Варианты понятия реализуемости для пропозициональных формул, приводящие к логике Янкова

Н. К. Верещагин [*] Д. П. Скворцов [†] Е. З. Скворцова [‡]
А. В. Чернов [§]

Аннотация

До сих пор неизвестно, является ли конечно (или хотя бы рекурсивно) аксиоматизируемой логика реализуемых пропозициональных формул. В настоящей работе мы предлагаем несколько естественных ослаблений клиниевской реализуемости пропозициональных формул, основанных на следующей неформальной идее: пропозициональная формула реализуема, если при любой подстановке у неё найдётся „простая“ реализация. Мы доказываем, что все эти ослабления приводят к одной конечно аксиоматизируемой логике — логике слабого закона исключённого третьего (логике Янкова). Доказательство использует характеризации суперинтуиционистских логик с интуиционистским позитивным фрагментом, полученные в 60-е годы Медведевым и Янковым.

Ключевые слова: реализуемость; колмогоровская сложность; суперинтуиционистские логики.

1. Введение

В 1932 году в своей статье [1] Колмогоров предложил конструктивное истолкование интуиционистской логики высказываний в терминах „исчисления задач“. Формулам сопоставляются задачи из некоторого заданного класса, а логическим связкам $\vee$, $\wedge$, $\to$ соответствуют естественные операции над задачами — „решить одну из задач“, „решить обе задачи“, „из

[*] 119992, Москва, ГСП-2, Ленинские Горы, МГУ им. Ломоносова, механико-математический факультет, кафедра математической логики и теории алгоритмов. E-mail: ver@mccme.ru. Работа выполнена при частичной поддержке грантов РФФИ № 01-01-01028 и 02-01-22001.

[†] Москва, ул. Усиевича, 20а, Всероссийский институт научной и технической информации. E-mail: skvortsov@viniti.ru

[‡] 119992, Москва, ГСП-2, Ленинские Горы, МГУ им. Ломоносова, Всероссийская заочная многопредметная школа.

[§] 119992, Москва, ГСП-2, Ленинские Горы, МГУ им. Ломоносова, механико-математический факультет, кафедра математической логики и теории алгоритмов. E-mail: chernov@mccme.ru. Работа выполнена при частичной поддержке грантов РФФИ № 01-01-01028, 01-01-00505 и 02-01-22001.

решения первой задачи получить решение второй“. Таким образом, подставив в формулу вместо пропозициональных переменных некоторые элементарные задачи, можно построить составную задачу. При этом решения задач, соответствующих интуиционистски выводимым формулам, можно указать „заранее“, до фиксации подставляемых элементарных задач.

В статье Колмогорова не конкретизируется, что следует понимать под „задачей“. Впоследствии было несколько попыток разработать на основе этой идеи формальную семантику для интуиционизма. К ним, в частности, можно отнести реализуемость по Клини (см. [2, §82]) и логику финитных задач Медведева ([3]–[5]). Однако пропозициональное интуиционистское исчисление оказалось неполным относительно этих интерпретаций. Более того, для логики финитных задач доказана невозможность конечной аксиоматизации (см. [6]) и неизвестно, возможна ли рекурсивная аксиоматизация; для логики реализуемых формул неизвестен ответ на оба вопроса.

В настоящей статье мы рассмотрим несколько новых интерпретаций типа реализуемости. Все они получаются следующим образом: мы считаем пропозициональную формулу реализуемой, если при подстановке в неё вместо переменных некоторых задач полученная задача имеет решение, сложность которого ограничена данной функцией от сложностей подставляемых задач. Варьируя тип задач, подставляемых вместо переменных, способ измерения сложности и ограничения на сложность решения, можно получить несколько разных „реализуемостей“. Примечательно, что все рассмотренные нами варианты приводят к одному и тому же множеству реализуемых формул.

Перейдём к точным определениям.

1.1. Пропозициональные формулы строятся из переменных p и q (с различными индексами) и константы $\bot$ („ложь“) при помощи логических связок $\vee$, $\wedge$, $\to$; будут также использоваться общепринятые сокращения: $(\Phi \leftrightarrow \Psi) \rightleftharpoons (\Phi \to \Psi) \wedge (\Psi \to \Phi)$, $\neg\Psi \rightleftharpoons (\Psi \to \bot)$, $\top \rightleftharpoons (\bot \to \bot)$. *Позитивные* формулы — это формулы, не содержащие константы $\bot$ (связки $\neg$). Пропозициональные формулы обычно будут обозначаться прописными буквами Φ и Ψ, а арифметические — строчными φ, ψ.

Суперинтуиционистской логикой называется множество пропозициональных формул, содержащее все аксиомы интуиционистской логики высказываний $\mathfrak{Int}$ и замкнутое относительно правил modus ponens и подстановки (аксиомы $\mathfrak{Int}$ приведены, например, в [2]). Запись $L \vdash \Phi$ означает, что формула Φ принадлежит логике L, а $(L + \Gamma)$, где Γ — некоторое множество формул, обозначает наименьшую суперинтуиционистскую логику, содержащую $(L \cup \Gamma)$. Множество позитивных формул логики L называется её позитивным фрагментом L_Π. Будем говорить, что логика L *имеет интуиционистский позитивный фрагмент*, если $L_\Pi = \mathfrak{Int}_\Pi$.

Задачей мы будем называть произвольное множество натуральных чисел, а *решением задачи* — любой элемент из этого множества. Содержательно наша формализованная задача является совокупностью всех решений некоторой „обычной“ задачи (примеры из [1]:„через данные три точки провести окружность“, „из рациональности числа π вывести рациональность числа e“), записанных на каком-нибудь подходящем языке и закодированных натуральными числами.

Пусть зафиксирована некоторая главная вычислимая нумерация для семейства частичных вычислимых функций из $\mathbb{N}$ в $\mathbb{N}$, то есть такая частичная вычислимая функция $U\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$, что для любой вычислимой функции $V\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ найдётся всюду определённая вычислимая функция s, для которой $U(s(n),x)=V(n,x)$ для всех n,x. Будем использовать запись $e(x)$, где $e,x\in\mathbb{N}$, как сокращение для $U(e,x)$. При фиксированном e выражение $e(x)$ задаёт вычислимую функцию от x, причём каждая одноместная вычислимая функция представима в таком виде (для надлежащего e), поэтому мы часто будем называть число e *программой* для вычисления этой функции. Ещё пусть зафиксирована некоторая вычислимая нумерация пар $\langle x,y\rangle$, и вообще кортежей произвольной длины $\langle x_1,\ldots,x_k\rangle$. В дальнейшем мы не будем различать кортеж и его номер.

Определим соответствующие логическим связкам *операции над задачами*, то есть подмножествами $\mathbb{N}$ (последние будут обозначаться прописными латинскими буквами).

Определение 1 (Операции над множествами).
$X\vee Y \rightleftharpoons \{\langle 0,x\rangle \mid x\in X\}\cup\{\langle 1,y\rangle\mid y\in Y\}$,
$X\wedge Y \rightleftharpoons \{\langle x,y\rangle \mid x\in X, y\in Y\}$,
$X\to Y \rightleftharpoons \{e\in\mathbb{N}\mid \forall x\in X\,[e(x)\in Y]\}$,
$\bot=\varnothing$ и $\neg X\rightleftharpoons X\to\bot\rightleftharpoons X\to\varnothing$
(то есть, $\neg X=\mathbb{N}$, если $X=\varnothing$, и $\neg X=\varnothing$, если $X\neq\varnothing$).

Теперь, если пропозициональным переменным $p_1,\ldots,p_n$ сопоставлены некоторые множества $X_1,\ldots,X_n$, то индукцией по построению формулы $\Phi(p_1,\ldots,p_n)$ можно определить множество $\Phi(X_1,\ldots,X_n)$, которое будет называться результатом подстановки указанных множеств в формулу Φ.

Перейдём к определению реализуемости по Клини. В рамках нашего подхода это удобно сделать, используя понятие множества реализаций замкнутой арифметической формулы. Если формула φ — атомарная, то множество её реализаций $R(\varphi)$ есть $\{0\}$ для истинной формулы φ и $\varnothing$ — для ложной. Для пропозициональных связок положим $R(\varphi\circ\psi)\rightleftharpoons R(\varphi)\circ R(\psi)$, где $\circ$ означает $\vee$, $\wedge$ или $\to$. Наконец, для кванторов положим $R(\forall x\varphi(x))\rightleftharpoons \{e\mid \forall k\in\mathbb{N}\,[e(k)\in R(\varphi(k))]\}$ и $R(\exists x\varphi(x))\rightleftharpoons\{\langle a,k\rangle\mid a\in R(\varphi(k))\}$. Будем говорить, что число r *реализует замкнутую арифметическую формулу* φ, если $r\in R(\varphi)$ (легко видеть, что это эквивалентно определению в [2, §82]). Число r *реализует арифметическую формулу* $\varphi(x_1,\ldots,x_n)$ *со свободными переменными* $x_1,\ldots,x_n$, если $r(\langle k_1,\ldots,k_n\rangle)\in R(\varphi(k_1,\ldots,k_n))$ для любых $k_1,\ldots,k_n\in\mathbb{N}$. Формула $\varphi(x_1,\ldots,x_n)$ называется *реализуемой*, если у неё есть хотя бы одна реализация (это равносильно реализуемости замкнутой формулы $\forall x_1\ldots\forall x_n\,\varphi(x_1,\ldots,x_n)$).

Пропозициональная формула $\Phi(p_1,\ldots,p_n)$ называется *реализуемой*, если для любых арифметических формул $\varphi_1,\ldots,\varphi_n$ (возможно, со свободными переменными[1]) реализуема формула $\Phi(\varphi_1,\ldots,\varphi_n)$. Множество реализуемых пропозициональных формул будем обозначать $\mathfrak{R}$.

Если реализацию формулы $\Phi(\varphi_1,\ldots,\varphi_n)$ можно эффективно найти по $\varphi_1,\ldots,\varphi_n$, то Φ называется *эффективно реализуемой* (здесь можно ограни-

[1]Если подставлять только замкнутые формулы, получится классическая логика. В частности, формула $\varphi\vee\neg\varphi$ реализуема для всякой замкнутой арифметической формулы φ (но формула $\forall x(\varphi(x)\vee\neg\varphi(x))$ реализуема не всегда).

читься только замкнутыми $\varphi_1, \ldots, \varphi_n$). Если же существует единая реализация формул $\Phi(\varphi_1, \ldots, \varphi_n)$ для всех замкнутых $\varphi_1, \ldots, \varphi_n$, то Φ называется *константно (или равномерно) реализуемой.* Множество эффективно реализуемых формул обозначим $\mathfrak{R}_{\mathrm{eff}}$, а множество константно реализуемых — $\mathfrak{R}_{\mathrm{const}}$. (Небольшое замечание по терминологии: во многих отечественных работах по конструктивной математике реализуемыми пропозициональными формулами принято называть те, которые мы здесь называем эффективно реализуемыми; реализуемые в нашем смысле формулы называют неопровержимыми. Мы надеемся, что эти разночтения не приведут к недоразумениям.)

Легко понять, что $\mathfrak{R}$, $\mathfrak{R}_{\mathrm{eff}}$, $\mathfrak{R}_{\mathrm{const}}$ являются суперинтуиционистскими логиками (это фактически доказывается в теореме Нельсона в [2]). Очевидно, что $\mathfrak{R}_{\mathrm{const}} \subseteq \mathfrak{R}_{\mathrm{eff}} \subseteq \mathfrak{R}$. Роуз в работе [7] показал, что $\mathfrak{R}_{\mathrm{const}} \neq \mathfrak{Int}$. Поэтому интересен вопрос, возможно ли задать логику реализуемых формул аксиоматически. Следующая теорема была сформулирована Медведевым в работе [4] (как следствие некоторого ошибочного утверждения; указал на ошибку и дал верное доказательство Плиско в работе [8]).

Теорема 1 (Медведев, Плиско). *Логики $\mathfrak{R}$, $\mathfrak{R}_{\mathrm{eff}}$, $\mathfrak{R}_{\mathrm{const}}$ имеют интуиционистский позитивный фрагмент.*

Некоторое исчисление с конечным числом аксиом (в подходящем расширенном языке), содержащее все ныне известные реализуемые формулы, сформулировано Варпаховским в [9]. Однако пока неизвестно, совпадают ли логики $\mathfrak{R}$, $\mathfrak{R}_{\mathrm{eff}}$, $\mathfrak{R}_{\mathrm{const}}$ и являются ли они рекурсивно перечислимыми.

