int} \leftrightarrow \mathbf{S4} \leftrightarrow ??? \leftrightarrow \text{КЛАССИЧЕСКИЕ ДОКАЗАТЕЛЬСТВА}$$

В лекции, прочитанной в Вене в 1938 году [46] Гёдель возвращается к вопросу о моделировании интуиционистской логики в классической логике, пополненной оператором доказуемости, и вновь указывает на остававшийся нерешенным вопрос о точной доказуемостной интерпретации его исчисления доказуемости. Говоря о своей работе 1933 года, Гёдель отмечает о ней следующее:

“Я снабдил обычное пропозициональное исчисление связкой B (“доказуемо в абсолютном смысле”) и аксиомами [приводятся аксиомы $\mathbf{S4}$ с B в качестве \square , С.А.]. *Интуиционизм выводим из этого.* Примечательно, что хотя эти аксиомы чрезвычайно правдоподобны, *есть утверждения о B , которые очевидно ложны для каждого определенного B .*”

В этой же лекции Гёдель также впервые предложил идею использования формата явных доказательств *t есть доказательство F* для интерпретации своего исчисления доказуемости. Именно на этом пути и было найдено окончательное решение в [17], [19].

Ниже мы будем называть задачу об интерпретации интуиционистской логики в классической логике с оператором доказуемости, которой занимался Гёдель в 1933 году и которая оставалась нерешенной из-за отсутствия точной доказуемостной модели самого гёделевского оператора доказуемости, **задачей Гёделя о доказуемостном исчислении.**

Изучением исчисления доказуемости Гёделя и его взаимоотношением с интуиционистской логикой занимался выдающийся математик Петр Сергеевич Новиков, чьи лекции 1950х годов и изданная на их основе после кончины Петра Сергеевича монография [10] чрезвычайно способствовали

росту интереса к этой тематике в России и окончательному решению задачи Гёделя о доказуемости исчисления в 1995 году.

Обзор исследований по семантике доказуемости для **S4** можно найти в [19]. Приведем лишь некоторые работы, которые касались этого вопроса: [8, 15, 32, 33, 36, 47, 56, 63, 65, 67, 68, 69, 75, 76]. Однако, задача Гёделя о доказуемости исчисления оставалась нерешенной. Более того, в 1963 году Р. Монтегю после тщательного анализа объявил эту задачу безнадежной [67].

Источник трудностей с доказуемостью интерпретацией модальности лежит в неявном характере квантора существования “ \exists ” в теориях первого порядка. Это явление иногда называют \exists -болезнью логики первого порядка. Рассмотрим, к примеру, первопорядковую арифметику Пеано **PA** и принцип рефлексии в ней, т.е. все формулы вида $\exists x \text{Proof}_{\text{PA}}(x, F) \rightarrow F$. Этот принцип рефлексии невыводим в **PA**, поскольку, говоря неформально, истинность посылки этой импликации недостаточна для вывода об истинности заключения. Формула $\exists x \text{Proof}_{\text{PA}}(x, F)$ не дает конкретного доказательства формулы F , т.к. это x может быть *нестандартным* натуральным числом, тем самым, не являющимся кодом никакого конкретного вывода в **PA**.

Иная картина наблюдается в языке с явным представлением доказательств терминами: принцип *явной рефлексии* $\text{Proof}_{\text{PA}}(p, F) \rightarrow F$ для каждого конкретного вывода p доказуем в **PA**. В самом деле, если $\text{Proof}_{\text{PA}}(p, F)$ истинна, то F , очевидно, доказуема в **PA**, что влечет доказуемость формулы $\text{Proof}_{\text{PA}}(p, F) \rightarrow F$. Если же $\text{Proof}_{\text{PA}}(p, F)$ ложна, то $\neg \text{Proof}_{\text{PA}}(p, F)$ истинна и доказуема, следовательно $\text{Proof}_{\text{PA}}(p, F) \rightarrow F$ также доказуема.

Это наблюдение подсказывает и средство от \exists -болезни: явное представление объектов терминами вместо неявного их задания кванторами \exists . В нашем случае речь идет о представлении доказательств достаточно полной системой термов t и их использовании в формате $\text{Proof}_{\text{PA}}(t, F)$, вместо неявного представления доказательств кванторами существования в формуле доказуемости $\exists x \text{Proof}_{\text{PA}}(x, F)$. В контексте задачи о доказуемости семантике **S4** и **Int** это означает возврат к изначальному формату *BHK* после попыток найти ответ в рамках более простого языка модальной логики. Как уже упоминалось выше, Гёдель еще в 1938 году предложил использовать формат явных доказательств для интерпретации **S4**, однако, эта его работа оставалась неопубликованной до 1995 года. По современным понятиям этот формат является примером *LDS*-языка в смысле [43].

В 1992-93 годах автор и Т. Штрассен ([25, 26, 27]) нашли первые системы логик доказательств в формате $t:F$, обозначающем t есть доказательство F . Первые логики из [25, 26, 27] не содержали операций над доказательствами и не ставили целью реализацию модальности в полном объеме.

Еще до опубликования в 1995 году работы Гёделя [46] с предложением искать доказуемую семантику для **S4** через доказуемые термины и совместную логику высказываний и доказательств, автору удалось найти искомое решение задачи Гёделя об исчислении доказуемости. В осеннем семестре 1994 года во время визита в Амстердамский Университет автором была найдена первая версия логики доказательств **LP** и теорема о реали-

зуюмости **S4** в **LP**, которые тогда же в конце 1994 года были доложены на семинаре в Амстердаме и конференции в Мюнстере. Текст с полными доказательствами вышел в материалах Института Математических Наук Корнелльского университета в 1995 году [17].

3 Логика Доказательств

Близким родственником **LP** является типовая комбинаторная логика **CL** (см., например, [83]). Хорошо известно, что комбинаторные термы могут пониматься как доказуемые термы в гильбертовской системе. Константы означают доказательства пропозициональных аксиом:

$$\mathbf{k}^{A,B} : (A \rightarrow (B \rightarrow A)), \quad \mathbf{s}^{A,B,C} : [(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))]$$

Переменные в **CL** обозначают произвольные доказательства, операция *апликации* “.” соответствует **интернализированному** правилу *modus ponens*.

$$t:(F \rightarrow G) \rightarrow (s:F \rightarrow (t \cdot s):G)$$

Интернализация - это формализация математической конструкции в виде соответствующего объекта в языке данной теории. В нашем случае операция перехода от выводов формулы $F \rightarrow G$ и формулы F к выводу формулы G по правилу *modus ponens* интернализирована в виде формальной операции *апликации* “.” на комбинаторных термах.

Забывчивая проекция **CL**, при которой каждое вхождение формул вида $t:F$ заменяется на $\Box F$, соответствует импликативному интуиционистскому фрагменту **S4**, состоящему только из формул $\Box A_1 \wedge \dots \wedge \Box A_n \rightarrow \Box B$, где A_1, \dots, A_n, B не содержат модальностей. Это наблюдение показывает насколько велика дистанция между типовой комбинаторной логикой и системой, дающей решение задачи Гёделя об исчислении доказуемости, в которой речь идет о реализации всей **S4** доказуемыми термами.

Определение Полиномы доказательств это термы, построенные из *доказуемых переменных* x, y, z, \dots и *доказуемых констант* a, b, c, \dots посредством трех операций: *апликация* “.” (двуместная), *объединение* “+” (двуместная), и *проверка доказательств* “!” (одноместная).

Точная семантика полиномов доказательств и формул логики доказательств обсуждается ниже после формулировки **LP**. Сейчас, однако, будет полезно иметь представление об общем формате **LP**. Переменные будут использоваться для обозначения произвольных доказательств, а константы – для доказательств аксиом. Каждое доказательство доказывает конечное множество теорем. Операция апликации соответствует интернализированному правилу *modus ponens*: для данных s и t доказательство $s \cdot t$ доказывает все формулы G такие, что s доказывает $F \rightarrow G$ и t доказывает F для некоторого F . Объединение “ $s + t$ ” доказательств s и t – это доказательство, которое доказывает все то, что доказывает s и все то, что доказывает t . Наконец, “!” интерпретируется как программа проверки корректности,

которая по доказательству t вычисляет доказательство того, что t доказывает F ([17, 19]).

Язык *логики доказательств* **LP** это язык классической логики высказываний, пополненный новым правилом порождения формул: для всякого полинома доказательств p и формулы F можно образовать новую формулу $p:F$, изображающую “ p есть доказательство F ”. Возможно также и теоретико-типовое прочтение, при котором формулы становятся типами, а $p:F$ понимается как утверждение “терм p имеет тип F ”.

Аксиомы и правила вывода **LP**:

A0. аксиомы классической логики высказываний

A1. $t:(F \rightarrow G) \rightarrow (s:F \rightarrow (t \cdot s):G)$ (аппликация)

A2. $t:F \rightarrow F$ (явная рефлексия)

A3. $t:F \rightarrow !t:(t:F)$ (проверка доказательств)

A4. $s:F \rightarrow (s+t):F, \quad t:F \rightarrow (s+t):F$ (объединение)

R1. Modus Ponens

R2. $\vdash c:A$, где $A \in A0-A4$, c есть доказуемая константа

Ниже “ \vdash ” будет означать выводимость в **LP**, если не оговорено противное. Под *спецификацией констант* CS мы будем понимать конечное множество формул вида $c_1:A_1, c_2:A_2, \dots, c_n:A_n$, где каждая A_i есть аксиома вида *A0-A4*. По умолчанию, с каждым выводом в **LP** мы связываем спецификацию констант CS , произведенных по правилу *R2* в данном выводе. Как при работе с выводами в **LP**, так и при определении интерпретации языка **LP** всегда подразумевается некоторая спецификация констант, которая обычно ясна из контекста, и явное упоминание о которой часто опускается.

Фундаментальным свойством **LP** является возможность интернализации своих собственных выводов. В узкой форме это свойство дает следующее допустимое правило в **LP** ([17, 19]):

если $\vdash F$, то $\vdash p:F$ для некоторого полинома доказательств p .

