Московский государственный университет
имени М. В. Ломоносова
Механико-математический факультет

На правах рукописи
УДК 510.52+510.642

Чернов Алексей Вячеславович

О некоторых вариантах понятия реализуемости

Диссертация на соискание учёной степени
кандидата физико-математических наук

01.01.06 — математическая логика, алгебра и теория чисел

Научный руководитель
доктор физико-математических наук, профессор Н. К. Верещагин

Москва 2003

Оглавление

Введение

Классическая логика изучает истинность и ложность высказываний, полученных из некоторых исходных элементарных высказываний при помощи логических операций $\vee$, $\wedge$, $\to$, $\neg$, называемых также логическими связками.

А. Н. Колмогоров в своей статье [16], написанной в 1932 году, предложил рассматривать аналогичные операции не над высказываниями, а над задачами. Логические связки в этом случае используются для построения составной задачи из нескольких исходных элементарных задач. Например, для задач A и B их конъюнкция $A \wedge B$ есть задача „решить обе задачи A и B“, а импликация $A \to B$ — „указать общий метод, позволяющий из решения задачи A получить решение задачи B“.

В некоторых случаях решение составной задачи можно указать, даже не зная использованных элементарных задач, а зная лишь структуру составной задачи, то есть задающую её формулу. Такова, например, задача вида $A \to A$. Колмогоров в статье [16] указывал, что множество формул, для которых можно указать заранее некоторое решение составной задачи, естественно назвать конструктивной логикой. Так определённое „исчисление задач“ он рассматривал как новый подход к построению интуиционистской логики, отличный от философских рассмотрений Брауэра.

Колмогоров ограничился лишь несколькими примерами элементарных задач и неформальным описанием операций, но не сформулировал математически строгой семантики, подобной той, которую булевы функции предоставляют для классической логики. Впоследствии было предложено несколько вариантов семантики, следующей этим идеям. Первым было понятие реализуемости, предложенное С. К. Клини (1945). На несколько других принципах

основывались интерпретации, введённые Ю. Т. Медведевым — исчисление массовых проблем (1955) и финитная общезначимость (1961).

Логика реализуемости (точнее, разные варианты такой логики) и логика финитных задач активно изучались разными исследователями. Довольно быстро было установлено, что эти логики расширяют интуиционистскую логику высказываний, но не совпадают с ней, и встал вопрос об их синтаксическом описании. Для логики финитных задач была доказана невозможность конечной аксиоматизации, для логики реализуемости этот вопрос остаётся открытым. Также не доказана и не опровергнута ни разрешимость, ни перечислимость этих логик.

Настоящая диссертация посвящена подходу, основанному на некоторой модификации исходной идеи Колмогорова. Этот подход был предложен А. Шенем (см. [19]) и опирается на понятие количества информации, рассмотренное Колмогоровым в 1965 году. Основная идея подхода состоит в следующем.

У любой задачи есть важный параметр — минимальное количество информации, достаточное для её решения. Пропозициональная формула, понимаемая как операция над задачами, задаёт некоторую связь между значениями этого параметра для задач-аргументов и задачи-результата. Рассмотрим те формулы, для которых у любой задачи, полученной подстановкой каких-то задач в эту формулу, количество информации, достаточное для её решения, очень мало по сравнению с количеством информации, необходимым для решения подставленных задач (например, ограничено единой константой для всех подставляемых задач). Естественно сказать, что такие формулы задают задачи, которые можно „почти решить“ заранее.

Конечно, формулы колмогоровского „исчисления задач“ обла-

дают рассматриваемым свойством: для них существует общее решение, и количество информации в нём никак не зависит от подставляемых задач. Однако этим свойством могут обладать и другие формулы. Представим себе, например, что мы можем заранее указать два каких-то объекта, и для любой задачи, полученной подстановкой в данную формулу, по меньшей мере один из этих объектов будет решением.

Таким образом, возникает следующий вопрос: каков класс пропозициональных формул, для которых некоторое решение задачи, полученной подстановкой в эту формулу, всегда можно указать, используя „небольшое“ количество информации?

Для ответа на этот вопрос нужно строго определить, что понимается под задачей, какие операции над задачами сопоставлены логическим связкам, как измеряется количество информации, наконец, каков точный смысл слова „небольшое“.