Изложим теперь эквивалентную переформулировку определения реализуемости, удобную для обобщений. Идея состоит в том, чтобы подставлять в пропозициональную формулу вместо переменных не арифметические формулы, а непосредственно задачи (подмножества $\mathbb{N}$). Для начала заметим, что подстановка в пропозициональную формулу $\Phi(p_1, \ldots, p_n)$ замкнутых арифметических формул сводится к подстановке *некоторых арифметических множеств* (а именно, множеств реализаций этих арифметических формул) и действиям с ними как подмножествами $\mathbb{N}$, то есть, $R(\Phi(\varphi_1, \ldots, \varphi_n)) = \Phi(R(\varphi_1), \ldots, R(\varphi_n))$. Следующее утверждение показывает, что на самом деле можно подставлять *произвольные* арифметические множества.

Утверждение 1.
1. Пропозициональная формула $\Phi(p_1, \ldots, p_n)$ константно реализуема тогда и только тогда, когда существует такая единая реализация r, что $r \in \Phi(A_1, \ldots, A_n)$ для любых арифметических множеств $A_1, \ldots, A_n$.
2. Пропозициональная формула $\Phi(p_1, \ldots, p_n)$ реализуема тогда и только тогда, когда для произвольных арифметических семейств множеств $A_1(x), \ldots, A_n(x)$ существует такое число r (реализация), что $r(k) \in \Phi(A_1(k), \ldots, A_n(k))$ для любого $k \in \mathbb{N}$. (Семейство множеств $\{A(k) \mid k \in \mathbb{N}\}$ (обозначаемое $A(x)$) называется арифметическим, если существует такая арифметическая формула $\varphi(x, y)$, что $A(k) = \{m \mid \varphi(m, k)\}$.)

(Похожим образом эффективную реализуемость можно определить как существование алгоритма, который по номерам произвольных арифметических множеств, подставленных вместо переменных, находит реализацию формулы.)

Доказательство.
Заметим сначала, что в определении реализуемости можно считать, что подставляемые арифметические формулы имеют только одну свободную переменную (достаточно использовать кодирование кортежей). Теперь докажем вторую часть утверждения (для константной реализуемости рассуждение аналогичное).
Тогда. Пусть $\varphi_1(x), \ldots, \varphi_n(x)$ — арифметические формулы со свободной переменной x. Рассмотрим семейства множеств $A_i(x) = R(\varphi_i(x))$. Существует такое r, что $r(k) \in \Phi(A_1(k), \ldots, A_n(k)) = R(\Phi(\varphi_1(k), \ldots, \varphi_n(k))$. Таким образом, формула $\Phi(\varphi_1(x), \ldots, \varphi_n(x))$ реализуема, что и требовалось.
Только тогда. Пусть $A_i(x) = \{m \mid \varphi_i(m, x)\}$ — арифметические семейства множеств. Мы не можем рассчитывать на то, что $A_i(x) = R(\varphi_i'(x))$ для какой-нибудь формулы φ_i'. Однако из изложенного в [2, §§ 81,82] следует, что для произвольной формулы $\varphi(y, x)$ если $A(x) = \{m | \varphi(m, x)\}$, то $\mathbb{N} \times A(k) = R(\psi(k))$, где $\psi(x) = \exists y \varphi^{\neg\neg}(y, x)$; формула $\varphi^{\neg\neg}$ (так называемый негативный перевод Колмогорова) получается из φ добавлением двойного отрицания перед каждой подформулой. Положим $\psi_i(k) = \exists y \varphi_i^{\neg\neg}(y, k)$. Теперь индукцией по построению Φ легко показать, что по элементу множества $\Phi(R(\psi_1(k)), \ldots, R(\psi_n(k))) = R(\Phi(\psi_1(k), \ldots, \psi_n(k)))$ можно эффективно получить элемент множества $\Phi(A_1(k), \ldots, A_n(k))$ и наоборот (более того, это преобразование, фактически являющееся решением задачи $\Phi(\mathbb{N} \times A_1(k), \ldots, \mathbb{N} \times A_n(k)) \to \Phi(A_1(k), \ldots, A_n(k))$, можно выбрать *единым* для всех $A_1, \ldots, A_n$; последнее важно при рассмотрении константной реализуемости). Поскольку формула $\Phi(\psi_1(x), \ldots, \psi_n(x))$ реализуема, элемент из $R(\Phi(\psi_1(k), \ldots, \psi_n(k)))$ можно эффективно найти по заданному k. □

Пользуясь этим утверждением, мы в дальнейшем будем говорить о семействах множеств, а не о формулах.

Естественной теперь кажется мысль подставлять в пропозициональную формулу вместо переменных произвольные, а не только арифметические, множества $X_1, \ldots, X_n$. Эту идею применительно к предикатным формулам рассматривал Плиско в [10]. Он назвал соответствующее понятие *абсолютной реализуемостью*. Возможно, представляет интерес и соответствующая пропозициональная логика L_{abs}. А именно, пропозициональная формула $\Phi(p_1, \ldots, p_n)$ *абсолютно реализуема*, если существует такая единая реализация r, что $r \in \Phi(X_1, \ldots, X_n)$ для любых множеств $X_1, \ldots, X_n \subseteq \mathbb{N}$ (ср. со первой частью утверждения 1). Оказывается, что равносильное определение получится, если аналогичным образом опустить слово „арифметических“ во второй части утверждения 1, то есть разница между обычной и константной реализуемостью исчезает (доказательство можно найти в [10], хотя результаты о пропозициональных формулах Плиско и не формулирует явно). Очевидно, $L_{\text{abs}} \subseteq \mathfrak{R}_{\text{const}}$. Неизвестно, является ли это включение строгим. Во всяком случае, все ныне известные реализуемые формулы (исчисление Варпаховского) абсолютно реализуемы.

1.2. Перейдём теперь к ослабленным вариантам реализуемости. Во всех ранее рассмотренных определениях реализацию требовалось указать эффективно по подставляемым множествам (из данного семейства) или даже независимо от этих множеств. Ослабим это требование: будем указывать „небольшое“ множество, заведомо содержащее реализацию (множество „кандидатов в реализацию“). Начнём с определения самого слабого (в том смысле, что множество реализуемых формул максимально) из таких аналогов реализуемости.

Определение 2. Пропозициональная формула $\Phi(p_1,\dots,p_n)$ слабо реализуема (множество таких формул обозначим через $\mathfrak{R}_{\mathrm{w}}$), если для некоторого натурального $i > 0$ выполнено следующее. Для любых арифметических семейств $A_1(x),\dots,A_n(x)$ найдется арифметическое семейство $B(x)$ такое, что задающая его формула принадлежит классу арифметической иерархии Σ_i, для всех $k \in \mathbb{N}$ множество $B(k)$ конечно, а пересечение его с $\Phi(A_1(k),\dots,A_n(k))$ непусто.

В силу утверждения 1 все реализуемые формулы слабо реализуемы, причём для них можно взять $i = 1$, а множества $B(k)$ — одноэлементными. Отметим, что если не ограничивать заранее сложность семейства $B(x)$ (то есть не фиксировать i), то формула $p \vee \neg p$ была бы реализуемой.

Следующее определение даёт аналог наиболее сильной реализуемости, константной[2].

Определение 3. Пропозициональная формула $\Phi(p_1,\dots,p_n)$ принадлежит множеству[3] $\mathfrak{R}_{O(1)}$, если существует натуральное число C такое, что для любых арифметических множеств $A_1,\dots,A_n$ существует такое $r \leqslant C$, что $r \in \Phi(A_1,\dots,A_n)$.

Непосредственно из определений следует, что $\mathfrak{R}_{\mathrm{w}}$ и $\mathfrak{R}_{O(1)}$ являются суперинтуиционистскими логиками, причём $\mathfrak{R} \subseteq \mathfrak{R}_{\mathrm{w}}$, $\mathfrak{R}_{\mathrm{const}} \subseteq \mathfrak{R}_{O(1)}$ и $\mathfrak{R}_{O(1)} \subseteq \mathfrak{R}_{\mathrm{w}}$ (Доказательства этого и последующих утверждений приведены в параграфе 3).

Теорема 2 (Верещагин, Чернов). *$\mathfrak{R}_{\mathrm{w}} = \mathfrak{R}_{O(1)} = \mathfrak{J}$, где $\mathfrak{J} = \mathfrak{Int} + (\neg p \vee \neg\neg p)$ — логика Янкова (логика слабого закона исключённого третьего).*

Другой подход к определению реализуемости предложен А. Шенем (см. [11]). Во-первых, как и в случае абсолютной реализуемости, в пропозициональную формулу будем подставлять произвольные, а не только арифметические множества. Во-вторых, потребуем, чтобы сложность реализации была ограничена какой-нибудь функцией от сложностей подставляемых множеств. В качестве сложностной меры множества будем использовать минимум колмогоровских сложностей его элементов. То есть простой задача считается в том случае, если можно коротко задать хотя бы одно из её решений (элемент соответствующего множества).

Неформально говоря, колмогоровской сложностью $K(x)$ слова x называется длина кратчайшей программы, порождающей x. Чтобы дать строгое определение, мы должны зафиксировать какую-нибудь (одноместную) частичную вычислимую функцию F со следующим свойством оптимальности: для любой частичной вычислимой функции G существует такая константа

[2]Мы ограничимся только двумя вариантами понятия слабой реализуемости, поскольку остальные возможные модификации занимают промежуточное положение между рассматриваемыми.

[3]Поскольку все наши ослабления приводят к одной и той же логике, далее мы будем вводить только обозначения для множеств формул, а не названия „реализуемостей“, чтобы не плодить лишних терминов.

c, что $\forall e \exists e' (\, \ell(e') \leqslant \ell(e) + c,\, F(e') = G(e))$, где $\ell(e)$ — длина двоичной записи числа e. Можно доказать (см. [12]), что такая функция F существует. Теперь положим по определению $K(x) \rightleftharpoons \min\{\, \ell(e) \mid F(e) = x\}$. Так определённая функция K называется функцией сложности, соответствующей оптимальному способу описания F. Хотя $K(x)$ зависит от выбора F, любые две функции сложности $K_1(x)$ и $K_2(x)$ различаются не более чем на константу (то есть, существует такая константа c (зависящая от K_1 и K_2), что $|K_1(x) - K_2(x)| \leqslant c$ для любого x). Поэтому в дальнейших формулировках будет содержаться либо аддитивная константа (зависящая от способа описания), либо член $O(1)$ (то есть функция, ограниченная константой при всех возможных значениях переменной).

Приведём без доказательства основные свойства колмогоровской сложности (подробнее об этом можно прочитать в монографии [12]):

1) $\exists c \forall x\, K(x) \leqslant \ell(x) + c$;

2) для любой частичной вычислимой функции f
$\exists c \forall x\, K(f(x)) \leqslant K(x) + c$;

3) множество $\{\langle x, n\rangle \mid K(x) < n\}$ рекурсивно перечислимо;

4) множество $\{x \mid K(x) < n\}$ содержит не более 2^{n-1} элементов;

5) $\forall x, y \quad K(\langle x, y\rangle) \leqslant K(x) + K(y) + O(\log\min\{K(x), K(y)\})$
(идея в том, что пару можно восстановить, зная коды x и y, записанные без разделителя, и длину одного из них, записанную, например, в префиксном коде).

Для множеств положим $K(X) \rightleftharpoons \min\{K(x) \mid x \in X\}$ (а $K(\varnothing)$ равно бесконечности).

Отметим (это будет доказано в параграфе 3), что для любой пропозициональной формулы $\Phi(p_1, \ldots, p_n)$ существует такая константа C, что для любых множеств $X_1, \ldots, X_n$, если $\Phi(X_1, \ldots, X_n) \neq \varnothing$, то

$$K(\Phi(X_1, \ldots, X_n)) \leqslant K(\bigwedge_{X_i \neq \varnothing} X_i) + O(1) \leqslant \sum_{X_i \neq \varnothing} K(X_i) + C \cdot \log \sum_{X_i \neq \varnothing} K(X_i)\,.$$

Таким образом, наибольшей естественной границей сложности, для которой „реализуемы“ ещё не все формулы, можно считать $o(\sum\limits_{X_i \neq \varnothing} K(X_i))$. Естественной нижней границей является $O(1)$, как по причинам, отмеченным при определении функции $K(x)$, так и потому, что для всех интуиционистски выводимых формул $K(\Phi(X_1, \ldots, X_n)) = O(1)$. Эти соображения приводят к определению наименьшего и наибольшего (из возможных при таком подходе) множеств „реализуемых“ формул.