Это правило является переводом на язык явных доказательств обычного правила усиления для модальных логик

$$\frac{\vdash F}{\vdash \Box F}$$

Имеет место более общее *свойство интернализации выводов в LP*: если

$$A_1, \dots, A_n \vdash B,$$

то можно построить полином доказательств $t(x_1, \dots, x_n)$, зависящий от свежих переменных x_1, \dots, x_n такой, что

$$x_1:A_1, \dots, x_n:A_n \vdash t(x_1, \dots, x_n):B.$$

Можно отметить, что изоморфизм Карри-Ховарда покрывает лишь простой частный случай интернализации, когда A_1, A_2, \dots, A_n, B — это чисто

пропозициональные формулы, не содержащие доказуемых термов. Еще одно легкое наблюдение: комбинаторная логика $\mathbf{CL}_{\rightarrow}$ соответствует интуиционистскому импликативному фрагменту $A1 + R2$ логики доказательств.

Логика доказательств \mathbf{LP} оказывается в состоянии реализовать все выводимые в $\mathbf{S4}$ формулы путем восстановления соответствующих полиномов доказательств во всех вхождениях модальности. В компактной математической форме этот факт выражается теоремой о реализуемости ([17, 19]), которая показывает, что $\mathbf{S4}$ есть забывчивая проекция \mathbf{LP} . В частности, алгоритм из [17, 19] строит реализацию r , которая расставляет доказуемые полиномы во всех модальностях генценовского нормального вывода в $\mathbf{S4}$ формулы F и выдает формулу F^r , выводимую в \mathbf{LP} , причем

а) все отрицательные вхождения модальностей в F реализуются переменными;

б) все положительные вхождения модальностей в F реализуются полиномами доказательств, зависящими только от переменных из (а);

в) выбор констант по правилу $R2$ в выводе F^r в \mathbf{LP} осуществляется инъективно, т.е. каждая константа используется для обозначения вывода не более чем одной аксиомы.

Заметим, что полиномы доказательств полиморфны. Операция “+” приводит к тому, что данный доказуемый полином может иметь в \mathbf{LP} несколько различных типов. В самом деле, если $s:F$ и $t:G$, то как $(s + t):F$, так и $(s + t):G$ оба имеют место. С точки зрения доказуемой семантики полиморфизм означает, что полиномы доказательств представляют многозначные доказательства, т.е. такие, каждое из которых может доказывать сразу несколько теорем. Например, любая система доказуемости гильбертовского типа является многозначной, если принять, что данный вывод, как конечная последовательность формул, доказывает все формулы, встречающиеся в этой последовательности, а не только последнюю из них. Как отмечено в [19], системы с многозначными и с однозначными выводами легко взаимно моделируются. Из приведенных ниже результатов следует, что исчисление доказуемости Гёделя соответствует именно многозначным доказательствам. Логика однозначных доказательств была найдена в [58, 59]; она имеет важные приложения, хотя и не соответствует никакой нормальной модальной логике.

За точными определениями арифметической семантики полиномов доказательств и формул логики доказательств мы рекомендуем читателю обратиться к работе [19], которую также можно найти на странице

<http://www.cs.gc.cuny.edu/~sartemov>.

В данном обзоре мы ограничимся описанием того, как устроена эта семантика. В принципе, после нахождения \mathbf{LP} и теоремы о реализуемости $\mathbf{S4}$ в \mathbf{LP} , для завершения решения задачи Гёделя о доказуемом исчислении достаточно было указать на очевидную интерпретацию \mathbf{LP} через гёделевский предикат доказательств. В [17, 19] сделано больше. Там показано, что \mathbf{LP} не только корректна, но и полна относительно класса так называемых нормальных систем доказательств. Этот класс включает в себя естественные системы доказательств, рассматриваемые в литературе, такие как гё-

делевский предикат доказательств x есть гёделев номер вывода в **PA**, содержащего формулу с гёделевым номером y и его обобщения. *Нормальная система доказательств* – это доказуемо разрешимый многозначный предикат доказательств $Proof(x, y)$ в арифметике **PA** или в некоторой непротиворечивой теории, содержащей **PA**. Как предикат доказательств, $Proof(x, y)$ нумерует теоремы **PA**, т.е. $\mathbf{PA} \vdash \varphi$ тогда и только тогда, когда для некоторого n имеет место $Proof(n, [\varphi])$, где $[\varphi]$ обозначает гёделев номер формулы φ . Предполагается также выполнение двух естественных свойств предиката доказательств:

1. функция, ставящая в соответствие доказательству n множество теорем $T(n)$, доказанных этим доказательством, вычислима;
2. доказательства можно объединять: для любых k и l найдется n такой, что $T(k) \cup T(l) \subseteq T(n)$.

Для каждой нормальной системы доказательств можно определить вычислимые операции на доказательствах, соответствующие аппликации “.”, объединению “+” и проверке доказательств “!”. Арифметическая интерпретация $*$ – это выбор нормальной системы доказательств с вычислимыми операциями аппликации, объединения и проверки доказательств, а также интерпретация доказуемых переменных и констант натуральными числами (кодами выводов), а пропозициональных переменных – арифметическими предложениями. При данной интерпретации $*$ полином доказательств p становится конкретным натуральным числом p^* (кодом доказательства). Булевы связки понимаются одинаково в **LP** и в **PA**, формула $p:F$ интерпретируется как арифметическая формула $Proof(p^*, [F^*])$. Таким образом, **LP**-формула F при интерпретации $*$ становится арифметическим предложением F^* . Интерпретация $*$ называется *CS-интерпретацией*, если все формулы из CS истинны при данной $*$. В [19] установлена непустота множества CS -интерпретаций для любой спецификации констант CS .

Как доказано в [19] (Следствие 8.9), для каждой спецификации констант CS логика доказательств **LP** полна относительно доказуемой интерпретации, т.е. F выводится в **LP** с данной CS тогда и только тогда, когда F^* верна при любой CS -интерпретации $*$. Принимая во внимание соглашение об опускании тривиального упоминания о спецификации констант, теорему о полноте можно сформулировать в более компактном виде как *F выводится в **LP** тогда и только тогда, когда F^* верна при любой интерпретации $*$* .

В [20] замечено, что в известном смысле, набор операций на доказательствах для пропозиционального языка исчерпывается полиномами доказательств. Было показано, что каждая операция на доказательствах, которая инвариантна относительно выбора нормальной системы доказательств и которую можно специфицировать на пропозициональном языке, реализуется некоторым полиномом доказательств.

В свете принятых выше допущений, логика доказательств **LP** дает решение задачи Гёделя о доказуемом исчислении. В совокупности с приведенными выше результатами Гёделя, МакКинси-Тарского, **LP** может рас-

сма­тривать­ся как фор­ма­ли­за­ция клас­си­че­ской семан­ти­ки *ВНК* для ин­ту­и­ци­о­ни­ст­ской ло­ги­ки вы­ска­зы­ва­ний, что да­ет ре­ше­ние во­про­са, ко­то­рым за­ни­ма­лись Кол­мо­го­ров и Гё­дель. Ло­ги­ка до­ка­за­тель­ств **LP** мо­жет так­же рас­сма­тривать­ся как еди­ный ло­ги­че­ский ап­па­рат, име­ю­ще­го де­ло с объ­ек­та­ми двух ти­пов - вы­ска­зы­ва­ни­я­ми и до­ка­за­тель­ства­ми (ре­ше­ни­я­ми за­дач), ап­па­рат, о ко­то­ром пи­сал Кол­мо­го­ров в 1985 го­ду ([7]).

В све­те это­го про­дви­же­ния, кар­ти­на в ос­но­ва­ни­ях ин­ту­и­ци­о­ни­ст­ской ло­ги­ки те­перь вы­гля­дит так:

$$\mathbf{Int} \leftrightarrow \mathbf{S4} \leftrightarrow \mathbf{LP} \leftrightarrow \text{КЛАС­СИ­ЧЕ­СКИЕ ДО­КА­ЗА­ТЕЛЬ­СТВА},$$

где все вло­же­ния точ­ные.

Почему, не­смот­ря на по­сто­янный ин­те­рес к этой те­ме, за­да­ча по­стро­е­ния ма­те­ма­ти­че­ской мо­де­ли из­на­чаль­ной семан­ти­ки до­ка­зу­е­мо­сти для ин­ту­и­ци­о­ни­ст­ской и мо­да­ль­ной ло­ги­ки не под­да­ва­лась ре­ше­нию в те­че­нии мно­гих лет? Мож­но упо­мя­нуть не­ко­то­рые труд­но­сти, ко­то­рые при­шлось пре­одо­леть на пу­ти к ре­ше­нию.

1. По­иск пра­виль­но­го фор­ма­та для до­ка­зу­е­мо­ст­ной мо­да­ль­ной ло­ги­ки **S4** ока­зал­ся не­просто­ым и дол­гим. Ра­бо­та Гё­де­ля 1938 го­да, где он пред­ло­жил этот фор­ма­т, не бы­ла опу­бли­ко­ва­на до фак­ти­че­ско­го ре­ше­ния за­да­чи и, тем са­мым, не мо­гла ус­ко­рить про­цесс по­ис­ка. Ре­ше­ние же за­да­чи толь­ко в рам­ках мо­да­ль­но­го язы­ка ока­за­лось не­воз­мож­ным, что и бы­ло за­ме­че­но Мон­те­гю в 1963 го­ду ([67]).

2. Тех­ни­че­ская сто­ро­на де­ла так­же ока­за­лась да­леко не­просто­й. Мно­гие стере­о­ти­пы род­ствен­ных об­ла­стей, та­ких как λ -ис­чис­ле­ние или ком­би­на­тор­ная ло­ги­ка, дол­жны бы­ли бы­ть пе­ре­смот­ре­ны. Пе­ре­ход от кван­то­ров по до­ка­за­тель­ствам к пред­став­ля­ю­щим их функ­ци­ям “по Ско­ле­му” при­во­дит к яв­ле­нию са­мос­сы­лоч­но­сти. На­до бы­ло по­нять, как ра­бо­тать с вы­ра­же­ни­я­ми ти­па $t:F(t)$, где до­ка­зу­е­мо­ст­ный терм мо­жет вхо­дить в фор­му­лу, им же и до­ка­зы­ва­е­мую. Это по­тре­бо­ва­ло спе­ци­аль­но­го опы­та ра­бо­ты с са­мос­сы­лоч­но­стью, ко­то­рый в дан­ном слу­чае бы­л на­коп­лен в те­че­нии 20 лет ис­сле­до­ва­ний по мо­да­ль­ной ло­ги­ке до­ка­зу­е­мо­сти Гё­де­ля-Лё­ба, где мо­да­ль­ность $\Box F$ ин­тер­пре­ти­ру­ет­ся как *Provable(F)* (Р. Со­ло­вей, Дж. Бу­лос, Д. де Йонг, Р. Ма­га­ри, Дж. Сам­бин, Ф. Мон­тан­ья, А. Вис­сер, Л. Бек­ле­ми­шев, В. Шав­ру­ков, ав­тор, и мно­гие дру­гие [32, 33, 51, 79, 80]).