В диссертации рассмотрены два подхода к определению задач и операций над ними: реализуемость (соответствующие задачи названы здесь алгоритмическими) и финитные задачи по Медведеву. Для измерения количества информации в случае алгоритмических задач используется колмогоровская сложность, а в случае финитных задач — мощность „достаточного множества решений“ и колмогоровская сложность (это соответствует двум подходам к определению количества информации из статьи [5], комбинаторному и алгоритмическому). Доказано, что для разнообразных ограничений на количество информации в решении (в случае колмогоровской сложности — для всех естественных ограничений) возникает один и тот же класс формул — логика слабого закона исключённого третьего $\mathfrak{J}$. Доказательства используют характеризацию логики $\mathfrak{J}$ при помощи формул специального вида — критических импликаций — вытекающую из работ Янкова и Медведева.

Диссертация разбита на три главы.

В первой главе изложены некоторые определения и утверждения, нужные для получения основных результатов. Она в основном содержит ранее известные факты. В первой части главы приведены используемые далее результаты из логики. В первом параграфе собраны основные определения и обозначения, относящиеся к логическим формулам и исчислениям. Во втором и третьем параграфах приведены необходимые факты о логике слабого закона исключённого третьего. Во второй части главы введены используемые далее термины и обозначения из теории алгоритмов и колмогоровской сложности.

Во второй главе изучается интерпретация логических связок как операций над алгоритмическими задачами. В первой части главы даны основные определения, описана связь рассматриваемого понятия с понятием реализуемости, и доказаны простые оценки на сложность задач. Во второй части главы доказаны основные результаты, и в частности, нижняя оценка сложности для критических импликаций. Также приведены некоторые оценки, дополняющие основные результаты.

Третья глава посвящена операциям над финитными задачами. В первой части главы дано определение финитных задач и доказаны утверждения, обосновывающие корректность последующих определений. Во второй части главы изложены результаты, связанные с комбинаторной мерой сложности финитных задач, а в третьей части — с алгоритмической мерой сложности.

Автор глубоко благодарен своему научному руководителю Н. К. Верещагину за постановку задачи и последующее постоянное участие и помощь в работе. Автор благодарит А. Шеня, В. Е. Плиско и особенно Д. П. Скворцова за полезные обсуждения. Автор признателен В. А. Успенскому, С. И. Адяну и всем сотрудникам кафедры математической логики и теории алгоритмов механико-математического факультета МГУ за благожелательное внимание к работе.

Глава 1.

Предварительные сведения

1.1. Сведения из логики

1.1.1. Основные определения

Формулы и логики. Пропозициональные формулы строятся обычным образом из переменных, которые будут обозначаться буквами t и s с различными индексами, и константы $\bot$ („ложь“) при помощи логических связок $\vee$, $\wedge$, $\to$. Для сокращения записи формул используются следующие обозначения: $\neg\Psi \rightleftharpoons (\Psi \to \bot)$, $(\Phi \leftrightarrow \Psi) \rightleftharpoons (\Phi \to \Psi) \wedge (\Psi \to \Phi)$, $\top \rightleftharpoons (\bot \to \bot)$. В доказательствах (в частности, при проведении индукции по построению формулы) предполагается, что формулы записаны без сокращений. Пропозициональные формулы во всех случаях, кроме специально оговоренных, будут обозначаться прописными греческими буквами Φ, Ψ, Θ с различными индексами. Через $\Phi(\Psi_1, \ldots, \Psi_k)$ обозначается результат подстановки в формулу $\Phi(t_1, \ldots, t_k)$ формул $\Psi_1, \ldots, \Psi_k$ вместо соответствующих переменных $t_1, \ldots, t_k$.

Позитивные формулы — это формулы, не содержащие константы $\bot$ (и связки $\neg$).