Определение 4. Пропозициональная формула $\Phi(p_1, \ldots, p_n)$ принадлежит множеству $L_{O(1)}$, если $\exists C\, \forall X_1, \ldots, X_n\, K(\Phi(X_1, \ldots, X_n)) \leqslant C$.
Пропозициональная формула $\Phi(p_1, \ldots, p_n)$ принадлежит множеству $L_{o(\Sigma)}$, если существует такая функция $f : [0, \infty) \to [0, \infty)$, что $f(x) = o(x)$ и $\forall X_1, \ldots, X_n \quad K(\Phi(X_1, \ldots, X_n)) \leqslant f(\sum\limits_{X_i \neq \varnothing} K(X_i))$.

Очевидно, что $L_{O(1)}$, $L_{o(\Sigma)}$ являются суперинтуиционистскими логиками. В параграфе 3 будут сделаны ещё некоторые замечания, поясняющие это определение, а сейчас скажем только, что если в определении $\mathfrak{R}_{O(1)}$ опустить требование арифметичности подставляемых множеств, то мы получим в точности $L_{O(1)}$, и потому $L_{O(1)} \subseteq \mathfrak{R}_{O(1)}$.

Теорема 3 (Верещагин, Чернов). $L_{O(1)} = L_{o(\Sigma)} = \mathfrak{I}$.

Третий подход к реализуемости, рассматриваемый в данной работе, использует более традиционный способ измерения сложности конечных множеств. А именно, фиксируем некоторую вычислимую нумерацию конечных множеств натуральных чисел и будем называть сложностью конечного множества натуральных чисел сложность его номера. Обозначим эту меру сложности $\tilde{K}(X)$. Легко видеть, что $K(X) \leqslant \tilde{K}(X) + O(1)$ для конечных непустых X. Заметим ещё, что для $\tilde{K}$, в отличие от K, выполнено $\tilde{K}(\varnothing) \neq \infty$, поэтому нам не требуется отдельно заботиться о непустоте подставляемых множеств при оценке сложности.

Определение 5. Пропозициональная формула Φ принадлежит множеству $\tilde{L}_{o(\Sigma)}$, если существует такая функция $f : [0,\infty) \to [0,\infty)$, что $f(x) = o(x)$ и для произвольных конечных множеств $X_1, \ldots, X_n$ выполнено $K(\Phi(X_1, \ldots, X_n)) \leqslant f(\tilde{K}(X_1) + \ldots + \tilde{K}(X_n))$.

В этом определении сложность $\Phi(X_1, \ldots, X_n)$ должна измеряться как сложность минимального элемента, поскольку это множество, как правило, бесконечно. В отличие от предыдущих определений, здесь неочевидно, что $\tilde{L}_{o(\Sigma)}$ является логикой (сомнительна замкнутость относительно правила подстановки). Тем не менее можно доказать такую теорему.

Теорема 4 (Верещагин, Чернов). $\tilde{L}_{o(\Sigma)} = \mathfrak{I}$.

Для наглядности представим описанные соотношения на двух диаграммах. Из ранее известных результатов и непосредственно из определений можно усмотреть следующее ($A \longrightarrow B$ обозначает включение $A \subseteq B$).

$$\begin{tikzcd}
\mathfrak{Int} \arrow[r] & L_{\mathrm{abs}} \arrow[r] \arrow[d] & \mathfrak{R}_{\mathrm{const}} \arrow[r] \arrow[d] & \mathfrak{R}_{\mathrm{eff}} \arrow[r] & \mathfrak{R} \arrow[d] \\
 & L_{O(1)} \arrow[r] \arrow[d] & \mathfrak{R}_{O(1)} \arrow[r] \arrow[d] & \ldots \arrow[r] & \mathfrak{R}_{\mathrm{w}} \\
 & L_{o(\Sigma)} \arrow[r] & \tilde{L}_{o(\Sigma)} & &
\end{tikzcd}$$

Наши результаты позволяют значительно упростить эту схему, превратив часть включений в равенства.

$$\mathfrak{Int} \subset L_{\mathrm{abs}} \subseteq \mathfrak{R}_{\mathrm{const}} \subseteq \mathfrak{R}_{\mathrm{eff}} \subseteq \mathfrak{R} \subset \mathfrak{R}_{\mathrm{w}} = \mathfrak{R}_{O(1)} = L_{O(1)} = L_{o(\Sigma)} = \tilde{L}_{o(\Sigma)} = \mathfrak{I}$$

Опишем дальнейший план статьи. Доказательства теорем 2, 3 и 4, как и принадлежащее Плиско доказательство теоремы 1, опираются на полученную в 1962 году Ю. Т. Медведевым характеризацию логик с интуиционистским позитивным фрагментом. В следующем параграфе мы приведём доказательство соответствующей теоремы (принадлежащее Скворцовым), поскольку сам Медведев только сформулировал её в [3], опустив доказательство, и за прошедшие сорок лет этот пробел так и не был устранён. В параграфе 3 сначала приводится подробный разбор простейших свойств введённых реализуемостей и соотношений между ними, а затем доказываются теоремы 2, 3 и 4.

2. Характеризация логик с интуиционистским позитивным фрагментом

2.1. В статье [3], посвящённой финитным задачам, Ю. Т. Медведев предложил удобный критерий, позволяющий определить, когда все позитивные формулы данной суперинтуиционистской логики выводимы в $\mathfrak{Int}$. С помощью этого критерия Медведев доказал, что логика финитных задач имеет интуиционистский позитивный фрагмент.

Определение 6 (Медведев). *Критическая импликация* — позитивная формула вида[4]

$$J = \bigwedge_{i=1}^{k} ((P_i \to Q_i) \to Q_i) \to R\,,$$

где P_i — конъюнкции переменных, Q_i и R — дизъюнкции переменных, причём при любом i формулы P_i и Q_i не имеют общих переменных, а каждая из формул P_i, Q_i, R содержит хотя бы одну переменную.

Легко показать (это будет сделано ниже, см. пример перед леммой 4), что все критические импликации не выводятся в $\mathfrak{Int}$.

Теорема 5 (Медведев,1962). *Пусть Φ — позитивная формула, $\mathfrak{Int} \nvdash \Phi$. Тогда существует такая критическая импликация J, что $(\mathfrak{Int} + \Phi) \vdash J$.*

На самом деле нам потребуется несколько более сильное утверждение. Для каждого натурального $n > 0$ фиксируем самую слабую[5] критическую импликацию в переменных $p_1, \ldots, p_n$:

$$J_n = \bigwedge_{\varnothing \neq E \subset \{1,\ldots,n\}} ((\bigwedge_{j \notin E} p_j \to \bigvee_{i \in E} p_i) \to \bigvee_{i \in E} p_i) \to \bigvee_{i=1}^{n} p_i\,.$$

В частности, $J_1 = p_1$.

Теорема 6. *Пусть $\Phi(q_1, \ldots, q_m)$ — позитивная формула и $\mathfrak{Int} \nvdash \Phi$. Тогда $\mathfrak{Int} \vdash (\Phi^* \to J_n)$ для некоторого $n > 0$, где Φ^* — результат подстановки вместо переменных $q_1, \ldots, q_m$ некоторых формул вида $\vee(\wedge p_i)$, где p_i — переменные критической импликации J_n.*

Чтобы пояснить соотношение теорем 5 и 6, напомним следующий вариант теоремы дедукции для суперинтуиционистских логик: $(L + \Phi) \vdash \Psi$ тогда и только тогда, когда $L \vdash (\Phi_1^* \wedge \ldots \wedge \Phi_k^* \to \Psi)$ для некоторых подстановочных примеров $\Phi_1^*, \ldots, \Phi_k^*$ формулы Φ. В нашем случае удаётся обойтись только одним подстановочным примером специального вида. Отметим еще, что из указанных теорем можно заключить следующее.

[4] Для критических импликаций и их подформул сохранены обозначения Медведева.

[5] В том смысле, что $\mathfrak{Int} \vdash J \to J_n$ для любой критической импликации J в тех же переменных.

Следствие 1. *Для суперинтуиционистской логики L следующие условия эквивалентны:*

- *логика L имеет интуиционистский позитивный фрагмент;*
- *в L невыводима ни одна критическая импликация;*
- $\forall n \quad (L \nvdash J_n)$.

Отметим, что аналогичная характеризация суперинтуиционистских логик с интуиционистским бездизъюнктным фрагментом (через невыводимость формул из некоторой счётной совокупности) доказана в [13]. Впервые о существовании такого рода результата заявил Медведев в [4]; впрочем, он даже не сформулировал, как выглядит упомянутый им аналог критических импликаций для бездизъюнктного случая.

Для доказательства основных результатов о слабой реализуемости нам понадобится ещё одна характеризация логик с интуиционистским позитивным фрагментом, полученная Янковым в [14].

Теорема 7 (Янков,1968). *Суперинтуиционистская логика L имеет интуиционистский позитивный фрагмент тогда и только тогда, когда $L \subseteq \mathfrak{J}$, где $\mathfrak{J} = \mathfrak{Int} + (\neg p \vee \neg\neg p)$ — логика Янкова.*

Иными словами, логика $\mathfrak{J}$ есть наибольшая логика с интуиционистским позитивным фрагментом. Этот критерий удобен для анализа логик, заданных аксиоматически (заметим, что логика $\mathfrak{J}$ разрешима). Наоборот, критерий Медведева приспособлен для логик, заданных семантически (а именно таковы все логики реализуемости). Мы используем эти критерии по следующей схеме: с помощью критерия Медведева доказываем, что исследуемая логика L имеет интуиционистский позитивный фрагмент, а затем из критерия Янкова заключаем, что $L \subseteq \mathfrak{J}$.

2.2. *Доказательство* теоремы 6 требует введения нескольких вспомогательных понятий.

Определение 7. *Шкалой Крипке F* называется частично упорядоченное множество с наименьшим элементом 0_F. *Конусом* называется подмножество $F^u \rightleftharpoons \{v \in F \mid u \leqslant v\}$. Подмножество $a \subseteq F$ называется *открытым*, если $\forall u \in a\ (F^u \subseteq a)$.

Семейство $H(F)$ всех открытых подмножеств шкалы F, упорядоченное по включению, образует гейтингову алгебру с операциями теоретико-множественного пересечения $\cap$, объединения $\cup$, импликацией $(a \to b) \rightleftharpoons \{u \in F \mid F^u \cap a \subseteq b\}$, наибольшим элементом $\mathbf{1} = F$ и наименьшим $\mathbf{0} = \varnothing$. Сопоставив связкам $\wedge$, $\vee$, $\to$ и константе $\perp$ операции $\cap$, $\cup$, $\to$ и элемент $\mathbf{0}$, для любой формулы $\Psi(p_1, \dots, p_k)$ и множеств $a_1, \dots, a_k \in H(F)$ можно определить $\Psi(a_1, \dots, a_k) \in H(F)$.

Логикой $L(F)$ шкалы F называется множество формул, общезначимых в алгебре $H(F)$, то есть $L(F) \rightleftharpoons \{\Phi(p_1, \dots, p_k) \mid \forall a_1, \dots, a_k \in H(F) \quad \Phi(a_1, \dots, a_k) = \mathbf{1}\}$. Если $\Phi \notin L(F)$, то говорят, что Φ *опровергается* на шкале F. Известно, что $L(F)$ является суперинтуиционистской логикой.

Схема доказательства теоремы 6 следующая: в леммах 1 и 2 будет доказано, что невыводимые в $\mathfrak{Int}$ позитивные формулы могут быть опровергнуты на конечных шкалах Крипке специального вида; леммы 3 и 4 показывают, что эти шкалы в некотором смысле полностью характеризуются критическими импликациями (а именно, критическая импликация выводится в $\mathfrak{Int}$ из любой опровержимой на соответствующей шкале позитивной формулы).

Определение 8. Сюръективное отображение $h : F \to F'$ называется *p-морфизмом* шкалы F на шкалу F', если

1) $u \leqslant v$ влечёт $h(u) \leqslant' h(v)$,

2) $h(u) \leqslant' w$ влечёт $\exists v\, (u \leqslant v, h(v) = w)$,

где $\leqslant$ и $\leqslant'$ — упорядочения шкал F и F' соответственно.

Иначе говоря, это определение означает, что $h(F^u) = (F')^{h(u)}$ для всех $u \in F$, то есть образ конуса есть конус. Отметим также, что сюръективность h равносильна $h(0_F) = 0_{F'}$.