4 Две мо­де­ли до­ка­зу­е­мо­сти

Ра­бо­та Гё­де­ля 1933 го­да [45] о ло­ги­ке до­ка­зу­е­мо­сти оста­ви­ла от­кры­ты­ми два во­про­са

(А) О точ­ной до­ка­зу­е­мо­ст­ной семан­ти­ке для мо­да­ль­ной ло­ги­ки **S4**, ко­то­рая ока­за­лась “ис­чис­ле­ни­ем до­ка­зу­е­мо­сти без до­ка­зу­е­мо­ст­ной семан­ти­ки”.

(Б) О мо­да­ль­ной ло­ги­ке гё­де­ле­вско­го пре­ди­ка­та фор­маль­ной до­ка­зу­е­мо­сти, ко­то­рый ока­зал­ся “до­ка­зу­е­мо­ст­ной семан­ти­кой без ис­чис­ле­ния”.

Во­про­с (Б) бы­л ре­шен в 1976 Р. Со­ло­ве­ем, ко­то­рый по­ка­зал, что мо­да­ль­ная ло­ги­ка **GL** (из­вест­ная так­же под име­на­ми **G**, **L**, **K4.W**, **PRL**)

аксиоматизирует все пропозициональные свойства предиката доказуемости $Provable(F)$ ([32, 33, 51, 79, 80]). Логика доказуемости **GL** формулируется следующим образом.

1. *Аксиомы и правила классической логики высказываний*
2. $\Box(F \rightarrow G) \rightarrow (\Box F \rightarrow \Box G)$ (неявная аппликация)
3. $\Box(\Box F \rightarrow F) \rightarrow \Box F$ (аксиома Лёба)
4. $\Box F \rightarrow \Box \Box F$ (неявная проверка доказательств)
5. *Правило неявной интернализации доказательств:*

$$\frac{\vdash F}{\vdash \Box F}$$

В логике **GL** естественно формализуются вторая теорема Гёделя о неполноте $\neg \Box(\neg \Box \perp)$, теорема Лёба $\Box(\Box F \rightarrow F) \rightarrow \Box F$, ряд других содержательных метаматематических принципов. Эта логика разрешима, обладает соответствующей семантикой Крипке, генценовской системой с устранением сечений и находит применения в теории доказательств (см, например, [30, 51]).

Решение вопроса (А) было получено через **S4** и **LP** (см. выше).

Выразительные возможности моделей (А) и (Б) существенно различны. **LP** содержит типовое λ -исчисление, модальную логику и модальное λ -исчисление ([2, 21]). Более того, модель **S4/LP** дает единый подход к ряду задач из таких областей как представление знаний, типовые функциональные языки и теории, оказывается полезной для анализа систем формализации и проверки доказательств (см. главу 5 ниже). С другой стороны, модель (А) не способна выразить теорему Гёделя о неполноте.

Модели доказуемости (А) и (Б) дополняют друг друга, вместе покрывая большинство приложений, множества которых для моделей (А) и (Б) практически не пересекаются.

Полиномы доказательств и **LP** предложили первую точную *экзистенциальную семантику модальной логики*. Первоначальное гёделевское прочтение модальности $\Box F$ было доказуемым, а именно,

существует доказательство (свидетельство, обоснование) для F.

Таким образом, модальность по Гёделю содержала неформальный квантор существования, пробегающий по доказательствам. Подобное прочтение модальности является типичным для “наивной” семантики широкого круга эпистемических логик и логик доказуемости. Однако, до появления логики доказательств **LP** основные модальные логики оставались без математической семантики экзистенциального характера. Исключением, подтверждающим правило, является модель арифметической доказуемости для системы **GL** из [32, 33, 51, 79, 80], которая, однако, не распространяется на основные модальные логики **S4** и **S5**.

Спустя почти 30 лет после первоначальных работ Гёделя была открыта иная по своей природе семантика Крипке для модальной логики. В этой

семантике модальность носит характер квантора всеобщности: $\Box F$ читается как

для всех возможных ситуаций имеет место F .

Мы будем называть подобные семантики *семантиками всеобщности*. Такое прочтение модальности естественно появляется в динамических и временных логиках, описывающих вычислительные процессы, множества состояний которых, в норме, образуют структуру Крипке, возможно ветвящуюся.

При всей своей естественности и простоте в обращении, семантика всеобщности не является единственным выбором средства решения конкретных задач, в которых участвуют модальные языки. К примеру, семантика всеобщности не привела к решению задачи Гёделя о доказуемости исчисления, которая носит ярко выраженный экзистенциальный характер.

Перспективной областью приложений логики доказательств является область логик знаний, где проблема построения систем с явными терминами для обоснований истинности дискутируется уже давно ([31]). **LP** подсказывает подход к проблеме *логического всезнания* (Logical Omniscience Problem, [70, 71, 72]). *Логическое всезнание* означает нереалистическое допущение о том, что интеллектуальный агент знает все логические следствия своих данных. Вот пример, заимствованный из доклада Дж. Халперна (Корнелльский Университет).

“Допустим некто знает произведение двух (очень больших) простых чисел. В каком смысле он/она знает каждое из этих чисел, если разложение на множители может потребовать миллиарды лет вычислений?”

Как справедливо отмечает М. Фиттинг [42], традиционная модальная логика есть скорее логика *потенциального знания*; адекватным эпистемическим прочтением формулы $\Box F$ является “ F можно узнать в принципе”, а не “ F известно”.

Проблема логического всезнания состоит в создании механизма различающего в логике знаний “легко добываемые” и “трудно добываемые” факты. Язык логики доказательств **LP** с его формулами, несущими доказательства, говорит о явно полученном знании. Размер полинома доказательств (возможно, в более богатом базисе, отражающем специфику задачи) несет информацию об объеме работы, проделанной при получении данного знания.

Еще одним перспективным направлением приложения логики доказательств является область типовых теорий и языков программирования. Обычное типовое λ -исчисление (и эквивалентная ей типовая комбинаторная логика) явилось теоретическим прототипом целого класса языков программирования (см., например, [37]). Логика доказательств и построенные на ее основе рефлексивное λ -исчисление и рефлексивная комбинаторная логика (см. 5.8 и 5.9) имеют гораздо большие выразительные возможности, в частности, более богатую систему типов, способов их образования и использования. Естественно ожидать, что эти новые возможности найдут применение

в языках программирования подобно тому, как нашли применение прежние основные теоретические разработки в области λ -исчислений.

Во многих отношениях логика доказательств отличается от типовой комбинаторной логики $\mathbf{CL}_{\rightarrow}$ и типового λ -исчисления.

1. Язык логики доказательств допускает свободное перемешивание формул разной глубины интернализации: $t:F \rightarrow F$ (глубина $n + 1$ и n), $t:F \rightarrow !t:(t:F)$ (глубина $n + 1$ и $n + 2$), и т.д. Заметим, что обычная комбинаторная логика и λ -исчисление оперируют только с выражениями глубины 1.

2. Полиномы доказательств имеют самоссылочный характер. К примеру, формула $x:(x:F)$ является правильно построенной и поддерживается существующей семантикой арифметической доказуемости для логики доказательств.

5 Дальнейшее развитие

Эта секция является главной в данном обзоре. В ней рассказывается о работах, сделанных в этой области после 1995 года.

5.1. Модели логики доказательств. Как уже было отмечено выше, логика доказательств обладает свойством полноты относительно естественной доказуемостной семантики. Однако, для успешного изучения \mathbf{LP} и приложений важно иметь также и набор удобных искусственных моделей \mathbf{LP} .

Первые искусственные модели для \mathbf{LP} были построены А.Мкртычевым в [66]. Фиксируем множество спецификаций доказуемостных констант $\mathcal{CS} = \{c_1:A_1, c_2:A_2, \dots\}$, где каждая из c_i это доказуемостная константа, а каждая из A_i это аксиома \mathbf{LP} . Модель Мкртычева (M -модель, в [66] эти структуры названы *пре-моделями*) для \mathbf{LP} , соответствующая данной спецификации констант \mathcal{CS} , представляет собой пару отображений $(*, \Vdash)$. Здесь $*$ – есть *свидетельская функция*, ставящая в соответствие полиному доказательств t множество формул $*(t)$, про которые говорят, что t является их “приемлемым свидетелем”. В свою очередь, \Vdash есть истинностная функция на формулах. Свидетельская функция согласована с данной спецификацией констант \mathcal{CS} , т.е. $c:A \in \mathcal{CS}$ влечет $A \in *(c)$. Кроме того, $*$ согласована с операциями \mathbf{LP} , т.е.

$$\text{если } (F \rightarrow G) \in *(s) \text{ и } F \in *(t), \text{ то } G \in *(s \cdot t),$$

$$\text{если } F \in *(t), \text{ то } t:F \in *(!t),$$

$$*(s) \cup *(t) \subseteq *(s + t).$$

Вынуждение \Vdash задается (произвольным) распределением истинности пропозициональных букв и распространяется на все \mathbf{LP} -формулы индуктивно по булевым законам для логических связей и на модализованных формулах согласно условию

$$\Vdash t:F \Leftrightarrow F \in *(t) \text{ and } \Vdash F.$$

Как видно из определения, истинность $t:F$ означает что t есть допустимый свидетель для F и F истинна. В принципе, по данной M -модели путем специального ограничения свидетельской функции $*$ можно построить эквивалентную ей модель где истинность формул вида $t:F$ определяется уже только свидетельской функцией:

$$\Vdash t:F \Leftrightarrow F \in *(t).$$

В [66] установлена корректность и полнота **LP** относительно M -моделей, последняя с помощью классической конструкции максимального непротиворечивого множества формул.

M -модели оказались удобным аппаратом исследования логики доказательств. Так, с их помощью в [66] была впервые установлена разрешимость **LP**.