Интуиционистское исчисление высказываний содержит следу-

ющие девять аксиом:

1) $t_1 \to (t_2 \to t_1)$;

2) $(t_1 \to (t_2 \to t_3)) \to ((t_1 \to t_2) \to (t_1 \to t_3))$;

3) $t_1 \wedge t_2 \to t_1$;

4) $t_1 \wedge t_2 \to t_2$;

5) $t_1 \to (t_2 \to t_1 \wedge t_2)$;

6) $t_1 \to t_1 \vee t_2$;

7) $t_2 \to t_1 \vee t_2$;

8) $(t_1 \to t_3) \to ((t_2 \to t_3) \to (t_1 \vee t_2 \to t_3))$;

9) $\bot \to t_1$.

Правилами вывода являются *modus ponens*, позволяющее из формул Φ и $\Phi \to \Psi$ вывести формулу Ψ, и правило подстановки, позволяющее из формулы $\Phi(t_1, \ldots, t_k)$ вывести формулу $\Phi(\Psi_1, \ldots, \Psi_k)$ для произвольных формул $\Psi_1, \ldots, \Psi_k$.

Множество формул, выводимых в интуиционистском исчислении высказываний, обозначается $\mathfrak{Int}$.

Произвольное множество L пропозициональных формул называется *суперинтуиционистской логикой*, если $L \supseteq \mathfrak{Int}$ и L замкнуто относительно правил *modus ponens* и подстановки. Запись $L \vdash \Phi$ означает, что формула Φ принадлежит логике L. Для произвольного множества пропозициональных формул Γ через $(L + \Gamma)$ обозначается наименьшая суперинтуиционистская логика, содержащая $(L \cup \Gamma)$.

Классическая логика высказываний получается из интуиционистской добавлением одной дополнительной аксиомы — закона исключённого третьего $(t \vee \neg t)$.

Формула $(\neg t \vee \neg\neg t)$ называется слабым законом исключённого третьего. Суперинтуиционистская логика $(\mathfrak{Int} + \{\neg t \vee \neg\neg t\})$ называется логикой слабого закона исключённого третьего и обозначается $\mathfrak{J}$.

Множество позитивных формул логики L называется её позитивным фрагментом. Говорят, что логика L *имеет интуиционистский позитивный фрагмент*, если для всех позитивных формул Φ выполнено

$$L \vdash \Phi \;\Leftrightarrow\; \mathfrak{Int} \vdash \Phi\,.$$

Критические импликации. При анализе суперинтуиционистских логик с интуиционистским позитивным фрагментом полезно использовать следующие формулы специального вида, введённые Медведевым в [7].

Критической импликацией называется формула вида

$$J = \bigwedge_i \Big((P_i \to Q_i) \to Q_i \Big) \to R\,,$$

где P_i — непустые конъюнкции переменных, Q_i и R — непустые дизъюнкции переменных, причём при любом i формулы P_i и Q_i не имеют общих переменных.

Всюду далее буква J используется для обозначения критических импликаций, а P, Q, R — соответствующих их подформул.

Для каждого натурального $m > 0$ зафиксируем следующую критическую импликацию в переменных $s_1, \ldots, s_m$:

$$J_m = \bigwedge_{\varnothing \neq E \subset \{1,\ldots,m\}} \Bigg(\Big(\bigwedge_{j \notin E} s_j \to \bigvee_{l \in E} s_l \Big) \to \bigvee_{l \in E} s_l \Bigg) \to \bigvee_{l=1}^{m} s_l\,.$$

В частности, $J_1 = s_1$.

Критическая импликация J_m является самой слабой в том смысле, что для любой критической импликации J в тех же переменных $\mathfrak{Int} \vdash J \to J_m$.

Будем называть *посылкой критической импликации* любую формулу вида $((P \to Q) \to Q)$, где P — непустая конъюнкция переменных, Q — непустая дизъюнкция переменных, причём формулы P и Q не имеют общих переменных.

Шкалы Крипке. Приводимые ниже понятия будут использованы в доказательствах этого раздела.