Легко понять, что если h есть p-морфизм F на F', то h^{-1} есть изоморфное вложение алгебры $H(F')$ в $H(F)$. Таким образом, верен следующий факт:

(I) Если существует p-морфизм F на F', то $L(F) \subseteq L(F')$.

Как известно (см. напр. [15]), логика $\mathfrak{Int}$ полна относительно конечных шкал, то есть $\mathfrak{Int} = \bigcap\{L(F) \mid F$ — конечная шкала Крипке$\}$. Ясно, что каждая конечная линейно упорядоченная шкала F' есть p-морфный образ некоторой конечной не линейно упорядоченной шкалы, например, шкалы F, полученной добавлением к F' второго максимального элемента. Таким образом, имеем следующее тривиальное усиление теоремы полноты для $\mathfrak{Int}$:

(II) $\mathfrak{Int} = \bigcap\{L(F) \mid F$ конечна и не линейно упорядочена$\}$.

Пусть a_0 есть собственное (не равное F) открытое подмножество шкалы F. Рассмотрим шкалу $(F \setminus a_0)$, получаемую удалением из F точек множества a_0 с сохранением порядка на оставшихся точках. При этом отображение $g(a) = a \cup a_0$ есть изоморфное вложение позитивного редукта алгебры $H(F \setminus a_0)$ в $H(F)$, так как g сохраняет $\cup$, $\cap$, $\to$ и единицу алгебры, хотя, разумеется, не сохраняет нуль (то есть отрицание): $g(\varnothing) = a_0$. Отсюда получаем:

(III) Если a_0 — открытое подмножество F, то $L_\Pi(F) \subseteq L_\Pi(F \setminus a_0)$, где L_Π — позитивный фрагмент логики L.

Определение 9. Каждому непустому конечному множеству F сопоставим шкалу Крипке $\sigma(F) \rightleftharpoons \{E \mid E \subset F\}$ — семейство собственных подмножеств F, упорядоченное по включению, с наименьшим элементом $\varnothing$. Положим $\sigma_n = \sigma(\{1, \ldots, n\})$.

Ясно, что для любого F шкала $\sigma(F)$ изоморфна σ_n, где n — количество элементов F.

Лемма 1. *Пусть F — конечная не линейно упорядоченная шкала Крипке. Тогда существует p-морфизм $h : (\sigma(F) \setminus a_0) \to F$, где a_0 — некоторое открытое подмножество $\sigma(F)$.*

Доказательство (Д. П. Скворцов). Возьмём

$$\begin{array}{rcl} a_0 & = & \{E \subset F \mid\ E \text{ не линейно упорядочено}\}, \\ \sigma(F) \setminus a_0 & = & \{E \subset F \mid\ E \text{ линейно упорядочено}\}. \end{array}$$

Открытость a_0 очевидна. Положим $h(\varnothing) = 0_F$, и $h(E)$ — наибольший элемент E для $E \neq \varnothing$. Отображение h сюръективно: если $u \in F$, то $u = h(\{u\})$. Проверим остальные свойства p-морфизма. Если $E \subseteq E'$, то очевидно $h(E) \leqslant h(E')$. Если $h(E) = u \leqslant w$, то $w = h(E')$ для $E' = E \cup \{w\}$ и $E \subseteq E'$ (здесь $E' \in \sigma(F)$, иными словами, $E' \neq F$, поскольку E' линейно упорядочено, а F — нет). $\square$

Лемма 2. *Пусть Φ — позитивная формула, $\mathfrak{Int} \nvdash \Phi$, тогда $\Phi \notin L(\sigma_n)$ для некоторого $n > 0$.*

Доказательство. Пусть Φ — позитивная формула, $\mathfrak{Int} \nvdash \Phi$. Тогда ввиду (II) $\Phi \notin L(F)$ для некоторой конечной не линейно упорядоченной шкалы F. Из (I) и предыдущей леммы имеем $\Phi \notin L(\sigma(F) \setminus a_0)$, а из (III) следует, что $\Phi \notin L(\sigma(F))$, и значит, $\Phi \notin L(\sigma_n)$ при n равном количеству элементов F. $\square$

Сделаем небольшое замечание о роли доказанной леммы. Известно, что логика финитных задач Медведева LM совпадает с $\bigcap\limits_{n>0} L(\sigma_n)$ (это по сути доказано в [5], хотя там изложение ведётся в терминах брауэровых алгебр, а не шкал Крипке). Поэтому лемма 2 эквивалентна утверждению, что логика финитных задач имеет интуиционистский позитивный фрагмент[6]. Последнее легко следует из теоремы 5 (см. [3]). С другой стороны, мы далее показываем, как из леммы 2 вывести теорему 6. Поэтому можно сказать, что лемма 2, теорема 5 (или 6) и тот факт, что логика финитных задач имеет интуиционистский позитивный фрагмент, в некотором смысле эквивалентны.

После такого отступления продолжим изложение доказательства теоремы 6.

2.3. Янков в [17] ввёл понятие характеристической формулы $X(F)$ для конечной шкалы F. Мы используем некоторую модификацию формулы $X(F)$, приспособленную для анализа позитивных формул.

Определение 10. Пусть F — конечная шкала Крипке, и элементам a алгебры $H(F)$ сопоставлены различные пропозициональные переменные q_a. *Позитивной характеристической формулой шкалы F* назовём формулу

$$X_\Pi(F) = Y_F \to q_\omega ,$$

[6] Доказательства этого факта содержатся в [6] и в [16]. В данной статье приведено ещё одно доказательство, возможно, более простое и ясное, чем упомянутые.

где $\omega \rightleftharpoons F \setminus \{0_F\}$ — наибольший неединичный элемент алгебры $H(F)$, а Y_F — конъюнкция всех формул вида

$$\begin{array}{rcl} q_a \wedge q_b & \leftrightarrow & q_{a\cap b}, \\ q_a \vee q_b & \leftrightarrow & q_{a\cup b}, \\ (q_a \to q_b) & \leftrightarrow & q_{a\to b}, \end{array}$$

где $a, b \in H(F)$.

Следующая лемма (аналог теоремы 2 из [17]) объясняет, почему формула $X_\Pi(F)$ названа характеристической.

Лемма 3. *Пусть Φ — позитивная формула, F — произвольная конечная шкала Крипке. Тогда $\Phi \notin L(F) \Leftrightarrow (\mathfrak{Int} + \Phi) \vdash X_\Pi(F)$. Более того, для любых $a_1, \ldots, a_k \in H(F)$, таких, что $\Phi(a_1, \ldots, a_k) \neq \mathbf{1}$, выполнено $\mathfrak{Int} \vdash \Phi(q_{a_1}, \ldots, q_{a_k}) \to X_\Pi(F)$.*

Доказательство. Ясно, что $X_\Pi(F) \notin L(F)$, поскольку при оценке переменных q_a соответствующими элементами a в алгебре $H(F)$ формула $X_\Pi(F)$ принимает значение ω. Таким образом, если $(\mathfrak{Int}+\Phi) \vdash X_\Pi(F)$, то $\Phi \notin L(F)$.

Обратно, пусть $\Phi \notin L(F)$. Тогда для некоторых элементов $a_1, \ldots, a_k$ алгебры $H(F)$ получим, что $\Phi(a_1, \ldots, a_k) = a_0 \neq \mathbf{1}$. Возьмём произвольные $a_1, \ldots, a_k$ с этим свойством. Ясно, что $\mathfrak{Int} \vdash Y_F \to (\Phi(q_{a_1}, \ldots, q_{a_k}) \leftrightarrow q_{a_0})$ (индукция по построению Φ). Так как $a_0 \leqslant \omega$ в $H(F)$, то $a_0 \to \omega = \mathbf{1} = \mathbf{1} \to \mathbf{1}$, $\mathfrak{Int} \vdash Y_F \to ((q_{a_0} \to q_\omega) \leftrightarrow (q_\mathbf{1} \to q_\mathbf{1}))$, и $\mathfrak{Int} \vdash Y_F \to (q_{a_0} \to q_\omega)$. Поэтому $\mathfrak{Int} \vdash \Phi(q_{a_1}, \ldots, q_{a_k}) \to X_\Pi(F)$ и $(\mathfrak{Int} + \Phi) \vdash X_\Pi(F)$. $\square$

Прежде чем двигаться дальше, разберём **пример**, поясняющий основную идею доказательства и демонстрирующий связь шкал σ_n и критических импликаций. А именно, докажем, что произвольная критическая импликация J в переменных $p_1, \ldots, p_n$ опровергается в шкале σ_n (причём даже при единой оценке для всех таких J). Переменную p_j оценим открытым множеством $a_j = \{E \subset \{1, \ldots, n\} \mid j \in E\}$. При этом значение R отлично от $\mathbf{1}$, так как $\varnothing \notin a_j$ для всех j. Значение же $((P_i \to Q_i) \to Q_i)$ равно $\mathbf{1}$, поскольку $(P_i \to Q_i)(a_1, \ldots, a_n) = Q_i(a_1, \ldots, a_n)$. Действительно, пусть $P_i = \bigwedge_{j\in E'} p_j$, $Q_i = \bigvee_{j\in E''} p_j$, $E' \cap E'' = \varnothing$, и пусть $E \notin \bigvee_{j\in E''} a_j$. Тогда $E \cap E'' = \varnothing$ и $(E \cup E') \cap E'' = \varnothing$. Поэтому $(E \cup E') \notin \bigvee_{j\in E''} a_j$ и $(E \cup E') \in \bigwedge_{j\in E'} a_j$, а значит, $E \notin (\bigwedge_{j\in E'} a_j \to \bigvee_{j\in E''} a_j)$. Таким образом, $(P_i \to Q_i)(a_1, \ldots, a_n) \subseteq Q_i(a_1, \ldots, a_n)$ (обратное включение тривиально).

Лемма 4. $(\mathfrak{Int} + X_\Pi(\sigma_n)) \vdash J_n$ *для любого $n > 0$. Более того, $\mathfrak{Int} \vdash (X^*_\Pi(\sigma_n) \to J_n)$, где $X^*_\Pi(\sigma_n)$ есть подстановочный пример $X_\Pi(\sigma_n)$, получаемый при подстановке $\top$ вместо $q_\mathbf{1}$ и $\bigvee_{E\in a}(\bigwedge_{i\in E} p_i)$ вместо остальных переменных q_a формулы $X_\Pi(\sigma_n)$ (вместо $q_\varnothing$ подставляется $\bigwedge\limits_{i=1}^{n} p_i$), $p_1, \ldots, p_n$ — переменные J_n.*

Доказательство (Е. З. Скворцова). Для краткости положим $F = \sigma_n$. Каждой точке $E \subseteq \{1, \ldots, n\}$ шкалы F сопоставим формулу P_E: $P_\varnothing = \top$, $P_E = \bigwedge\limits_{i\in E} p_i$ для $\varnothing \neq E \subseteq \{1, \ldots, n\}$ (в частности, $P_{\{i\}} = p_i$). Каждое непустое открытое множество $a \in H(F)$ можно представить в виде $a = F^{E_1} \cup \ldots \cup F^{E_k}$, где $\{E_1, \ldots, E_k\}$ — антицепь минимальных по включению элементов a; положим $Q_a = \bigvee_{s=1}^{k} P_{E_s}$ (в частности, $Q_{F^E} = P_E$ для $E \in F$, $Q_F = P_\varnothing = \top$, $Q_\omega = \bigvee_{i=1}^{n} P_{\{i\}} = \bigvee_{i=1}^{n} p_i$). Положим также $Q_\varnothing = P_{\{1,\ldots,n\}} = \bigwedge_{i=1}^{n} p_i$ (заметим, что $\varnothing = \mathbf{0} = \bigcap_{i=1}^{n} F^{\{i\}}$ в $H(F)$, а $Q_\varnothing = \bigwedge_{i=1}^{n} P_{\{i\}}$). Для единообразия дальнейших вычислений удобно обозначить $F^{\{1,\ldots,n\}} = \varnothing$, тогда при любом $E \subseteq \{1, \ldots, n\}$ верно $Q_{F^E} = P_E$ и $F^E = \{E' \in F \mid E \subseteq E'\}$.