Р. Кузнец в [61] получил верхнюю оценку Σ_2^P сложности проблемы выполнимости **LP**-формул в M -моделях, что оказалось ниже известной верхней оценки *PSPACE* сложности проблемы выполнимости в **S4**. Возможным объяснением этого выигрыша в сложности **LP** по сравнению с родственной ей **S4** является то, что проверка выполнимости в **LP** это, в основном, проверка типизации, т.е. правильности приписывания типов (формул) термам (доказательствам), которая в классических случаях имеет относительно невысокую сложность.

Дальнейшее развитие M -модели получили в работе Н. Крупского [57], где построена минимальная модель **LP**, которая в точности соответствует выводимости в **LP** “модализированных” формул (т.е. формул вида $t:F$):

$$\Vdash t:F \Leftrightarrow \mathbf{LP} \vdash t:F.$$

На этой основе в [57] дана улучшенная верхняя оценка (*NP*) разрешимости “модализированного” фрагмента логики доказательств. В [57] минимальная модель также применена для решения известного вопроса о дизъюнктивном свойстве в логике доказательств:

$$\mathbf{LP} \vdash s:F \vee t:G \Leftrightarrow \mathbf{LP} \vdash s:F \text{ или } \mathbf{LP} \vdash t:G.$$

М. Фиттинг в [41, 42] дал описание канонической модели для **LP** как модели Крипке. Каноническая модель – это класс всех максимальных непротиворечивых множеств со структурой Крипке на нем. Отношение достижимости R определяется как:

$$\Gamma R \Delta \Leftrightarrow \{F \mid t:F \in \Gamma, \text{ для некоторого } t\} \subseteq \Delta.$$

Свидетельская функция $*(\Gamma, t)$ и вынуждение \Vdash на атомарных формулах определяются канонически через принадлежность к Γ :

$$\begin{aligned} *(\Gamma, t) &= \{F \mid t:F \in \Gamma\}, \\ \Gamma \Vdash P &\text{ тогда и только тогда, когда } P \in \Gamma. \end{aligned}$$

Отношение вынуждения естественным образом обобщается до следующего:

$$\Gamma \Vdash t:F \Leftrightarrow F \in *(\Gamma, t) \text{ и } \text{“} \Delta \Vdash F \text{ для каждого } \Delta \text{ такого, что } \Gamma R \Delta \text{”}.$$

Нетрудно видеть, что каждый узел канонической модели Фиттинга является M -моделью.

В [42] установлено, что введенная таким образом структура Крипке является точной моделью \mathbf{LP} для данной спецификации констант:

$$\mathbf{LP} \vdash F \Leftrightarrow F \text{ выполнена в каждом } \Gamma.$$

Фиттинг в [42] установил фундаментальное свойство **полной объяснимости** канонической модели \mathbf{LP} : *если F верна во всех мирах достижимых из Γ , то $t:F$ верна в Γ для некоторого полинома t .*

Неожиданное и остроумное применение канонической модели найдено в [41], где предложено альтернативное “семантическое” доказательство теоремы о реализуемости $\mathbf{S4}$ в \mathbf{LP} , а также прояснена роль операции “+” в этой реализуемости.

В [42] также дано и общее определение модели типа Крипке для \mathbf{LP} . Модель Фиттинга (называемая здесь F -моделью), это четверка $(W, R, *, \Vdash)$, где

(W, R) есть рефлексивная и транзитивная шкала Крипке;

$*(u, t)$ есть свидетельская функция, указывающая в каждом мире $u \in W$ для доказуемого полинома t множество формул, для которых t мог бы быть приемлемым свидетелем;

\Vdash есть отношение вынуждения \mathbf{LP} -формул в мирах из W .

Свойства свидетельской функции и вынуждения естественно считаются с канонической модели для \mathbf{LP} , включая ключевой пункт определения вынуждения модализованной формулы:

$$u \Vdash t:F \Leftrightarrow F \in *(u, t) \text{ и } \text{“} v \Vdash F \text{ для каждого } v \in W \text{ такого, что } uRv \text{”},$$

и свойство полной объяснимости. Свойства канонической модели немедленно влекут полноту \mathbf{LP} относительно класса всех F -моделей.

Как заметил В. Крупский, несложное применение конструкции Хенкина позволяет установить полноту \mathbf{LP} также и относительно M -моделей со свойством полной определимости. Таким образом, свойство полноты для F -моделей достигается уже на одноэлементных F -моделях (т.е. M -моделях со свойством полной определимости). Совместная ответственность вынуждения и свидетельской функции за принятие решения об истинности формул в F -моделях оставляет возможность игнорировать вынуждение и сводит F -модели к M -моделям в вопросе полноты \mathbf{LP} . Несмотря на это, модели Фиттинга дают более широкую и гибкую семантику для логики доказательств. Естественно ожидать, что модели Фиттинга также найдут применение в эпистемических логиках содержащих как доказуемые полиномы, так и обычную модальность, т.к. в таких логиках отношение вынуждения не вырождается.

Система табличного вывода для логики доказательств была построена Б. Ренне в [73], с установлением теоремы о полноте относительно M -моделей и доказательством устранимости сечения в \mathbf{LP} . Заметим, что устранение сечения в \mathbf{LP} с пустой спецификацией констант было доказано в [19].

5.2. Интерполяция в логике доказательств. Вопрос об интерполяции в логиках доказательств рассмотрен Татьяной Сидон (Яворской) в [12]. Обычная формулировка интерполяционного свойства Крейга для данного логико-математического исчисления I гласит, что коль скоро $I \vdash A \rightarrow B$, то можно найти формулу C (интерполянт A и B) в *пересечении языков* формул A и B такую, что $I \vdash A \rightarrow C$ и $I \vdash C \rightarrow B$. В случае \mathbf{LP} можно говорить о двух типах интерполяции: *слабой*, когда лишь пропозициональные переменные C обязаны быть общими для A и B , и *сильной*, когда как пропозициональные так и доказуемые переменные C обязаны быть общими для A и B . Как было показано в [12], фрагмент \mathbf{LP} без функциональных символов (известный также как \mathcal{P} , \mathbf{BLP}) обладает сильным интерполяционным свойством. В логике \mathbf{LP} выводы с пустой спецификацией констант CS обладают слабым (но не сильным) интерполяционным свойством. Если CS непусто, то даже слабое интерполяционное свойство может нарушаться.

5.3. Объединенная логика доказательств и доказуемости \mathbf{LPP} .

Две логические системы, описывающие доказуемость: эксплицитная $\mathbf{S4/LP}$ и имплицитная \mathbf{GL} математически основаны на одном и том же классе гёделевских предикатов доказательств $Proof(x,y)$. Естественно, что эти модели оказались совместными и на логическом уровне. Совместная логика доказательств и доказуемости \mathbf{LPP} была успешно аксиоматизирована Татьяной Яворской-Сидон в [77, 78].

Язык логики доказательств и доказуемости \mathbf{LPP} (также известной под именем $\mathbf{GL+LP}$) является расширением языка \mathbf{LP} посредством добавления модальности \Box и двух новых одноместных функциональных символов \Downarrow_{\Box} и \Uparrow_{\Box} . Аксиомы логики \mathbf{LPP} естественно разбиваются на две группы. Первая группа *Общие принципы* описывает взаимоотношения между предикатами доказуемости и доказательств. Вторая группа *Определение операций* содержит аксиомы, специфицирующие операции на доказательствах.

Система \mathbf{LPP}_{\emptyset} .

Аксиомы: I. *Общие принципы* II. *Определение операций*

- | | |
|--|---|
| 1. аксиомы \mathbf{GL} | 5. аксиомы \mathbf{LP} |
| 2. $t:A \rightarrow A$ | 6. $t:\Box A \rightarrow (\Downarrow_{\Box} t):A$ |
| 3. $t:A \rightarrow \Box(t:A)$ | 7. $t:A \rightarrow (\Uparrow_{\Box} t):\Box A$ |
| 4. $\neg(t:A) \rightarrow \Box\neg(t:A)$ | |

Правила: *modus ponens* и два модальных правила

$$\frac{A}{\Box A} \qquad \frac{\Box A}{A}$$

Система **LPP** есть замыкание **LPP**₀ по правилу *введения констант*:

sA, где *s* есть доказуемая константа, *A* это любая из аксиом 1.–7.

Основные результаты, касающиеся **LPP** были получены в [77, 78]: разрешимость, корректность и полнота относительно семантики арифметической доказуемости, при которой $t : F$ интерпретируется как предикат доказательств $Proof(t, F)$, а $\Box F$ как предикат доказуемости $\exists x Proof(x, F)$.

5.4. Логика однозначных доказательств FLP. Как было отмечено в секции 4, в решении проблемы Гёделя был использован класс многозначных доказательств. Нетрудно видеть, что многозначность доказательств является необходимым атрибутом модального описания доказуемости. Для *однозначных* доказательств, каждое из которых, по определению, доказывает только одну формулу, есть тождества, несовместимые с нормальной модальной логикой. Например, принцип $t : F \rightarrow \neg t : (F \wedge F)$ верен для однозначных доказательств. Однако, его "забывчивая проекция" приводит к формуле $\Box F \rightarrow \neg \Box (F \wedge F)$, очевидно неверной в модальной логике.

Задача нахождения логики однозначных доказательств представляла большой интерес по многим причинам: однозначные доказательства более привычны логикам, такие аналоги доказательств как типовые λ -термы и комбинаторные термы, ссылки в базах данных, соответствуют однозначным доказательствам. Первые шаги построения логики однозначных доказательств были сделаны в [16, 26]. Полное решение было найдено В. Крупским в его системе **FLP** ([58, 59]), и развито им же в системе **FLP**_{ref} ([60]).

В логике однозначных доказательств формула $t : F$ по-прежнему понимается как "*t* есть доказательство формулы *F*", но класс допустимых интерпретаций ограничивается однозначными системами доказательств. Математически задача состояла в построении полной аксиоматики для всех возникающих при этом тавтологий в языке **LP** (без операции "+", которая несовместима с однозначными системами доказательств), установлении разрешимости, нахождении моделей.

Первой задачей на пути к построению искомой полной системы стало нахождение пропозиционального аналога свойства однозначности доказательств: если $p:F \wedge p:G$, то *F* и *G* совпадают синтаксически. Оказалось, что искомое свойство можно адекватно выразить с помощью т.н. условной унификации. Это было установлено в [26] для **LP**-языка без функциональных символов, а затем распространено в [58, 59, 60] на более богатые языки.