Шкалой Крипке F называется частично упорядоченное множество с наименьшим элементом 0_F. *Конусом* в шкале F называется подмножество $F^u \rightleftharpoons \{v \in F \mid u \leqslant v\}$. Подмножество a шкалы 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 объединения $\cup$, пересечения $\cap$, импликацией $(a \to b) \rightleftharpoons \{u \in F \mid F^u \cap a \subseteq b\}$, наименьшим элементом $\mathbf{0} = \varnothing$ и наибольшим $\mathbf{1} = F$. Сопоставив связкам $\vee$, $\wedge$, $\to$ и константе $\bot$ операции $\cup$, $\cap$, $\to$ и элемент $\mathbf{0}$, для любой формулы $\Phi(t_1, \ldots, t_k)$ и множеств $a_1, \ldots, a_k \in H(F)$ можно определить множество $\Phi(a_1, \ldots, a_k) \in H(F)$.

Логикой $L(F)$ *шкалы* F называется множество формул, общезначимых в алгебре $H(F)$, то есть

$$L(F) \rightleftharpoons \{\Phi(t_1, \ldots, t_k) \mid \forall a_1, \ldots, a_k \in H(F) \quad \Phi(a_1, \ldots, a_k) = \mathbf{1}\}.$$

Если $\Phi \notin L(F)$, то говорят, что Φ *опровергается* на шкале F.

1.1.2. Логика слабого закона исключённого третьего

Логика слабого закона исключённого третьего $\mathfrak{J}$ обладает рядом свойств, которые сильно упрощают её изучение. Многие из этих свойств содержатся в опубликованной в 1968 году статье Янкова [13]. Здесь они будут сформулированы в виде, удобном для последующих применений.

Начнём с леммы, демонстрирующей связь между выводимостями в логиках $\mathfrak{J}$ и $\mathfrak{Int}$. Хорошо известен следующий вариант теоремы дедукции для произвольной суперинтуиционистской логики L: $(L+\{\Psi\}) \vdash \Phi$ тогда и только тогда, когда $L \vdash (\Psi_1^* \wedge \ldots \wedge \Psi_I^* \to \Phi)$ для некоторых формул $\Psi_1^*, \ldots, \Psi_I^*$, полученных из формулы Ψ по правилу подстановки. Для логики $L = \mathfrak{Int}$ и для $\mathfrak{J} = \mathfrak{Int}+\{\neg t \vee \neg\neg t\}$ можно ограничиться подстановками в формулу $(\neg t \vee \neg\neg t)$ только переменных.

Лемма 1.1. *Пусть все переменные формулы Ψ содержатся среди $t_1, \ldots, t_k$. Тогда*

$$\mathfrak{Int} \vdash \bigwedge_{i=1}^{k} (\neg t_i \vee \neg\neg t_i) \to (\neg\Psi \vee \neg\neg\Psi)\,.$$

Доказательство. Для каждого истинностного значения b и формулы Ψ определим формулу Ψ^b:

$$\Psi^b = \begin{cases} \neg\neg\Psi\,, & \text{если } b \text{ истинно,} \\ \neg\Psi\,, & \text{если } b \text{ ложно.} \end{cases}$$

Индукцией по построению формулы докажем следующее утверждение: если $b_1, \ldots, b_k$ — произвольные истинностные значения, а $b = \Psi(b_1, \ldots, b_k)$ — истинностное значение формулы Ψ (вычисленное по правилам классической логики) при подстановке $b_1, \ldots, b_k$

вместо переменных $t_1, \ldots, t_k$, то

$$\mathfrak{Int} \vdash \bigwedge_{i=1}^{k} t_i^{b_i} \to \Psi^b .$$

(Фактически это доказано, хотя и не сформулировано явно, в лемме 3 статьи [13]. Однако в силу того, что изложение в статье [13] крайне схематично, здесь подробнее выписаны все возможные случаи.)

Если Ψ — одна из переменных $t_1, \ldots, t_k$, то утверждение тривиально.

Если $\Psi = \bot$, то при любых $b_1, \ldots, b_k$ формула Ψ ложна, $\Psi^b = \top$, и утверждение тривиально.