В дальнейшем будут использованы следующие очевидные соотношения:

(a) $\mathfrak{Int} \vdash (P_E \wedge P_{E'} \leftrightarrow P_{E \cup E'})$ для $E, E' \subseteq \{1, \ldots, n\}$;

(b) $\mathfrak{Int} \vdash (P_E \to P_{E'})$ при $E' \subseteq E$;

(c) $\mathfrak{Int} \vdash (Q_a \leftrightarrow \bigvee_{E \in a} P_E)$ для $a \in H(F)$, $a \neq \varnothing$;

(d) $\mathfrak{Int} \vdash (Q_\varnothing \to Q_a)$ для $a \in H(F)$.

Обозначим через X^* результат подстановки формул Q_a вместо переменных q_a в $X_\Pi(F)$. Тогда $X^* = Y^* \to \bigvee_{i=1}^{n} p_i$, где Y^* есть конъюнкция следующих формул (для всех $a, b \in H(F)$):

$$(Q_a \wedge Q_b) \quad \leftrightarrow \quad Q_{a \cap b} \tag{1}$$

$$(Q_a \vee Q_b) \quad \leftrightarrow \quad Q_{a \cup b} \tag{2}$$

$$(Q_a \to Q_b) \quad \leftrightarrow \quad Q_{a \to b} \tag{3}$$

Теперь надо убедиться, что $\mathfrak{Int} \vdash (X^* \to J_n)$. Поскольку заключения формул X^* и J_n совпадают, то достаточно проверить, что из посылки J_n следует посылка X^*, то есть $\mathfrak{Int} \vdash (\bigwedge_{\varnothing \neq E \subset \{1,\ldots,n\}} Z_E \to C)$ для всех конъюнктивных членов C из Y^*, где $Z_E = (\bigwedge_{j \notin E} p_j \to \bigvee_{i \in E} p_i) \to \bigvee_{i \in E} p_i$.

Ввиду (c), формулы (2) непосредственно выводимы в $\mathfrak{Int}$: $(\bigvee_{E \in a} P_E) \vee (\bigvee_{E \in b} P_E) \leftrightarrow (\bigvee_{E \in a \cup b} P_E)$. Выводимость формул (1) тоже легко доказать: из (a) и (c) имеем $Q_a \wedge Q_b \leftrightarrow (\bigvee_{E \in a} P_E) \wedge (\bigvee_{E' \in b} P_{E'}) \leftrightarrow (\bigvee_{E \in a, E' \in b} P_E \wedge P_{E'}) \leftrightarrow (\bigvee_{E \in a, E' \in b} P_{E \cup E'}) \leftrightarrow (\bigvee_{E \in a, E' \in b} Q_{F^{E \cup E'}}) \leftrightarrow Q_{a \cap b}$, где последняя эквивалентность следует из ранее доказанного соотношения для дизъюнкции и того, что $a \cap b = (\bigcup_{E \in a} F^E) \cap (\bigcup_{E' \in b} F^{E'}) = \bigcup_{E \in a, E' \in b} (F^E \cap F^{E'}) = \bigcup_{E \in a, E' \in b} F^{E \cup E'}$ в $H(F)$. Вырожденные случаи, когда a или b равно $\varnothing$, очевидны с учётом (d).

Осталось разобрать формулы (3). Положим $a_E = F^E = \bigcap_{i \in E} F^{\{i\}}$ и $b_E = \bigcup_{i \in E} F^{\{i\}}$, где $\varnothing \neq E \subset \{1, \ldots, n\}$. Соответственно, $Q_{a_E} = P_E = \bigwedge_{i \in E} p_i$ и $Q_{b_E} = \bigvee_{i \in E} p_i$. Каждое a из $H(F)$, кроме $\mathbf{0}$ и $\mathbf{1}$, представимо как объединение a_E, а каждое b, кроме $\mathbf{1}$, представимо как пересечение $b_{E'}$ (в частности, $\varnothing = \bigcap_{i=1}^{n} b_{\{i\}}$). При этом, ввиду выводимости (2) и (1), формулы Q_a и Q_b

эквивалентны (в $\mathfrak{Int}$) соответственно дизъюнкции и конъюнкции формул вида Q_{a_E} и $Q_{b_{E'}}$. Также, поскольку $\mathfrak{Int} \vdash (\vee_i \Phi_i \to \wedge_i \Psi_j) \leftrightarrow \wedge_{ij}(\Phi_i \to \Psi_j)$, формула $(Q_a \to Q_b)$ эквивалентна конъюнкции формул $(Q_{a_E} \to Q_{b_{E'}})$, а множество $(a \to b)$ равно пересечению соответствующих $(a_E \to b_{E'})$, так как в алгебре $H(F)$ выполнены все интуиционистские законы. Итак, достаточно вывести формулы (3) для случая $a = a_E$, $b = b_{E'}$.

Если $E \cap E' \neq \varnothing$, то, во-первых, $\mathfrak{Int} \vdash (Q_{a_E} \to Q_{b_{E'}})$, а во-вторых, $a_E \subseteq b_{E'}$ (так как $F^E \subseteq F^{\{i\}}$ для $i \in E \cap E'$), то есть $a_E \to b_{E'} = \mathbf{1}$ и $Q_{a_E \to b_{E'}} = \top$.

Пусть теперь $E \cap E' = \varnothing$. Тогда $a_E \to b_{E'} = b_{E'}$ в алгебре $H(\sigma_n)$. Действительно, если $E'' \notin b_{E'}$, то есть $\forall i \in E'\ (E'' \notin F^{\{i\}})$, то $E' \cap E'' = \varnothing$, $(E \cup E'') \cap E' = \varnothing$, поэтому $E'' \subseteq E \cup E'' \in (a_E \setminus b_{E'})$, а значит, $E'' \notin (a_E \to b_{E'})$. Далее, $Z_{E'}$ влечет $(\bigwedge\limits_{j \in E} p_j \to \bigvee\limits_{i \in E'} p_i) \to \bigvee\limits_{i \in E'} p_i$, так как $E \subseteq \{1, \ldots, n\} \setminus E'$, и следовательно, $\mathfrak{Int} \vdash (Z_{E'} \to [(Q_{a_E} \to Q_{b_{E'}}) \leftrightarrow Q_{b_{E'}}])$.

Оставшиеся недоразобранными вырожденные случаи тривиальны. Если $b = \mathbf{1}$, то $(a \to b) = \mathbf{1}$, и $Q_b = Q_{a \to b} = \top$. Если $a = \mathbf{1}$, то $Q_a = \top$, $(a \to b) = b$, и $\mathfrak{Int} \vdash (Q_a \to Q_b) \leftrightarrow Q_b$. Наконец, случай $a = \mathbf{0} = \varnothing$, $a \to b = \mathbf{1}$, обеспечен ввиду (d). □

Теорема 6 вытекает из лемм 2, 3 и 4, только необходимо сделать одно небольшое, но существенное замечание. В лемме 4, в отличие от теоремы 6, вместо одной из переменных (а именно, $q_{\mathbf{1}}$) подставляется константа $\top$. Покажем, что можно считать, что $\top$ не подставляется вместо исходных переменных формулы Φ. Действительно, пусть $\Phi(\tilde{q}_1, \ldots, \tilde{q}_m)$ — позитивная формула и $\mathfrak{Int} \nvdash \Phi$. Используя лемму 2, выберем такое n, что $\Phi \notin L(\sigma_{n-1})$. Возьмём шкалу $F_0 = \sigma_n$ и её конус F', изоморфный σ_{n-1}. Тогда $\Phi(a'_1, \ldots, a'_k) \neq \mathbf{1}$ в $H(F_0)$ для соответствующих $a'_1, \ldots, a'_k \in H(F') \subseteq H(F_0) \setminus \mathbf{1}$. Именно к этим $a'_1, \ldots, a'_k$ применим лемму 3. Теперь, при применении леммы 4, вместо исходных переменных $\tilde{q}_1, \ldots, \tilde{q}_m$ в формулу Φ будут подставлены формулы $Q_{a'_i} \neq Q_{\mathbf{1}} = \top$. Теорема полностью доказана.

Заметим ещё, что $(\mathfrak{Int} + J_n) \vdash X_\Pi(\sigma_n)$ по лемме 3 (так как $J_n \notin L(\sigma_n)$), поэтому J_n и $X_\Pi(\sigma_n)$ дедуктивно эквивалентны, то есть формулу J_n тоже естественно было бы назвать характеристической для шкалы σ_n. Чрезвычайной элегантностью и простотой своей структуры критические импликации обязаны тому, что алгебры $H(\sigma_n)$ являются свободными дистрибутивными решётками с n образующими и присоединённым наибольшим элементом (на это фактически указывал ещё Медведев в [5]).

3. Слабая реализуемость

3.1. Сначала мы разберём подробнее факты, названные во введении очевидными, в частности, обоснуем включения, изображённые на первой диаграмме, и то, что построенные множества действительно являются логиками.

Замкнутость множеств $\mathfrak{R}_{O(1)}$ и $\mathfrak{R}_{\mathrm{w}}$ относительно правила подстановки следует из того, что подстановка в формулу $\Phi(\Psi_1, \ldots, \Psi_k)$ арифметических множеств $A_1, \ldots, A_n$ эквивалентна подстановке в формулу Φ арифметических же множеств $\Psi_i(A_1, \ldots, A_n)$, поэтому реализуемость полученной по правилу подстановки формулы $\Phi(\Psi_1, \ldots, \Psi_k)$ непосредственно следует из реализуемости Φ.

Для доказательства замкнутости относительно modus ponens достаточно заметить, что „кандидаты в реализацию" формулы Φ могут быть получены применением всех программ — „кандидатов в реализацию" $(\Psi \to \Phi)$ ко всем „кандидатам в реализацию" Ψ. Получающееся множество ответов остановившихся программ конечно и может быть задано арифметической формулой ограниченной сложности.

Включение $\mathfrak{R} \subseteq \mathfrak{R}_{\mathrm{w}}$ следует из того, определение $\mathfrak{R}$ получается из определения $\mathfrak{R}_{\mathrm{w}}$, если положить $i = 1$ и потребовать одноэлементности множеств $B(k)$. Аналогично, сужая определение $\mathfrak{R}_{\mathrm{w}}$ (потребовав, чтобы одно и то же $B(k) \equiv \{1, \ldots, C\}$ годилось для любых $A_1(x), \ldots, A_n(x)$), можно получить $\mathfrak{R}_{O(1)}$, поэтому $\mathfrak{R}_{O(1)} \subseteq \mathfrak{R}_{\mathrm{w}}$. Заменив в определении $\mathfrak{R}_{O(1)}$ требование $r \leqslant C$ на $r = C$, получим $\mathfrak{R}_{\mathrm{const}}$, следовательно, $\mathfrak{R}_{\mathrm{const}} \subseteq \mathfrak{R}_{O(1)}$. Как известно, $\mathfrak{Int} \subset \mathfrak{R}_{\mathrm{const}}$, поэтому $\mathfrak{R}_{O(1)}$ и $\mathfrak{R}_{\mathrm{w}}$ также являются суперинтуиционистскими логиками.

Перейдём теперь к $L_{O(1)}$, $L_{o(\Sigma)}$, $\tilde{L}_{o(\Sigma)}$. Вначале сделаем два замечания по поводу определений.

Во-первых, $\Phi \in L_{O(1)}$ означает, что существует такая константа C, что для произвольных множеств $X_1, \ldots, X_n$ выполнено $\Phi(X_1, \ldots, X_n) \cap \{x \mid K(x) \leqslant C\} \neq \varnothing$. В силу свойства 4 колмогоровской сложности существует число $C' = \max\{x \mid K(x) \leqslant C\}$, а в силу свойства 1, если $x \leqslant C'$, то $K(x) \leqslant \ell(C') + O(1)$. Поэтому определение $L_{O(1)}$ можно переформулировать так: пропозициональная формула $\Phi(p_1, \ldots, p_n)$ принадлежит $L_{O(1)}$, если существует такое натуральное число C, что для любых множеств $X_1, \ldots, X_n$ существует такое $r \leqslant C$, что $r \in \Phi(X_1, \ldots, X_n)$. Таким образом, логика $L_{O(1)}$ является „абсолютным" (то есть получаемым отказом от требования арифметичности) аналогом логики $\mathfrak{R}_{O(1)}$. Как следствие получаем два включения: $L_{O(1)} \subseteq \mathfrak{R}_{O(1)}$ и $L_{\mathrm{abs}} \subseteq L_{O(1)}$.