Каждая формула *C* вида $t_1:F_1 \wedge \dots \wedge t_n:F_n$ порождает множество квазиуравнений вида $S := \{t_i = t_j \Rightarrow F_i = F_j \mid 1 \leq i, j \leq n\}$. Унификатор σ системы *S* это подстановка σ такая, что $t_i\sigma \neq t_j\sigma$ или $F_i\sigma \equiv F_j\sigma$ имеет место при каждом *i, j*. Здесь и ниже " $X \equiv Y$ " означает синтаксическое совпадение *X* и *Y*.

Определение условной унификации. $A = B \text{ (mod } S)$ означает, что для каждого унификатора σ системы *S* имеет место $A\sigma \equiv B\sigma$.

Разрешимость условной унификации. $A = B \text{ (mod } S)$ разрешимо как отношение между *A, B, S*.

Аксиома унификации: Для каждого условия C вида $t_1:F_1 \wedge \dots \wedge t_n:F_n$ если $A = B \pmod{S_C}$, то $t_1:F_1 \wedge \dots \wedge t_n:F_n \rightarrow (A \leftrightarrow B)$.

Логика **FLP** однозначных доказательств была введена в [58]. Язык **FLP** это язык **LP** без операции “+” и доказуемых констант. Аксиомы и правила **FLP**

A0. Аксиомы и правила классической логики высказываний

A1. $t:(F \rightarrow G) \rightarrow (s:F \rightarrow (t \cdot s):G)$

A2. $t:F \rightarrow F$

A3. $t:F \rightarrow \neg t:t:F$

A4. Аксиома унификации.

Теорема ([58, 59]): *Логика **FLP** разрешима, корректна и полна по отношению к арифметической доказуемой интерпретации, основанной на однозначных предикатах доказательств.*

Дальнейшее развитие логика однозначных доказательств получила в [60], где построена логика доказательств со ссылками **FLP**_{ref}. Система **FLP**_{ref} расширяет **FLP** переменными второго порядка, обозначающими конструкцию восстановления объекта по ссылке на него, например, вычисление формулы, доказанной данным выводом. **FLP**_{ref} может рассматриваться как естественная формальная система для допустимых правил вывода в арифметике.

В связи с приложениями также следует отметить совместную работу В. Крупского и автора [23], где на основе логики доказательств была построена логическая система описания и синтеза ссылочных баз данных.

5.5. Полиномы доказуемости для других модальных логик. Задаче нахождения реализующей системы доказуемых термов для модальной логики **S5**=**S4**+($\neg \Box F \rightarrow \Box \neg \Box F$) посвящена работа Казакова, Шапиро и автора [22]. Система **S5** важна в связи с приложениями в логиках знаний. Отличием этого случая от **S4** является присутствие в **S5** отрицательной информации о доказательствах. В [22] рассмотрена возможная система доказуемых термов для **S5**, установлена реализуемость логики **S5** данными доказуемыми термами, разрешимость и полнота возникающей при этом логики доказательств. Наличие и других естественных систем доказуемых термов для **S5** говорит о том, что проблема представления отрицательных знаний посредством операций над свидетельствами далеко не исчерпана.

Полиномы доказательств, соответствующие известным модальным логикам **K**, **K4**, **D**, **D4**, **T** были описаны В. Брежневым в [34, 35]. Работа [35] интересна еще и тем, что в ней построены полиномы доказательств для генценовских систем вывода.

5.6. Логика доказательств с кванторами. Арифметическая доказуемая семантика логики доказательств естественно расширяется на язык первого порядка, а также на язык **LP** с кванторами по доказательствам. Обе эти возможности усиления выразительной силы **LP** были иссле-

дованы. Методами, восходящими к работам [1, 3], в [24] было установлено, что множество тавтологий в языке логики доказательств первого порядка не является рекурсивно перечислимым. Этот отрицательный результат показывает невозможность построения полной системы аксиом для логики доказательств первого порядка.

Пропозициональная логика с кванторами по доказательствам изучалась в [87]. В этой работе Р. Яворский установил, что совокупность соответствующих формул истинных при естественной доказуемой интерпретации не является рекурсивно перечислимой, следовательно, пропозициональная логика с кванторами по доказательствам не аксиоматизируема.

5.7. Логика стандартного предиката доказуемости. Логика доказательств аксиоматизирует все свойства высказываний и доказательств выразимых в пропозициональном языке и инвариантных относительно выбора системы доказательств. Для конкретных систем доказательств могут существовать и другие истинные в них пропозициональные тождества. Например, стандартный предикат доказуемости “из учебника” основан на гёделевской нумерации синтаксиса, которая обладает свойством монотонности номеров. В частности, номер данного доказательства (конечной последовательности формул) строго больше номеров входящих в это доказательство формул, в частности, каждой доказанной данной последовательностью теоремы. На основании этого наблюдения можно указать серию тождеств (введенную в [27] и названное там *аксиомой монотонности*), истинных для стандартного предиката доказуемости, но не доказуемых в **LP**:

$$\neg(t_1:A_2(t_2) \wedge t_2:A_3(t_3) \dots \wedge t_n:A_1(t_1)),$$

где t_i явно входит в $A_i(t_i)$. Как показано в [27], базовая логика доказательств с аксиомой монотонности (система \mathcal{M}) полна относительно стандартного предиката доказуемости. В [16] этот результат о полноте перенесен на систему в более богатом языке содержащую как \mathcal{M} , так и логику доказуемости **GL**. Интересные результаты о полноте по отношению к стандартному предикату доказуемости получены в [86] для некоторого фрагмента логики доказательств первого порядка.

5.8. Рефлексия в λ -исчислениях Логика доказательств естественно объединила две области: эпистемическую, представленную модальной логикой, и вычислительную, представленную типовыми λ -исчислениями и комбинаторной логикой. **LP** может рассматриваться и как реализованная модальная логика **S4** и как типовая комбинаторная логика с дополнительными выразительными возможностями ([21]). При этом напрашивается аналогия с изоморфизмом Карри-Ховарда, выражающим тождественность интуиционистских доказательств и типовых λ -термов, рассматриваемых как вычислительные программы. Этой аналогии может быть предана точная математическая форма, как это сделано, например, в работе [14], где введено рефлексивное λ -исчисление λ^∞ .

По причинам компактности изложения и близости его к объекту изучения — модальной логике **S4**, каноническая формулировка логики дока-

зательств \mathbf{LP} была выбрана скорее в стиле типовой комбинаторной логики $\mathbf{CL}_{\rightarrow}$, нежели в более распространенном формате λ -исчисления. Разумеется, в \mathbf{LP} можно эмулировать оператор λ -абстракции ([19]), например, в стиле Карри, как это обычно делается в комбинаторной логике $\mathbf{CL}_{\rightarrow}$ (см., например, [83], с.17). Однако, задача перевода \mathbf{LP} и ее фрагментов в формат λ -термов очень важна. Мотивировкой такого сорта исследований является построение нового поколения λ -исчислений, гораздо более выразительных, чем их предшественники. Ввиду того, что λ -исчисления являются прототипом определенного класса языков программирования, прогресс в этом направлении представляет значительный дополнительный интерес.

Логика доказательств \mathbf{LP} обладает рядом черт, не типичных для λ -исчислений: полиморфизм, самоссылочные возможности, классическая логика в основаниях, способность интернализировать свои собственные выводы, и т.п.. Для сохранения надежды на такое фундаментальное свойство как нормализуемость термов, следует отказаться от их полиморфизма и согласиться с тем, что каждый терм имеет единственный тип. Это делает невозможной самоссылочность в языке λ -термов: в терме $x : A(x)$ типы внешнего и внутренних вхождений переменной x синтаксически различны. Напомним, что в \mathbf{LP} формулы вида $x : x : F$ являются вполне законными образованиями и поддерживаются стандартной доказуемостной семантикой. Как было показано в [14], свойство интернализации может быть перенесено в формат λ -исчисления.

Мы строим λ -исчисление на основе импликативной интуиционистской (минимальной) логики в качестве исчисления типов. Система λ^{∞} из [14] содержит в качестве атомов обычные пропозициональные переменные (атомарные типы), равно как и утверждения сорта $t : F$, где t терм и F тип. Соответствие “терм:тип” жестко фиксированно “по Чёрчу”. Система λ^{∞} построена на следующих принципах:

1. λ^{∞} содержит систему натурального вывода для импликативной интуиционистской логики.
2. В λ^{∞} постулирован принцип $x:A \vdash A$.
3. В λ^{∞} имеет место правило интернализации: *если $A_1, \dots, A_n \vdash B$, то для любых свежих переменных x_1, \dots, x_n соответствующих типов можно построить λ -term $t(x_1, \dots, x_n)$ такой, что*

$$x_1:A_1, \dots, x_n:A_n \vdash t(x_1, \dots, x_n):B.$$

За полным определением системы λ^{∞} мы отсылаем читателя к работе [14].

Выбранная в [14] формулировка λ^{∞} постулирует несколько счетных серий термообразующих операций. Допустимость правила интернализации в λ^{∞} доказывается в качестве метатеоремы. Представляется интересным построить формулировку λ^{∞} , где правило интернализации постулируется, наряду с 1 и 2 выше, после чего все конкретные операции становятся его частными случаями.

Назовем уровнем λ^{∞} -формулы F максимальную глубину операции типового приписывания в F . Нетрудно заметить, что изоморфизм Карри-

Ховарда соответствует в λ^∞ интернализации на уровне 0, что дает некоторое представление о новых выразительных возможностях системы λ^∞ .

Выбор системы редукций, существование и единственность нормальных форм в λ^∞ оказываются связанными с вопросом о глубине сохранения типов при редукциях, который не возникает в обычном λ -исчислении. Соответствующая теория находится в стадии разработки.

5.9. Рефлексивная комбинаторная логика. Системы комбинаторной логики обычно имеют более компактную формулировку, чем соответствующие λ -исчисления. Рефлексивное λ -исчисление не стало исключением.

Ниже сформулирована рефлексивная комбинаторная логика \mathbf{RCL}_\rightarrow , построенная на основе гильбертовского исчисления для импликативной интуиционистской логики с жесткой типизацией термов. Термы в \mathbf{RCL}_\rightarrow строятся из переменных и констант строго определенных типов.