Пусть $\Psi = \Psi_1 \vee \Psi_2$. Обозначим $b' = \Psi_1(b_1, \ldots, b_k)$ и $b'' = \Psi_2(b_1, \ldots, b_k)$. Надо показать, что $\mathfrak{Int} \vdash \Psi_1^{b'} \wedge \Psi_2^{b''} \to \Psi^b$. Если b' истинно, то b истинно, и легко убедиться, что

$$\mathfrak{Int} \vdash \big((\Psi_1 \to \bot) \to \bot\big) \to \big((\Psi_1 \vee \Psi_2 \to \bot) \to \bot\big) .$$

Случай, когда b'' истинно, аналогичен. Если b' и b'' ложны, то b ложно и очевидно, что

$$\mathfrak{Int} \vdash \big((\Psi_1 \to \bot) \wedge (\Psi_2 \to \bot)\big) \to (\Psi_1 \vee \Psi_2 \to \bot) .$$

Пусть $\Psi = \Psi_1 \wedge \Psi_2$. Обозначим $b' = \Psi_1(b_1, \ldots, b_k)$ и $b'' = \Psi_2(b_1, \ldots, b_k)$. Надо показать, что $\mathfrak{Int} \vdash \Psi_1^{b'} \wedge \Psi_2^{b''} \to \Psi^b$. Если b' ложно, то b ложно, и очевидно, что $\mathfrak{Int} \vdash (\Psi_1 \to \bot) \to (\Psi_1 \wedge \Psi_2 \to \bot)$. Случай, когда b'' ложно, аналогичен. Если b' и b'' истинны, то b истинно, и легко убедиться, что

$$\mathfrak{Int} \vdash \Big(\big((\Psi_1 \to \bot) \to \bot\big) \wedge \big((\Psi_2 \to \bot) \to \bot\big)\Big) \to \big((\Psi_1 \wedge \Psi_2 \to \bot) \to \bot\big) .$$

Пусть $\Psi = \Psi_1 \to \Psi_2$. Обозначим $b' = \Psi_1(b_1, \ldots, b_k)$ и $b'' = \Psi_2(b_1, \ldots, b_k)$. Надо показать, что $\mathfrak{Int} \vdash \Psi_1^{b'} \wedge \Psi_2^{b''} \to \Psi^b$. Если b' истинно, а b'' ложно, то b ложно, и очевидно, что

$$\mathfrak{Int} \vdash \Big(\big((\Psi_1 \to \bot) \to \bot\big) \wedge (\Psi_2 \to \bot)\Big) \to \big((\Psi_1 \to \Psi_2) \to \bot\big)\,.$$

Если b' ложно, то b истинно, и легко проверить, что

$$\mathfrak{Int} \vdash (\Psi_1 \to \bot) \to \Big(\big((\Psi_1 \to \Psi_2) \to \bot\big) \to \bot\Big)\,.$$

Если b'' истинно, то b истинно, и легко убедиться, что

$$\mathfrak{Int} \vdash \big((\Psi_2 \to \bot) \to \bot\big) \to \Big(\big((\Psi_1 \to \Psi_2) \to \bot\big) \to \bot\Big)\,.$$

Таким образом, для любых $b_1, \ldots, b_k$

$$\mathfrak{Int} \vdash \bigwedge_{i=1}^{k} t_i^{b_i} \to (\neg\Psi \vee \neg\neg\Psi)\,,$$

и утверждение леммы следует из того, что

$$\mathfrak{Int} \vdash \bigwedge_{i=1}^{k} (\neg t_i \vee \neg\neg t_i) \to \bigvee_{b_1 \ldots b_k} \Big(\bigwedge_{i=1}^{k} t_i^{b_i}\Big)\,.$$

□

Лемма 1.2. *Если все переменные формулы* Φ *содержатся среди* $t_1, \ldots, t_k$, *то*

$$\mathfrak{J} \vdash \Phi(t_1, \ldots, t_k)$$

тогда и только тогда, когда

$$\mathfrak{Int} \vdash \bigwedge_{i=1}^{k} (\neg t_i \vee \neg\neg t_i) \to \Phi(t_1, \ldots, t_k)\,.$$

Доказательство. Очевидно, что если формула $\bigwedge_{i=1}^{k}(\neg t_i \vee \neg\neg t_i) \to \Phi(t_1, \ldots, t_k)$ выводима в $\mathfrak{Int}$, то $\Phi(t_1, \ldots, t_k)$ выводима в $\mathfrak{J}$.