Во-вторых, суммирование в определении $L_{o(\Sigma)}$ ведётся только по непустым подставляемым множествам, и это существенно. Напомним, что $\Phi \in L_{o(\Sigma)}$, если существует функция $f : [0, \infty) \to [0, \infty)$, такая что $\lim_{x \to \infty} f(x)/x = 0$ и для произвольных множеств $X_1, \ldots, X_n$ выполнено $K(\Phi(X_1, \ldots, X_n)) \leqslant f(\sum\limits_{X_i \neq \varnothing} K(X_i))$. Если в последней сумме учитывать и бесконечные слагаемые (то есть пустые множества X_i), то потребуется как-то интерпретировать выражения $\infty \leqslant f(\infty)$ и $n \leqslant f(\infty)$ для натуральных n. Можно либо принять, что истинно неравенство $\infty \leqslant f(\infty)$, либо, считая $\infty \leqslant f(\infty)$ ложным, положить $f(\infty) \geqslant n$ для любого натурального n. В обоих случаях множество $L_{o(\Sigma)}$ получилось бы незамкнутым относительно правила подстановки: в первом случае $\neg\neg p \in L_{o(\Sigma)}$ и $\neg\neg\neg p \notin L_{o(\Sigma)}$, а во втором $\neg\neg p \vee q \vee \neg q \in L_{o(\Sigma)}$ и $\neg\neg\neg p \vee q \vee \neg q \notin L_{o(\Sigma)}$.

Обоснуем теперь оставшиеся включения. Очевидно, что $L_{O(1)} \subseteq L_{o(\Sigma)}$ и $\mathfrak{R}_{O(1)} \subseteq \tilde{L}_{o(\Sigma)}$ (все конечные множества арифметичны). Наконец, включение $L_{o(\Sigma)} \subseteq \tilde{L}_{o(\Sigma)}$ следует из того, что для непустых конечных множеств $K(X) \leqslant \tilde{K}(X) + O(1)$. Для доказательства этого неравенства заметим, что, зная номер конечного множества, можно вычислимо восстановить список всех его элементов, поэтому в соответствии со свойством 2 колмогоровской сложности $\tilde{K}(\{x_1, \ldots, x_n\}) \geqslant K(\langle x_1, \ldots, x_n \rangle) - O(1) \geqslant K(\min\{x_1, \ldots, x_n\}) -$

$O(1) \geqslant \min\{K(x_1), \ldots, K(x_n)\} - O(1) \geqslant K(\{x_1, \ldots, x_n\}) - O(1)$.

Замкнутость $L_{O(1)}$, $L_{o(\Sigma)}$, $\tilde{L}_{o(\Sigma)}$ относительно modus ponens обеспечена тем, что $K(\Phi) \leqslant K(\Psi \to \Phi) + K(\Psi) + O(\log(K(\Psi)))$ (это следует из свойств 5 и 2).

Замкнутость $L_{O(1)}$ относительно правила подстановки очевидна, а для $L_{o(\Sigma)}$ следует из упомянутой во введении оценки: для любой пропозициональной формулы $\Phi(p_1, \ldots, p_n)$ существует такая константа C, что для любых множеств $X_1, \ldots, X_n$, если $\Phi(X_1, \ldots, X_n) \neq \varnothing$, то

$$K(\Phi(X_1, \ldots, X_n)) \leqslant K(\bigwedge_{X_i \neq \varnothing} X_i) + O(1) \leqslant \sum_{X_i \neq \varnothing} K(X_i) + C \cdot \log \sum_{X_i \neq \varnothing} K(X_i)\,.$$

Второе неравенство следует из свойства 5. Чтобы доказать первое неравенство, для каждой формулы Φ мы индукцией по построению формулы определим такую вычислимую функцию f_Φ, что для любых таких множеств $X_1, \ldots, X_n$, что $\Phi(X_1, \ldots, X_n) \neq \varnothing$, выполнено: если $x_i \in X_i$ для $X_i \neq \varnothing$ и $x_i = *$ для $X_i = \varnothing$, то $f_\Phi(x_1, \ldots, x_n) \in \Phi(X_1, \ldots, X_n)$ (строго говоря, функция определена на некотором коде кортежа из натуральных чисел и звёздочек).

1) $\Phi(p_1, \ldots, p_n) = p_i$. Положим $f_\Phi(x_1, \ldots, x_n) = x_i$.

2) $\Phi(p_1, \ldots, p_n) = \bot$. Положим $f_\Phi(x_1, \ldots, x_n) = *$.

3) $\Phi = \Psi_1 \wedge \Psi_2$. Если $f_{\Psi_1} \neq *$ и $f_{\Psi_2} \neq *$ (здесь и далее у f подразумеваются аргументы $x_1, \ldots, x_n$), то $f_\Phi = \langle f_{\Psi_1}, f_{\Psi_2} \rangle$, иначе $f_\Phi = *$.

4) $\Phi = \Psi_1 \vee \Psi_2$. Если $f_{\Psi_1} \neq *$, то $f_\Phi = \langle 0, f_{\Psi_1} \rangle$; иначе если $f_{\Psi_2} \neq *$, то $f_\Phi = \langle 1, f_{\Psi_2} \rangle$, а в оставшемся случае $f_\Phi = *$.

5) $\Phi = \Psi_1 \to \Psi_2$. Если $f_{\Psi_2} \neq *$, то $f_\Phi = \lambda z. f_{\Psi_2}$; если $f_{\Psi_1} \neq *$ и $f_{\Psi_2} = *$, то $f_\Phi = *$; если же $f_{\Psi_1} = *$, то $f_\Phi = \lambda z.0$ (здесь $\lambda z.C$ — какая-нибудь программа, вычисляющая функцию, тождественно равную константе C).

Неравенство теперь следует из свойства 2 колмогоровской сложности.

Итак, мы доказали, что $L_{O(1)}$ и $L_{o(\Sigma)}$ являются суперинтуиционистскими логиками. О множестве $\tilde{L}_{o(\Sigma)}$ этого сказать пока нельзя по следующей причине: если подставляемая формула содержит импликацию, то порождаемое ею множество может быть бесконечно, поэтому для доказательства реализуемости $\Phi(\Psi_1, \ldots, \Psi_k)$ недостаточно просто сослаться на реализуемость Φ. Однако позже мы используем такой факт: *множество $\tilde{L}_{o(\Sigma)}$ замкнуто относительно подстановок формул, не содержащих импликаций (в частности, подстановок константы $\bot$).* Действительно, индукцией по построению формулы легко показать, что для любой не содержащей импликаций формулы Φ множество $\Phi(X_1, \ldots, X_n)$ конечно и его номер вычислимо восстанавливается по номерам конечных множеств $X_1, \ldots, X_n$. Поэтому (как следует из свойств 2 и 5 колмогоровской сложности) существует такая константа C, что для любых конечных множеств $X_1, \ldots, X_n$ верна оценка

$$\tilde{K}(\Phi(X_1, \ldots, X_n)) \leqslant \tilde{K}(X_1) + \ldots + \tilde{K}(X_n) + C \cdot \sum_{i=1}^{n} \log \tilde{K}(X_i)\,.$$

3.2. Приступим теперь к изучению соотношения между логикой Янкова и различными типами слабой реализуемости. Из критерия Янкова (теорема 7) и теоремы 1 следует, что логика (клиниевской) реализуемости $\mathfrak{R} \subseteq \mathfrak{J}$. Хорошо известно, что $\neg p \vee \neg\neg p \notin \mathfrak{R}$ (чтобы в этом убедиться, достаточно взять какое-нибудь неразрешимое множество K и рассмотреть такое арифметическое семейство $A(x)$, что $A(k) = \varnothing$ если и только если $k \in K$), и потому $\mathfrak{R} \neq \mathfrak{J}$.

Лемма 5.

1) $\neg p \vee \neg\neg p \in L_{O(1)}$*;*

2) $p \vee \neg p \notin L_{o(\Sigma)}$*;*

3) $p \vee \neg p \notin \mathfrak{R}_{\mathrm{w}}$*.*

Доказательство.

1) Если $X = \varnothing$, то $\neg X = \mathbb{N}$, а если $X \neq \varnothing$, то $\neg X = \varnothing$ и $\neg\neg X = \mathbb{N}$, поэтому $K(\neg X \vee \neg\neg X) \leqslant \max\{K(\langle 0,0\rangle), K(\langle 1,0\rangle)\} = O(1)$.

2) Положим $X = \{x \mid K(x) = n\}$. Тогда $K(X) = n$, $\neg X = \varnothing$, поэтому $K(X \vee \neg X) = K(\{0\} \times X) = n + O(1) \neq o(n)$ (так как $K(x) \leqslant K(\langle 0, x\rangle) + O(1)$).

3) Зафиксируем произвольное $i > 0$ и какую-нибудь арифметическую нумерацию $B_1(x), B_2(x), \ldots$ всех семейств множеств из Σ_i. Возьмём арифметическое семейство множеств $D(x) = \{r \mid \langle 0, r\rangle \notin B_x(x)\}$.

   Пусть некоторое семейство $B_k(x) \in \Sigma_i$ слабо реализует $D(x) \vee \neg D(x)$, то есть для любого m множество $B_k(m)$ конечно и $B_k(m) \cap (D(m) \vee \neg D(m)) \neq \varnothing$. Рассмотрим множество $D(k)$. Поскольку $B_k(k)$ конечно, множество $D(k)$ не может быть пустым, и поэтому $\neg D(k)$ пусто. Следовательно, $D(k) \vee \neg D(k) = \{\langle 0, r\rangle \mid r \in D(k)\}$, и $B_k(k) \cap (D(k) \vee \neg D(k)) = \{\langle 0, r\rangle \mid r \in D(k) \text{ и } \langle 0, r\rangle \in B_k(k)\} = \varnothing$. Таким образом, B_k не реализует $D \vee \neg D$, и формула $p \vee \neg p$ не принадлежит $\mathfrak{R}_{\mathrm{w}}$.

□

Из леммы, в частности, следует, что $L_{o(\Sigma)}$ и $\mathfrak{R}_{\mathrm{w}}$ строго содержатся в множестве классически истинных формул (поскольку если суперинтуиционистская логика L содержит классически ложную формулу, то она тривиальна, то есть содержит все формулы). Кроме того, в логике $L_{O(1)}$ верен слабый закон исключённого третьего, а потому $L_{O(1)}$, а значит, и $L_{o(\Sigma)}$, $\tilde{L}_{o(\Sigma)}$, $\mathfrak{R}_{O(1)}$, $\mathfrak{R}_{\mathrm{w}}$, содержат логику Янкова $\mathfrak{J}$.

3.3. Таким образом, для доказательства теорем 2 и 3 нам достаточно доказать, что логики $L_{o(\Sigma)}$ и $\mathfrak{R}_{\mathrm{w}}$ имеют интуиционистский позитивный фрагмент, а потому по критерию Янкова содержатся в $\mathfrak{J}$.

По теореме Медведева, для этого достаточно показать, что ни одна критическая импликация не принадлежит этим логикам. Основную роль в доказательстве играет следующая лемма. Будем говорить, что программа q *перечисляет* множество A, если $A = \{q(i) \mid i \in \mathbb{N}\}$. Программа q *коперечисляет* множество, если она перечисляет его дополнение.

Лемма 6. *Путь нам даны натуральное число $m \geqslant 1$ и программа q, перечисляющая некоторое множество M из не более чем 2^m натуральных чисел, а также критическая импликация J_n от n переменных. Тогда мы можем эффективно найти программы $a_1, \dots, a_n$, коперечисляющие некоторые непустые множества натуральных чисел $A_1, \dots, A_n$ такие, что множества M и $J_n(A_1, \dots, A_n)$ не пересекаются. При этом все элементы множеств $A_1, \dots, A_n$ не превосходят 2^{Cm}, где константа C зависит только от n (то есть от вида критической импликации).*

Доказательство. Сначала определим $A_1^0, \dots, A_n^0$ как множества натуральных чисел, меньших $K_1, \dots, K_n$ соответственно, где числа $K_1, \dots, K_n$ и такую константу C, что $K_1, \dots, K_n \leqslant 2^{Cm}$, подберём позднее. Затем будем постепенно удалять из них элементы с помощью некоторого алгоритма $\mathfrak{A}$, имеющего m, n, q как параметры. Мы будем обозначать через A_j^t ту часть A_j^0, которая осталась после выполнения шага t (это будет уточнено далее). Мы докажем, что ни одно из A_j^t не станет пустым и начиная с некоторого шага t_0 удаления прекратятся, то есть множества A_j^t перестанут изменяться. Предельные множества

$$A_j = A_j^{t_0} = \bigcap_t A_j^t$$

и будут искомыми.