Язык \mathbf{RCL}_\rightarrow , правильно построенные формулы и выводимые формулы определяются совместной индукцией.

1. Язык \mathbf{RCL}_\rightarrow содержит пропозициональные переменные p_0, p_1, \dots и пропозициональную связку “ \rightarrow ”. Каждая пропозициональная переменная есть (атомарная) формула.
2. Если S и T формулы, то $S \rightarrow T$ — также формула.
3. Для каждой формулы F фиксируется свой набор доказуемых переменных x_0, x_1, \dots . Если x это переменная типа F , то $x:F$ есть формула. Здесь и ниже утверждения “ $t:F$ есть формула” и “ t есть терм типа F ” используются как синонимы.
4. Каждая аксиома А1-А6 является формулой.

А1. Для каждой формулы A и $t:A$ есть аксиома

$$t:A \rightarrow A.$$

А2. Для каждой формулы $A \rightarrow (B \rightarrow A)$ фиксируется константа \mathbf{k} и аксиома

$$\mathbf{k}:(A \rightarrow (B \rightarrow A)).$$

А3. Для каждой формулы $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$ фиксируется константа \mathbf{s} и аксиома

$$\mathbf{s}:[(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))].$$

А4. Для каждой формулы $t:A \rightarrow A$ фиксируется константа \mathbf{d} и аксиома

$$\mathbf{d}:(t:A \rightarrow A).$$

А5. Если $A, B, u:(A \rightarrow B), v:A$ формулы, то $(u \cdot v):B$ также формула, причем для формулы $u:(A \rightarrow B) \rightarrow (v:A \rightarrow (u \cdot v):B)$ фиксируется константа \mathbf{o} и аксиома

$$\mathbf{o}:[u:(A \rightarrow B) \rightarrow (v:A \rightarrow (u \cdot v):B)].$$

А6. Если A и $t:A$ формулы, то $!t:t:A$ также формула, причем для формулы $t:A \rightarrow !t:t:A$ фиксируется константа \mathbf{c} и аксиома

$$\mathbf{c}:(t:A \rightarrow !t:t:A).$$

5. Каждая доказуемая из гипотез формула есть правильно построенная формула. *Гипотезы* — это произвольное конечное мультимножество Γ формул. Вывод из гипотез Γ есть конечная последовательность формул, каждая из которых есть либо гипотеза из Γ , либо аксиома, либо следует из предшествующих в данной последовательности по правилу *modus ponens*:

$$\frac{A \rightarrow B, \quad A}{B}$$

Выражение $\Gamma \vdash F$ означает, что существует вывод из Γ , содержащий F .

Очевидной семантикой $\mathbf{RCL}_{\rightarrow}$ является доказуемость, унаследованная от \mathbf{LP} . Комбинаторные термы понимаются как доказательства, например, в \mathbf{PA} или в интуиционистской арифметике \mathbf{HA} . Формулы $t:F$ интерпретируются как арифметические утверждения о доказуемости $Proof(t, F)$, комбинаторы $\mathbf{k, s, d, o, c}$ обозначают термы, соответствующие доказательствам арифметических переводов аксиом из А2-А6.

Терминология формул в $\mathbf{RCL}_{\rightarrow}$ может быть переведена на обычный типовой язык. При этом правильно построенные формулы становятся *типами*, объекты t в формулах $t:F$ — *комбинаторными термами типа F*, константы — *константными комбинаторами* данного типа, гипотезы — *контекстом*, выводимые из Γ формулы — *непустыми типами в контексте* Γ , и т.д.

Нетрудно видеть, что $\mathbf{RCL}_{\rightarrow}$ содержит импликативную интуиционистскую логику, обычную комбинаторную логику $\mathbf{CL}_{\rightarrow}$. Вот пример того, как $\mathbf{RCL}_{\rightarrow}$ эмулирует комбинаторное правило аппликации

$$\frac{u:(A \rightarrow B), \quad v:A}{(u \cdot v):B}.$$

- | | |
|---|-----------------|
| 1. $u:(A \rightarrow B)$ | <i>гипотеза</i> |
| 2. $v:A$ | <i>гипотеза</i> |
| 3. $\mathbf{o}:[u:(A \rightarrow B) \rightarrow (v:A \rightarrow (u \cdot v):B)]$ | А5 |
| 4. $\mathbf{o}:[u:(A \rightarrow B) \rightarrow (v:A \rightarrow (u \cdot v):B)] \rightarrow [u:(A \rightarrow B) \rightarrow (v:A \rightarrow (u \cdot v):B)]$ | А4 |
| 5. $u:(A \rightarrow B) \rightarrow (v:A \rightarrow (u \cdot v):B)$ | <i>из 3,4</i> |
| 6. $v:A \rightarrow (u \cdot v):B$ | <i>из 1,5</i> |
| 7. $(u \cdot v):B$ | <i>из 2,6</i> |

Вот еще один пример вывода в $\mathbf{RCL}_{\rightarrow}$, уже без гипотез. Пусть $f:A$ есть одна из аксиом А2-А6.

- | | |
|---|----------------|
| 1. $f:A$ | <i>аксиома</i> |
| 2. $\mathbf{c}:(f:A \rightarrow !f:f:A)$ | А6 |
| 3. $\mathbf{c}:(f:A \rightarrow !f:f:A) \rightarrow (f:A \rightarrow !f:f:A)$ | А4 |

4. $f:A \rightarrow !f:f:A$ из 2,3
 5. $!f:f:A$ из 1,4

Теорема $\mathbf{RCL}_{\rightarrow}$ обладает свойством интернализации: если $A_1, \dots, A_n \vdash B$, то для любых свежих переменных x_1, \dots, x_n соответствующих типов можно построить λ -term $t(x_1, \dots, x_n)$ такой, что

$$x_1:A_1, \dots, x_n:A_n \vdash t(x_1, \dots, x_n):B.$$

Доказательство. Индукция по выводу $A_1, \dots, A_n \vdash B$. Пусть даны гипотезы $\Gamma' = \{x_1:A_1, \dots, x_n:A_n\}$. Если B есть A_i , то положим $t := x_i$. Если B есть аксиома A1, то положим t равной константе \mathbf{d} типа $t:A \rightarrow A$ и воспользуемся A4. Если B есть аксиома A2-A6, вида $f:A$ то положим t равным $!f$ и воспользуемся вышеприведенным примером. Поскольку $!f:f:A$ выводима без гипотез, она же выводима и из Γ' . Наконец, пусть B получена по правилу *modus ponens* из $A \rightarrow B$ и A . По предположению индукции, $\Gamma' \vdash p(\vec{x}):(A \rightarrow B)$ и $\Gamma' \vdash q(\vec{x}):A$. Положим t равным $p(\vec{x})q(\vec{x})$ и воспользуемся первым из приведенных выше примеров на выводимость в $\mathbf{RCL}_{\rightarrow}$, чтобы показать, что $\Gamma' \vdash t:B$.

Одной из целей $\mathbf{RCL}_{\rightarrow}$ является построение более богатой системы типов и термов для использования в языках программирования. В связи с этим представляет интерес следующая естественная (но пока неформальная) вычислительная семантика комбинаторов из $\mathbf{RCL}_{\rightarrow}$. Отправной точкой этой семантики является стандартная теоретико-множественная семантика типов, согласно которой тип это множество, а тип-импликация $U \rightarrow V$ это множество функций из U в V . Среди элементов данного типа могут встречаться конструктивные объекты, которым соответствуют *имена*, т.е. вычислительные программы. Термы в $\mathbf{RCL}_{\rightarrow}$ являются именами конструктивных объектов, конкретных (например, комбинаторы $\mathbf{k}, \mathbf{s}, \mathbf{d}, \mathbf{o}, \mathbf{c}$) или произвольных (например, переменные). Тип $t:F$ интерпретируется как множество, состоящее из объекта, соответствующего терму t . Базисные комбинаторы $\mathbf{RCL}_{\rightarrow}$ получают следующее прочтение:

$\mathbf{k}: [A \rightarrow (B \rightarrow A)]$	<i>функции-константы</i>
$\mathbf{s}: [(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))]$	<i>суперпозиция</i>
$\mathbf{d}: [t:F \rightarrow F]$	<i>денотат</i>
$\mathbf{o}: [u:(F \rightarrow G) \rightarrow (v:F \rightarrow (u \cdot v):G)]$	<i>интерпретатор</i>
$\mathbf{c}: [t:F \rightarrow !t:(t:F)]$	<i>кодирование</i>

Комбинаторы \mathbf{k} и \mathbf{s} заимствованы из комбинаторной логики $\mathbf{CL}_{\rightarrow}$ и сохраняют свою обычную функциональную семантику. Так, например, \mathbf{k} ставит в соответствие элементу $x \in A$ функцию-константу $\lambda y.x$, где y пробегает B .

Комбинатор *денотат* $\mathbf{d}: [t:F \rightarrow F]$ реализует фундаментальную функцию денотат, которая ставит в соответствие имени (программе) объект, имеющий данное имя. Каноническим примером может служить соответствие между индексом вычислимой функции и самой функцией.

Комбинатор *интерпретатор* $\mathbf{o}: [u:(F \rightarrow G) \rightarrow (v:F \rightarrow (u \cdot v):G)]$ реализует программу-интерпретатор, которая отображает данную программу u и данный вход v в результат применения u к v .

Комбинатор *кодирование* $\mathbf{c}: [t:F \rightarrow !t:(t:F)]$ отображает программу t в ее код $!t$ (алиас, специальный код в базе данных, etc.).

5.10. Новый взгляд на основания верификации. В приведенном ниже примере принцип доказуемости явной рефлексии $t:F \rightarrow F$ из **LP** применяется к теории верификации. Из этого примера видно, как основная идея логики доказательств — замена кванторов по доказательствам представляющими их явными функциями, может привести к более адекватной математической модели.