Каждое из A_j^0 мы разобьём на 2^m множеств $A_{j1}^0, \dots, A_{j2^m}^0$ одинакового размера, и обозначим $A_{jl}^t = A_{jl}^0 \cap A_j^t$.

Напомним, что $J_n(p_1, \dots, p_n) = (\bigwedge_{i=1}^{I} ((P_i \to Q_i) \to Q_i) \to R$, где P_i — конъюнкции переменных p_j, а Q_i, R — дизъюнкции p_j. Обозначим через P_i^t, Q_i^t, R^t результат подстановки множеств A_j^t вместо переменных p_j (а через P_i, Q_i, R — результат подстановки A_j). Для упрощения обозначений мы будем считать, что элементы множеств Q_i^t и R^t имеют вид $\langle j, a\rangle$, где $a \in A_j^t$ и переменная p_j входит в соответствующую дизъюнкцию (такую модификацию легко обеспечить при помощи вычислимого преобразования, имеющего в качестве параметра число n).

Мы определим вспомогательные программы f_{ilr} для $i = 1, \dots, I$, $l = 1, \dots, 2^m$, $r = 1, 2, \dots$ Наша цель заключается в том, чтобы для всех $e \in M$ существовали такие $l = l(e)$, $r = r(e)$, что

$$f_{ilr} \in ((P_i \to Q_i) \to Q_i)$$

для всех $i \leqslant I$ и $e(\langle f_{1lr}, \dots, f_{Ilr}\rangle)$ либо не определено, либо определено и не принадлежит R. Результат работы программы f_{ilr} на исходном данном s будет вычисляться тем же алгоритмом $\mathfrak{A}$. При этом, пользуясь теоремой о неподвижной точке (см. напр. [2, § 66, теорема XXVII]), мы можем считать, что алгоритму известны все программы f_{ilr}. Действительно, поскольку результат, выдаваемый программой f_{ilr} на некотором входе s, вычисляется алгоритмом $\mathfrak{A}$ по данным s и i, l, r, m, n, q, а нумерация $U(e,x)$ является главной, чтобы изготовить программу f_{ilr}, достаточно знать программу для $\mathfrak{A}$ и значения i, l, r, m, n, q. Так как эти значения алгоритму известны, ему не хватает только знания своей собственной программы. Но одна из формулировок теоремы о неподвижной точке как раз и заключается в том, что, определяя алгоритм, можно считать известной его программу.

Алгоритм $\mathfrak{A}$ работает следующим образом. Мы перечисляем по шагам график функции $U(x, y)$. Будем считать, что на каждом шаге перечисления появляется ровно одно новое значение $U(x, y)$. Через U^t мы будем обозначать часть U, перечисленную на шагах $1, \ldots, t$. Положим также $s^t(x) = U^t(s, x)$, и через M^t обозначим часть M, порождённую на шагах $1, \ldots, t$, (то есть область значений функции q^t). После шага номер $t > 0$ перечисления графика U наш алгоритм будет выполнять последовательно 5 шагов, обозначаемых $5t + 1$, $5t + 2$, $5t + 3$, $5t + 4$, $5t + 5$.

Шаг $5t + 1$. Если на шаге t перечисления графика U множество M^t пополнилось новым элементом e, то полагаем $l(e)$ равным наименьшему из чисел $l = 1, \ldots, 2^m$, отличному от $l(e')$ для всех ранее появившихся элементов M, и полагаем $r(e) = t$. В дальнейшем $r(e)$ может увеличиваться, а $l(e)$ меняться не будет.

Шаг $5t + 2$. Если на шаге t перечисления графика U мы обнаружили, что для некоторого $e \in M^t$ значение $e^t(\langle f_{1l(e)r(e)}, \ldots, f_{Il(e)r(e)}\rangle)$ определено и равно, скажем, $\langle j, a\rangle$, то удаляем a из A_j^{t-1} (если оно там было). Назовём такую программу e ***опровергнутой*** (в дальнейшем она может перестать быть таковой). В начале мы считаем все программы неопровергнутыми.

Отметим, что удаления могли произойти для того e, которое было добавлено в M^t на шаге $5t + 1$, а также для конечного числа e, для которых на шагах $5(t - 1) + 4$ и $5(t - 1) + 5$ изменилось значение $r(e)$. Множества, которые состоят из элементов, оставшихся после выполнения всех удалений на этом шаге, и обозначаются A_j^t.

Шаг $5t+3$. Пусть для некоторых $i \leqslant I$ и s выполнено $s^t \in P_i^t \to Q_i^t$. Для каждого t все множества $A_1^t, \ldots, A_n^t$ будут непустыми, поэтому и P_i^t будут непустыми. Поскольку график U^t конечен, отсюда следует, что программ s с этим свойством лишь конечное число. Для всех таких i, s, всех $r \leqslant t$ и $l \leqslant 2^m$ мы определяем значение f_{ilr} на s следующим образом (если оно не было определено ранее). Пусть P_{il}^t обозначает результат подстановки множеств A_{jl}^t вместо p_j в P_i (ясно, что $P_{il}^t \subseteq P_i^t$), а $s(P_{il}^t)$ обозначает множество всех результатов работы программы s на входных кортежах из P_{il}^t. Мы подберём размеры множеств $A_1^0, \ldots, A_n^0$ таким образом, что для всех t будет выполнено

$$\begin{aligned} &|A_{jl}^t| > n|A_{j+1}^0| \quad \text{для всех } j < n, \\ &|A_{nl}^t| > 0 \end{aligned} \tag{4}$$

для всех $l \leqslant 2^m$. Из этого следует, что найдётся некоторый элемент $\langle j, a\rangle \in s(P_{il}^t) \subseteq Q_i^t$ со следующим свойством:

> Для всех $k < j$ существуют два кортежа из P_{il}^t, различающиеся в k-ой координате и отображаемые программой s в $\langle j, a\rangle$.

Действительно, если такого $\langle j, a\rangle$ нет, то выберем для каждого $\langle j, a\rangle \in s(P_{il}^t)$ такое $k < j$, что все кортежи из P_{il}^t, отображаемые s в $\langle j, a\rangle$, имеют одну и ту же k-ую координату. Количество таких кортежей не превосходит

$$|P_{il}^t|/|A_{kl}^t| < |P_{il}^t|/(n|A_j^t|)\,.$$

Поэтому количество кортежей из P_{il}^t, отображаемых s в $\{j\} \times A_j^t$, меньше $|P_{il}^t|/n$. Но каждый кортеж из P_{il}^t отображается в $Q_i^t = \bigcup_j \left(\{j\} \times A_j^t\right)$

(объединение берётся по всем j, для которых p_j входит в дизъюнкцию Q_i). Поэтому получается, что P^t_{il} имеет менее $n|P^t_{il}|/n$ элементов; противоречие.

В качестве значения f_{ilr} на s выбираем первый элемент $\langle j,a\rangle \in s(P^t_{il}) \subseteq Q^t_i$ с указанным свойством. Множество кортежей из P^t_{il}, отображаемых программой s в $\langle j,a\rangle$, мы будем называть *обоснованием значения* f_{ilr} на s.

Шаг $5t+4$. Для всех опровергнутых $e \in M^t$ и всех $i \leqslant I$ делаем следующее. Если после выполнения шага $5t+2$ программа $f_{il(e)r(e)}$ стала *некорректной*, то есть для некоторого s выполнено $s^t \in P^t_i \to Q^t_i$, но $f_{il(e)r(e)}(s) \notin Q^t_i$, то меняем значение $r(e)$, полагая его равным t. Программа e при этом объявляется неопровергнутой. Заметим, что если программа $f_{il(e)r(e)}$ стала некорректной, то для некоторого s на шагах $5t'+2$ с $t' \leqslant t$ было удалено $f_{il(e)r(e)}(s)$ и удален хоть один компонент каждого кортежа из обоснования значения $f_{il(e)r(e)}$ на s (иначе $s^t \notin P^t_i \to Q^t_i$). Поэтому такое событие будет происходить нечасто по сравнению с удалениями элементов (далее мы это уточним).

Шаг $5t+5$. Если на шаге $5t+2$ из-за удаления элемента a из A_j для некоторых s,i,l,r обоснование значения f_{ilr} на s уменьшилось (за счёт уменьшения P^t_{il}) или удалено само это значение, мы объявляем программу f_{ilr} *подозрительной* (так как повышаются шансы, что она станет в будущем некорректной). Для всех неопровергнутых $e \in M^t$ и всех $i \leqslant I$ таких, что программа $f_{il(e)r(e)}$ стала подозрительной, мы меняем значение $r(e)$, полагая его равным t. Заметим, что обоснования всех значений программ вида f_{ilt} не могли уменьшиться и сами значения не могли быть удалены на шаге $5t+2$ и тем более раньше, поскольку определение значений программы f_{ilt} впервые началось только на шаге $5t+3$. Поэтому перед выполнением любого шага $5t'+2$ для любой неопровергнутой программы $e \in M^{t'}$ и любого $i \leqslant I$ все программы $f_{il(e)r(e)}$ неподозрительны. Для опровергнутых программ значение $r(e)$ не меняется, даже если программа $f_{il(e)r(e)}$ стала подозрительной.

Описание алгоритма $\mathfrak{A}$ закончено.

Теперь достаточно доказать, что можно определить размеры $A^0_1,\dots,A^0_n$ так, для любого t будет выполнено (4). Действительно, допустим временно, что это уже доказано, и пусть t_0 есть номер шага, начиная с которого множества $A^t_1,\dots,A^t_n$ и M^t уже не меняются (такой шаг существует, поскольку множества $A^t_1,\dots,A^t_n$ и M^t конечны, причём все A^t_j непусты в силу (4)). Нам надо доказать, что множества M^{t_0} и $J_n(A^{t_0}_1,\dots,A^{t_0}_n)$ не пересекаются. Пусть $e \in M^{t_0}$. Значение $r(e)$ не меняется после шага t_0 перечисления U. При этом после выполнения каждого шага вида $5t'+3$ при $t' \geqslant t_0$ для всех s выполнена импликация

$$s^{t'} \in (P^{t_0}_i \to Q^{t_0}_i) \quad \Longrightarrow \quad f_{il(e)r(e)}(s) \text{ определено и принадлежит } Q^{t_0}_i\,.$$

Отсюда следует, что

$$f_{il(e)r(e)} \in (P^{t_0}_i \to Q^{t_0}_i) \to Q^{t_0}_i\,.$$

Допустим, что $e(\langle f_{1l(e)r(e)},\dots,f_{Il(e)r(e)}\rangle)$ определено и принадлежит R^{t_0}. Тогда на каком-то шаге $t' > t_0$ перечисления графика U мы обнаружим, что это значение определено и удалим $e(\langle f_{1l(e)r(e)},\dots,f_{Il(e)r(e)}\rangle)$ на шаге $5t'+2$; противоречие.

Для того, чтобы доказать неравенства (4) для подходящих мощностей $A_1^0, \ldots, A_n^0$, нам нужно оценить количество удалений элементов на шагах вида $5t+2$. Пусть N_k обозначает количество удалений на тех шагах вида $5t+2$, на которых удалялся элемент a из A_k^{t-1} (для значения $e^t(\langle f_{1l(e)r(e)}, \ldots, f_{Il(e)r(e)}\rangle) = \langle k, a\rangle$). Будем называть такие удаления *удалениями порядка* k. Мы докажем, что

$$N_k \leqslant 2^{m+1}(N_1 + \ldots + N_{k-1}) + 2^{m+1}\,.$$

Заметим, что при каждом удалении количество опровергнутых программ увеличивается на 1. Часть этих программ потом могут перестать быть опровергнутыми на шагах $5t'+4$. Обозначим через K_0 количество троек $\langle e, t_1, t_2\rangle$ таких, что на шаге $5t_1+2$ программа e стала опровергнутой, а потом впервые на шаге $5t_2+4$ перестала быть таковой. Тогда очевидно

$$N_1 + \ldots + N_n \leqslant K_0 + 2^m\,.$$

Оценим K_0. Чтобы для тройки $\langle e, t_1, t_2\rangle$ могло произойти указанное событие, должны существовать s,i такие, что на шагах *между* $5t_1+2$ и $5t_2+2$ удалено $f_{il(e)r(e)}(s)$ и из каждого кортежа из обоснования значения $f_{il(e)r(e)}$ на s удалён хоть один компонент. Фиксируем i, s для каждой такой тройки. Если на шаге $5t+2$ (где $t_1 \leqslant t \leqslant t_2$) произошло одно из указанных удалений, то мы будем говорить, что это удаление *связано* с тройкой $\langle e, t_1, t_2\rangle$, причем если это было удаление второго типа (удаление компонента кортежа из обоснования), то будем говорить, что это удаление *сильно связано* с тройкой $\langle e, t_1, t_2\rangle$. Разделим тройки $\langle e, t_1, t_2\rangle$ на три вида:

1) те, которые связаны хотя бы с одним удалением порядка меньше k;

2) те, которые связаны только с удалениями порядка k или больше, причём сильно связаны хоть с одним удалением порядка строго больше k;

3) те, которые связаны только с удалениями порядка k или больше, причём сильно связаны только с удалениями порядка k.