Метатеория формальных (в том числе компьютерных) систем проверки доказательств, называемых здесь *системами верификации*, была разработана в работе Дэвиса и Шварца [40]. Рассматривается следующая схема построения формальной системы для верификации V . Фиксируется ядро системы V_0 , достаточно простое для того, чтобы его непротиворечивость считалась очевидной и постулировалась; предполагается, что V_0 имеет достаточно выразительных средств для формализации доказательств и проверки их корректности. Рассматривается процесс пополнения системы верифицированными правилами вывода, в частности, доказуемыми фактами. В отличие от типичного для оснований математики пополнения теории новыми аксиомами для усиления теории, здесь задача пополнения V состоит в увеличении эффективности дедуктивного аппарата V без усиления, по возможности, метаматематической силы теории V .

Правило вывода Γ/F считается *верифицированным* в V , если

$$V \vdash \Box \Gamma \rightarrow \Box F,$$

где $\Box \Gamma$, $\Box F$ есть формальные утверждения о доказуемости в V всех формул из Γ и формулы F соответственно. Добавлению правила Γ/F соответствует переход от V к $V' = V + \Gamma/F$. Расширение системы называется *стабильным*, если V' консервативна над V . Основной метаматематический вопрос об этой схеме пополнения состоит в том, всегда ли теория V способна доказать свою собственную стабильность. В [40] получен отрицательный ответ на вопрос о доказуемости стабильности внутри самой системы V . Причину этого можно увидеть из следующего рассуждения. Допустим мы хотим установить, что $V' \vdash F$ влечет $V \vdash F$ индукцией по выводу в V' . Существенный шаг индукции соответствует переходу от $V \vdash \Gamma$ к $V \vdash F$ для произвольного частного случая данного правила вывода Γ/F . Из $V \vdash \Gamma$ по интернализации получаем $V \vdash \Box \Gamma$; этот шаг очевидно формализуется в V . Пользуясь выводимостью $V \vdash \Box \Gamma \rightarrow \Box F$, устанавливаем $V \vdash \Box F$, из чего и заключаем $V \vdash F$. Последний переход от $V \vdash \Box F$ к $V \vdash F$ невозможно, вообще говоря, обосновать средствами V в силу того, что рефлексия $\Box A \rightarrow A$ недоказуема в V (теорема Лёба). В [40] делается вывод о том, что принятый процесс построения систем верификации невозможно обосновать в рамках первоначальных предположений о непротиворечивости системы.

В работе [18] проведен анализ роста метаматематических допущений о теории в процессе ее пополнения по вышеприведенной схеме, а также предложена новая схема пополнения, свободная от ограничений Дэвиса-Шварца. Согласно новой схеме, верификация правила вывода Γ/F производится в явном виде и состоит в построении вычислимого терма $t(x)$ и доказательства $V \vdash x:\Gamma \rightarrow t(x):F$. Выигрыш состоит в том, что стабильность построенных на этой основе расширений доказуема в самой системе, что позволяет избавиться от дополнительных метаматематических предположений о данной верификационной системе. Вот схема рассуждений, показывающая доказуемую стабильность явной верификации. Вновь, мы хотим установить, что $V' \vdash F$ влечет $V \vdash F$. Существенный шаг индукции по выводу в V' соответствует переходу от $V \vdash \Gamma$ к $V \vdash F$ для правила Γ/F . Из $V \vdash \Gamma$ путем интернализации данного вывода в виде терма s мы заключаем, что $V \vdash s:\Gamma$. Пользуясь выводимостью $V \vdash x:\Gamma \rightarrow t(x):F$ устанавливаем $V \vdash s:\Gamma \rightarrow t(s):F$ и $V \vdash t(s):F$. В силу доказуемости явной рефлексии, $V \vdash t(s):F \rightarrow F$, следовательно и $V \vdash F$.

Анализ примеров показывает, что при неявной верификации по Дэвису-Шварцу, для доказательства того, что в V “существует доказательство Γ ” влечет “существует доказательство F ”, обычно сначала устанавливается, что $V \vdash x:\Gamma \rightarrow t(x):F$, а затем явные термы $x, t(x)$ заменяются на кванторы существования, чтобы удовлетворить формату неявной верификации. Точное знание терма $t(x)$ при этом оставалось неиспользованным из-за отсутствия теоретически обоснованного механизма его утилизации. Таким образом, несмотря на более ограничительный вид явной верификации, есть основания полагать, что в практическом смысле явная верификация применима тогда же, когда и неявная.

Список литературы

- [1] С.Н.Артемов, “Неарифметичность истинностных предикатных логик доказуемости.” Доклады Академии Наук СССР, т.284, no.2, с.270–271, 1985; English translation, “Nonarithmeticity of truth predicate logics of provability”, Soviet Mathematics Doklady, vol.33, pp. 403–405, 1986.
- [2] С.Н.Артемов, “Погружение модального λ -исчисления в Логику Доказательств” Труды математического интситута им. В.А.Стеклова, т.242, с.1-15, 2003.
- [3] В.А.Варданян, “Арифметическая сложность предикатных логик доказуемости и их фрагментов”, Доклады Академии Наук СССР, т.288, no.1, с.11-14, 1986; English translation: “Arithmetical complexity of predicate logics of provability and their fragments”, Soviet Mathematics Doklady, vol.34, pp.384–387, 1986.
- [4] А.Гейтинг, *Интуиционизм*, Москва, Мир, 1965; перевод с англ. А. Нейтинг. Intuitionism: An Introduction. North-Holland, 1956.

- [5] С.К.Клини, *Введение в метаматематику*, Москва, Изд-во иностр. лит., 1957; перевод с англ. S. Kleene. *Introduction to Metamathematics*, Van Norstrand, 1952.
- [6] А.Н.Колмогоров, “К толкованию интуиционистской логики”, В сборнике: С.М.Никольский, ред. *А.Н.Колмогоров. Избранные труды. Математика и Механика*, с.142-148, 1985; перевод с нем. А. Kolmogoroff, “Zur Deutung der intuitionistischen Logik”, *Math. Ztschr.*, Bd. 35, S.58–65, 1932.
- [7] А.Н.Колмогоров, “О моих работах по интуиционистской логике”. В сборнике: С.М.Никольский, ред. *А.Н.Колмогоров. Избранные труды. Математика и Механика*, с. 393, 1985; English transl.: A.Kolmogorov, “About my papers on intuitionistic logic”, In: A.N.Kolmogorov, *Selected works*, p.451–452.
- [8] А.В.Кузнецов, А.Ю.Муравицкий, “Логика Доказуемости”, Тезисы докладов *Четвертой Всесоюзной Конференции по Математической Логике*, с.73, 1976.
- [9] Ю.Т.Медведев, “Финитные задачи”, Доклады Академии Наук СССР, т.142, no.5, с.1015–1018, 1985; English translation, Yu.Medvedev, “Finite problems”, *Soviet Mathematics Doklady*, v. 3. pp. 227-230, 1962.
- [10] П.С.Новиков, *Конструктивная математическая логика с точки зрения классической*, Москва, Наука, 1977.
- [11] В.Е.Плиско, “Неарифметичность класса реализуемых предикатных формул”, *Известия АН СССР. Сер. Мат.*, т.41, No.3, с.483–502, 1977.
- [12] Т.Л.Сидон, “Интерполяционное свойство Крейга для операторных логик доказуемости”, Вестник Московского университета. Сер.1, Математика, Механика. 1998. No.2 с.34-38. English transl.: T.L.Sidon, “Craig Interpolation Property for Operational Logics of Proofs”, *Moscow University Mathematics Bulletin*, v.53, n.2, pp.37–41, 1999.
- [13] В.А.Успенский, В.Е.Плиско, “Интуиционистская логика”, В сборнике: С.М.Никольский, ред. *А.Н.Колмогоров. Избранные труды. Математика и Механика*, с.394–404, 1985.
- [14] J. Alt and S. Artemov, “Reflexive lambda-calculus”, In *Springer Lecture Notes in Computer Science*, v. 2183, Proceedings of the Dagstuhl-Seminar on Proof Theory in Computer Science, 2001.
- [15] S. Artemov. “Kolmogorov logic of problems and a provability interpretation of intuitionistic logic”, *Theoretical Aspects of Reasoning about Knowledge - III Proceedings*, Morgan Kaufman Pbl., pp. 257-272, 1990
- [16] S. Artemov, “Logic of Proofs”, *Annals of Pure and Applied Logic*, v. 67, pp. 29–59, 1994.

- [17] S. Artemov, “Operational Modal Logic,” *Tech. Rep. MSI 95-29*, Cornell University, December 1995.
- [18] S. Artemov, “On explicit reflection in theorem proving and formal verification,” In Springer *Lecture Notes in Artificial Intelligence*, v.1632 , Automated Deduction - CADE-16. Proceedings of the 16th International Conference on Automated Deduction, Trento, Italy, pp. 267–281, 1999.
- [19] S. Artemov, “Explicit provability and constructive semantics”, The *Bulletin for Symbolic Logic*, v.7, No. 1, pp. 1–36, 2001.
- [20] S. Artemov, “ Operations on proofs that can be specified by means of modal logic ”, *Advances in Modal Logic*, Volume 2, CSLI Publications, Stanford University, pp. 59-72, 2001.
- [21] S. Artemov, “Unified semantics for modality and lambda-terms via proof polynomials,” In Kees Vermeulen and Ann Copestake eds. *Algebras, Diagrams and Decisions in Language, Logic and Computation*, CSLI Publications, Stanford University, pp.89-119, 2002.
- [22] S. Artemov, E. Kazakov and D. Shapiro “On logic of knowledge with justifications ”, *Technical Report CFIS 99-12*, Cornell University, 1999. <http://www.cs.gc.cuny.edu/~sartemov/publications/S5LP.ps>.
- [23] S. Artemov and V. Krupski. “ Data storage interpretation of labeled modal logic ,” *Annals of Pure and Applied Logic*, v. 78, pp. 57-71, 1996.
- [24] S. Artemov and T. Sidon-Yavorskaya, “On the first order logic of proofs”, *Moscow Mathematical Journal*, vol.1, No.4, pp.475–490, 2001.
- [25] S. Artemov and T. Strassen, “The Basic Logic of Proofs”, *Springer Lecture Notes in Computer Science* , v.702, pp.14–28, 1993.
- [26] S. Artemov and T. Strassen, “Functionality in the Basic Logic of Proofs”, *Tech.Rep. IAM 92-004*, *Department for Computer Science*, University of Bern, Switzerland, 1993.
- [27] S. Artemov and T. Strassen, “The logic of the Gödel proof predicate”, *Springer Lecture Notes in Computer Science* , v. 713 , pp. 71–82, 1993.
- [28] J. Avigad and S. Feferman, “Gödel’s Functional (“Dialectica”) Interpretation”. In: S. Buss, ed., *Handbook of Proof Theory*, Elsevier, pp. 337-406, 1998.
- [29] M. Beeson. *Foundations of Constructive Mathematics*. Springer-Verlag, 1980.
- [30] L. Beklemishev, Induction rules, reflection principles, and provably recursive functions. *Annals of Pure and Applied Logic*, v.85, pp.193-242, 1997.