Количество троек первого типа не больше $2^m(N_1 + \ldots + N_{k-1})$. Действительно, для двух различных троек $\langle e, t_1, t_2\rangle$ и $\langle e, t_1', t_2'\rangle$ с одинаковым первым компонентом интервалы $[t_1, t_2]$ и $[t_1', t_2']$ не пересекаются. Если удаление на шаге $5t+2$ связано с тройкой $\langle e, t_1, t_2\rangle$, то $t_1 \leqslant t \leqslant t_2$, а поэтому оно не связано ни с одной другой тройкой $\langle e, t_1', t_2'\rangle$. Значит, общее количество троек, связанных с каждым удалением, не превосходит $|M| \leqslant 2^m$.

Количество троек второго типа не больше $N_{k+1} + \ldots + N_n$. Действительно, любое удаление может быть сильно связано только с одной тройкой, поскольку для различных e_1, e_2 и для любого j множества $A^t_{jl(e_1)}$ и $A^t_{jl(e_2)}$ не пересекаются, поэтому невозможно удалить одновременно компоненту из кортежа некоторого обоснования $f_{i'l(e_1)r(e_1)}$ и некоторого обоснования $f_{i''l(e_2)r(e_2)}$.

Количество троек третьего типа не больше $N_k/2$. Чтобы доказать это, достаточно установить, что каждая такая тройка $\langle e, t_1, t_2\rangle$ сильно связана по меньшей мере с двумя удалениями порядка k. Пусть $f_{il(e)r(e)}(s)$ имеет вид $\langle j, a\rangle$, то есть переменная p_j входит в Q_i. Удаления компонентов кортежей из обоснования значения $f_{il(e)r(e)}$ на s имеют порядок k, поэтому переменная p_k входит в P_i, и по определению критической импликации p_k не входит в Q_i. Отсюда $j \neq k$. Поскольку $f_{il(e)r(e)}(s)$ имеет порядок k или больше, мы можем заключить, что $k < j$. Таким образом, в обосновании значения $f_{il(e)r(e)}$ на s есть два кортежа с разными k-координатами (элемент $\langle j, a\rangle$ именно с этим свойством выбирался при определении $f_{il(e)r(e)}$ на s), поэтому невозможно удалить компоненту из обоих кортежей одним удалением порядка k (напомним, что шаги вида $5t' + 5$ гарантируют нам, что на шаге $5t_1 + 2$ функция $f_{il(e)r(e)}$ была неподозрительной).

Итак, мы доказали, что

$$N_1 + \ldots + N_n \leqslant 2^m(N_1 + \ldots + N_{k-1}) + N_k/2 + N_{k+1} + \ldots + N_n + 2^m\,,$$

откуда

$$N_k \leqslant 2^{m+1}(N_1 + \ldots + N_{k-1}) + 2^{m+1}\,,$$

и $N_k \leqslant 2^{m+1}(2^{m+1}+1)^{k-1} < 2^{(m+2)n}$. Чтобы было выполнено последнее из неравенств (4), достаточно положить $|A_n^0| = 2^{(m+2)(n+1)}$. Далее нам нужно, чтобы $|A_{k-1}^0|2^{-m} > n|A_k^0| + N_{k-1}$ для всех $k = n, \ldots, 2$. Поскольку в правой части этого неравенства второе слагаемое меньше первого, мы можем положить $|A_{k-1}^0| = n2^{m+1}|A_k^0|$. Окончательно получаем оценку $|A_k^0| = 2^{(m+2)(n+1)}(n2^{m+1})^{n-k}$. Константу C из условия леммы достаточно положить равной $6(n+1)$. $\square$

Теорема 8. *Логики $\mathfrak{R}_{\mathrm{w}}$ и $L_{o(\Sigma)}$ имеют интуиционистский позитивный фрагмент.*

Доказательство.

1. В соответствии с теоремой 6 достаточно доказать, что для всех n критическая импликация J_n не принадлежит $\mathfrak{R}_{\mathrm{w}}$. Фиксируем некоторое $i > 0$. Пусть $D(x)$ — такое арифметическое семейство множеств, что $D(k)$ конечно для всех k и для любого семейства $B(x) \in \Sigma_i$ существует такое k, что либо $B(k)$ бесконечно, либо $D(k) = B(k)$ (например, можно взять $D(k) = B_k(k)$ для конечных $B_k(k)$ и $D(k) = \varnothing$ для бесконечных $B_k(k)$, где $B_1(x), B_2(x), \ldots$ — какая-нибудь арифметическая нумерация всех семейств множеств из Σ_i). Ясно, что существует арифметическая функция F, выдающая по k программу $F(k)$, перечисляющую множество $D(k)$. Применяя лемму 6 к множеству $M = D(k)$ (точнее, к программе $q = F(k)$) и числу $m = \lceil \log_2 |D(k)| \rceil$, получим некоторые $A_1(k), \ldots, A_n(k)$. Ясно, что отношение $x \in A_j(k)$ арифметично для всех $j \leqslant n$. По построению для любого k ни один из элементов множества $D(k)$ не принадлежит $J_n(A_1(k), \ldots, A_n(k))$. Следовательно, для любого семейства $B(x) \in \Sigma_i$ найдётся $k \in \mathbb{N}$, для которого или множество $B(k)$ бесконечно, или ни один из его элементов не реализует $J_n(A_1(k), \ldots, A_n(k))$.

2. Достаточно доказать, что для всех n формула J_n не принадлежит $L_{o(\Sigma)}$. В соответствии со свойством 3 колмогоровской сложности по числу m можно построить программу q, перечисляющую множество $M = \{x \mid K(x) < m\}$, а по свойству 4 $|M| \leqslant 2^m$. Применяя лемму 6 к множеству M и числу m, получим такие непустые конечные множества $A_1^m, \ldots, A_n^m$, что $K(A_i^m) \leqslant Cm + O(1)$, но при этом $K(J_n(A_1^m, \ldots, A_n^m)) \geqslant m$. $\square$

3.4. Нам осталось доказать только равенство $\tilde{L}_{o(\Sigma)} = \mathfrak{J}$. К этому мы и перейдём.

Доказательство теоремы 4. В статье [14] Янков фактически доказал, хотя и не сформулировал явно, следующее утверждение. Если формула Φ не выводится в логике $\mathfrak{J}$, то существуют такая позитивная формула Ψ, не выводимая в $\mathfrak{Int}$, и такая формула Φ^*, являющаяся результатом замены некоторых переменных формулы Φ другими переменными и константой $\bot$, что $\mathfrak{Int} \vdash (\Phi^* \to \Psi)$.[7]

Поскольку в критерии Медведева (теорема 6) используются только подстановки формул вида $\vee(\wedge p_i)$, а множество $\tilde{L}_{o(\Sigma)}$ замкнуто относительно выводимости с использованием modus ponens и подстановок формул без импликаций, в частности, $\bot$ (но не $\top = \bot \to \bot$), нам теперь достаточно показать, что $J_n \notin \tilde{L}_{o(\Sigma)}$ для критических импликаций J_n. Тогда мы получим, что $\tilde{L}_{o(\Sigma)} \subseteq \mathfrak{J}$, что вместе с имеющимся обратным включением даст искомое равенство.

Возьмём построенные при доказательстве второй части теоремы 8 множества $A_1^m, \ldots, A_n^m$ и покажем, что $\tilde{K}(A_i^m) \leqslant C'm + O(1)$, что и завершит рассуждение. Во-первых, $A_i^m \subseteq \{0, \ldots, 2^{Cm}\}$. Во-вторых, у нас есть программы, которые по m перечисляют дополнения A_i^m, поэтому, зная точное количество элементов в A_i^m и в $\{0, \ldots, 2^{Cm}\} \setminus A_i^m$, мы можем эффективно найти сами множества $\{0, \ldots, 2^{Cm}\} \setminus A_i^m$ и A_i^m. Таким образом, $\tilde{K}(A_i^m) \leqslant K(m) + K(|A_i^m|) + O(\log K(m)) \leqslant C'm + O(1)$. □

Благодарности

А. Шень предложил рассмотренный здесь новый подход к понятию реализуемости. Он, а также Ан. А. Мучник, активно участвовали в обсуждении результатов и высказали много полезных замечаний. Авторы выражают им свою глубокую благодарность.

[7] План доказательства в статье [14] таков. Для формулы Φ, невыводимой в $\mathfrak{J}$, строится опровергающая конечная шкала Крипке F с наибольшим элементом (изложение ведётся в терминах псевдобулевых алгебр, но это различие несущественно). Далее, строится её характеристическая формула $X(F)$ (в отличие от определения 10, она содержит также члены, описывающие отрицание, см. [17]). Как и в лемме 3 доказывается, что $\mathfrak{Int} \vdash \Phi' \to X(F)$, где Φ' получена из Φ заменой исходных переменных на некоторые q_a, $a \in H(F)$. Наконец, строится позитивная формула Ψ и доказывается, что $\mathfrak{Int} \vdash \Psi' \to \Psi$, где Ψ' получена из $X(F)$ заменой переменной $q_\varnothing$ на $\bot$.

Литература

[1] A. Kolmogoroff. Zur Deutung der intuitionistishen Logik. *Mathematische Zeitschrift*, Bd. 35, H. 1, S. 57–65.

[2] С. К. Клини. *Введение в метаматематику.* М.: ИЛ, 1957.

[3] Ю. Т. Медведев. Финитные задачи. *Доклады АН СССР*, т. 142, вып. 5, 1962, с. 1015–1018.

[4] Ю. Т. Медведев. Интерпретация логических формул посредством финитных задач и связь её с теорией реализуемости. *Доклады АН СССР*, т. 148, вып. 4, 1963, с. 771–774.

[5] Ю. Т. Медведев. Об интерпретации логических формул посредством финитных задач. *Доклады АН СССР*, т. 169, вып. 1, 1966, с. 20–24.

[6] Л. Л. Максимова, Д. П. Скворцов, В. Б. Шехтман. Невозможность конечной аксиоматизации логики конечных задач Медведева. *Доклады АН СССР*, т. 245, вып. 5, 1979, с. 1051–1054.

[7] G. F. Rose. Propositional calculus and realizability. *Transactions of the American Mathematical Society*, v. 75, N. 1, 1953, p. 1–19.

[8] В. Е. Плиско. О реализуемых предикатных формулах. *Доклады АН СССР*, т. 212, вып. 3, 1973, с. 553–556.

[9] Ф. Л. Варпаховский. К вопросу об аксиоматизации реализуемых пропозициональных формул. *Доклады АН СССР*, т. 314, вып. 1, 1990, с. 32–36.

[10] В. Е. Плиско. Абсолютная реализуемость предикатных формул. *Известия АН СССР*, сер. матем., т. 47, вып. 2, 1983, с. 315–334.

[11] A. Shen, N. Vereshchagin. Logical operations and Kolmogorov complexity. *Theoretical Computer Science*, v. 271, 2002, p. 125–129 .

[12] M. Li, P. Vitányi. *An introduction to Kolmogorov complexity and its applications.* New York, Springer-Verlag, 1997.

[13] P. Minari. Intermediate logics with the same disjunctionless fragment as intuitionistic logic. *Studia Logica*, v. 45, N. 2, 1986, p. 207–222.

[14] В. А. Янков. Об исчислении слабого закона исключённого третьего. *Известия АН СССР*, сер. матем., т. 32, вып. 5, 1968, с. 1044–1051.

[15] Н. К. Верещагин, А. Шень. *Языки и исчисления.* М.: МЦНМО, 2000.

[16] M. Szatkowski. On Fragments of Medvedev's Logic. *Studia Logica*, v. 40, N. 1, 1981, p. 39–54.

[17] В. А. Янков. О связи между выводимостью в интуиционистском исчислении высказываний и конечными импликативными структурами. *Доклады АН СССР*, т. 151, вып. 6, 1963, с. 1293–1294.