- [31] J. van Benthem. “Reflections on epistemic logic”, *Logique & Analyse*, 133-134, pp. 5-14, 1991.
- [32] G. Boolos, *The Unprovability of Consistency: An Essay in Modal Logic*, Cambridge University Press, 1979.
- [33] G. Boolos, *The Logic of Provability*, Cambridge University Press, 1993.
- [34] V. Brezhnev, “On explicit counterparts of modal logics,” *Tech. Rep. CFIS 2000-06*, Cornell University, 2000.
- [35] V. Brezhnev, “On the Logic of Proofs,” *Proceedings of the Sixth ESSLLI Student Session*, Helsinki, pp. 35-46, 2001. <http://www.helsinki.fi/esslli/>
- [36] S. Buss, “The Modal Logic of Pure Provability”, *Notre Dame Journal of Formal Logic*, v. 31, No. 2, 1990
- [37] R. Constable, “Types in Logic, Mathematics and Programming”. In: *S. Buss, ed., Handbook of Proof Theory*, Elsevier, pp. 683-786, 1998.
- [38] D. van Dalen, “Intuitionistic Logic”. In *D. Gabbay and F. Guenther, eds., Handbook of Philosophical Logic*, Reidel Publishing Company, v. 3. p. 225-340, 1986.
- [39] D. van Dalen, *Logic and Structure*, Springer-Verlag, 1994
- [40] M. Davis and J. Schwartz, “Metamathematical Extensibility for Theorem Verifiers and Proof Checkers”, *Computers and Mathematics with Applications*, v.5, pp.217-230, 1979.
- [41] M. Fitting, “A Semantic Proof of the Realizability of Modal Logic in the Logic of Proofs”, *CUNY Ph.D. Program in Computer Science, Technical Report TR-2003010*, 2003.
- [42] M. Fitting, “A Semantics for the Logic of Proofs”, *CUNY Ph.D. Program in Computer Science, Technical Report TR-2003012*, 2003.
- [43] D.M. Gabbay, *Labelled Deductive Systems*, Oxford University Press, 1994.
- [44] J.-Y. Girard, Y. Lafont, P. Taylor, *Proofs and Types*, Cambridge University Press, 1989.
- [45] K. Gödel, “Eine Interpretation des intuitionistischen Aussagenkalküls”, *Ergebnisse Math. Colloq.*, Bd. 4 (1933), S. 39-40.
- [46] K. Gödel, “Vortrag bei Zilsel” (1938), in S. Feferman, ed. *Kurt Gödel Collected Works. Volume III*, Oxford University Press, 1995.
- [47] R. Goldblatt, “Arithmetical necessity, provability and intuitionistic logic”, *Theoria*, 44, pp. 38-46, 1978.

- [48] N.K. Goodman, “A theory of constructions is equivalent to arithmetic”, *Intuitionism and proof theory* (J.Myhill, A.Kino, R.E. Vesley, editors), North Holland, pp. 101–120, 1970.
- [49] A. Heyting, “Die intuitionistische Grundlegung der Matematik”, *Erkenntnis* v.2, pp.106-115, 1931.
- [50] A. Heyting, *Mathematische Grundlagenforschung. Intuitionismus. Beweistheorie*, Springer, Berlin, 1934.
- [51] D. de Jongh and G. Japaridze, “Logic of Provability”, in S. Buss, ed., *Handbook of Proof Theory*, Elsevier, 1998.
- [52] S. Kleene. “On the interpretation of intuitionistic number theory”, *Journal of Symbolic Logic*, v. 10, pp. 109-124, 1945.
- [53] G. Kreisel, “Foundations of intuitionistic logic”, in E.Nagel, P.Suppes and A.Tarski, eds., *Logic, Methodology and Philosophy of Science. Proceedings of the 1960 International Congress*, Stanford University Press, Stanford, pp. 198-210, 1962.
- [54] G. Kreisel, “On weak completeness of intuitionistic predicate logic”, *Journal of Symbolic Logic*, v. 27, pp. 139-158, 1962.
- [55] G. Kreisel, “Mathematical Logic”, in T.L.Saaty, ed., *Lectures in Modern Mathematics III* Wiley and Sons, New York, pp. 95-195, 1965.
- [56] S. Kripke, “Semantical considerations on modal logic”, *Acta Philosophica Fennica*, 16, pp. 83-94, 1963.
- [57] N.V. Krupski, “On the Complexity of the Reflected Logic of Proofs”, *CUNY Ph.D. Program in Computer Science, Technical Report TR-2003007*, 2003.
- [58] V.N. Krupski, “Operational Logic of Proofs with Functionality Condition on Proof Predicate”, *Lecture Notes in Computer Science*, v. 1234, *Logical Foundations of Computer Science’ 97, Yaroslavl’*, pp. 167-177, 1997.
- [59] V.N. Krupski, “The single-conclusion proof logic and inference rules specification”, *Annals of Pure and Applied Logic*, v. 113, No. 1-3, pp. 181-206, 2001.
- [60] V.N. Krupski, “Referential Logic of Proofs”, *Theoretical Computer Science*, accepted for publication, 2004.
- [61] R. Kuznets, “On the Complexity of Explicit Modal Logics”, *Lecture Notes in Computer Science*, v. 1862, *Computer Science Logic 2000*, pp. 371-383, 2000.
- [62] H. Läuchli, “An abstract notion of realizability for which intuitionistic predicate logic is complete”, in: J. Myhill, A.Kino and R.E. Vesley, eds., *Intuitionism and Proof Theory*, North-Holland, Amsterdam, pp. 227-234, 1970.

- [63] E. Lemmon, "New Foundations for Lewis's modal systems", *Journal of Symbolic Logic*, v. 22, pp. 176-186, 1957.
- [64] J.C.C. McKinsey and A. Tarski, "Some theorems about the sentential calculi of Lewis and Heyting", *Journal of Symbolic Logic*, v. 13, pp. 1-15, 1948.
- [65] G. Mints. "Lewis' systems and system T (1965-1973)". In *Selected papers in proof theory*, Bibliopolis, Napoli, 1992.
- [66] A. Mkrtychev, "Models for the Logic of Proofs", Lecture Notes in Computer Science, v. 1234, *Logical Foundations of Computer Science' 97, Yaroslavl'*, pp. 266-275, 1997.
- [67] R. Montague. "Syntactical treatments of modality with corollaries on reflection principles and finite axiomatizability", *Acta Philosophica Fennica*, 16, pp. 153-168, 1963.
- [68] J. Myhill, "Some Remarks on the Notion of Proof", *Journal of Philosophy*, 57, pp. 461-471, 1960
- [69] J. Myhill, "Intensional Set Theory", In: S. Shapiro, ed., *Intensional Mathematics*, North-Holland, pp. 47-61, 1985.
- [70] Y. Moses, "Resource-bounded knowledge", In *Theoretical Aspects of Reasoning about Knowledge*, ed. M. Vardi, Morgan Kaufmann, pp. 261-276, 1988.
- [71] R. Parikh. "Knowledge and the problem of logical omniscience", *ISMIS-87* (International Symposium on Methodology for Intellectual Systems), ed/ Z. Ras and M. Zemankova, North Holland, pp.432-439, 1987.
- [72] R. Parikh. "Logical omniscience" in *Logic and Computational Complexity*, Ed. Leivant, Springer Lecture Notes in Computer Science No. 960, pp. 22-29, 1995.
- [73] B. Renne, "Tableaux for the Logic of Proofs", *CUNY Ph.D. Program in Computer Science, Technical Report TR-2004001*, 2004.
- [74] D. Scott. "Constructive validity". In: M. Laudet et al, eds., *Symposium on Automatic Demonstration* Springer, Berlin, 1970.
- [75] S. Shapiro. "Intensional Mathematics and Constructive Mathematics". In: S. Shapiro, ed., *Intensional Mathematics*, North-Holland, pp. 1-10, 1985.
- [76] S. Shapiro. "Epistemic and Intuitionistic Arithmetic". In: S. Shapiro, ed., "Intensional mathematics", North-Holland, pp. 11-46, 1985.
- [77] T. Sidon, "Provability Logic with Operations on Proofs", Lecture Notes in Computer Science, v. 1234, *Logical Foundations of Computer Science' 97, Yaroslavl'*, pp. 342-353, 1997.

- [78] T. Yavorskaya (Sidon), “Logic of proofs and provability”, *Annals of Pure and Applied Logic*, v. 113, No. 1-3, pp. 345-372, 2001.
- [79] C. Smorynski, *Self-Reference and Modal Logic*, Springer-Verlag, Berlin, 1985.
- [80] R. Solovay, “Provability interpretations of modal logic”, *Israel Journal of Mathematics*, 25, pp. 287-304, 1976.
- [81] A.S. Troelstra “Realizability”. In *S. Buss, ed., Handbook of Proof Theory*, Elsevier, pp. 407-474, 1998.
- [82] A.S. Troelstra and D. van Dalen, *Constructivism in Mathematics. An Introduction*, v. 1, Amsterdam; North Holland, 1988.
- [83] A.S. Troelstra and H. Schwichtenberg, *Basic Proof Theory*, Cambridge University Press, 1996.
- [84] V.A. Uspensky, “Kolmogorov and mathematical logic”, *Journal of Symbolic Logic*, 57, No.2, 1992.
- [85] S. Weinstein, “The intended interpretation of intuitionistic logic”, *Journal of Philosophical Logic*, 12, pp. 261-270 1983.
- [86] R. Yavorsky, “On the Logic of the Standard Proof Predicate” Lecture Notes in Computer Science, v. 1862, *Computer Science Logic 2000*, pp.527-541, 2000.
- [87] R. Yavorsky, “Provability logics with quantifiers on proofs”, *Annals of Pure and Applied Logic*, v. 113, No. 1-3, pp. 373-387, 2001.