Пусть, наоборот, формула $\Phi(t_1, \ldots, t_k)$ выводима в $\mathfrak{J}$. Тогда в $\mathfrak{Int}$ выводима формула $\bigwedge_{i=1}^{I}(\neg\Psi_i \vee \neg\neg\Psi_i) \to \Phi(t_1, \ldots, t_k)$ для некоторых формул $\Psi_1, \ldots, \Psi_I$. В силу леммы 1.1 выводима и формула $\bigwedge_{i=1}^{K}(\neg t_i \vee \neg\neg t_i) \to \Phi(t_1, \ldots, t_k)$, где среди $t_1, \ldots, t_K$ содержатся все переменные формул $\Psi_1, \ldots, \Psi_I$. Иными словами,

$$\mathfrak{Int} \vdash \bigwedge_{i=k+1}^{K}(\neg t_i \vee \neg\neg t_i) \to \Big(\bigwedge_{i=1}^{k}(\neg t_i \vee \neg\neg t_i) \to \Phi(t_1, \ldots, t_k)\Big).$$

Для доказательства леммы осталось подставить в последнюю формулу константу $\bot$ вместо переменных $t_{k+1}, \ldots, t_K$ и заметить, что в $\mathfrak{Int}$ выводима формула $\neg\bot$. □

Из двух предыдущих лемм, в частности, несложно выводится теорема полноты для $\mathfrak{J}$: формула выводима в $\mathfrak{J}$ тогда и только тогда, когда она общезначима на всех (конечных) шкалах Крипке с наибольшим элементом. Эта теорема (в терминах псевдобулевых алгебр) сформулирована и доказана в [13]. В силу этой теоремы логика $\mathfrak{J}$ финитно аппроксимируема. Поскольку логика $\mathfrak{J}$ также конечно аксиоматизируема, она разрешима.

Следующее утверждение показывает, что логика $\mathfrak{J}$ является наибольшей логикой с интуиционистским позитивным фрагментом.

Теорема 1.1 (Янков,1968). *Суперинтуиционистская логика L имеет интуиционистский позитивный фрагмент тогда и только тогда, когда $L \subseteq \mathfrak{J}$.*

Анализ доказательства этой теоремы, приведённого в [13], позволяет сформулировать следующее более подробное утверждение.

Лемма 1.3. *Если позитивная формула* Φ *невыводима в* $\mathfrak{Int}$*, то она невыводима и в* $\mathfrak{J}$*.*

Пусть формула $\Phi(t_1, \ldots, t_k)$ *невыводима в* $\mathfrak{J}$*. Тогда найдётся такая позитивная формула* $\Psi(t_1, \ldots, t_l)$*, что* $\mathfrak{Int} \vdash \Phi^* \to \Psi$ *и* $\mathfrak{Int} \nvdash \Psi$*, где* Φ^* *получается из* Φ *подстановкой вместо каждой из исходных переменных либо константы* $\bot$*, либо одной из переменных* $t_1, \ldots, t_l$*. При этом если* Φ *опровергается на некоторой шкале Крипке с наибольшим элементом, то формулу* Ψ *можно выбрать так, что она опровергается на той же шкале.*

Таким образом, анализ невыводимых в $\mathfrak{J}$ формул можно свести к анализу позитивных формул, невыводимых в интуиционизме.

1.1.3. Свойства позитивных формул

Среди позитивных формул, невыводимых в $\mathfrak{Int}$, особую роль играют критические импликации (их невыводимость следует, например, из леммы 1.8). Это показывает следующий результат Медведева из [7].

Теорема 1.2 (Медведев, 1962). *Пусть* Φ *— позитивная формула,* $\mathfrak{Int} \nvdash \Phi$*. Тогда найдётся такая критическая импликация* J*, что* $(\mathfrak{Int} + \Phi) \vdash J$*.*

Медведев опубликовал эту теорему без доказательства. Только сорок лет спустя, в статье [20], было впервые опубликовано доказательство, предложенное Д. П. Скворцовым и Е. З. Скворцовой.

Теоремы Янкова и Медведева по сути являются критериями того, что некоторая суперинтуиционистская логика L имеет интуиционистский позитивный фрагмент. Достаточно проверить, что все формулы логики L выводятся из слабого закона исключённого третьего (критерий Янкова), или что в логике L невыводима ни

одна из критических импликаций (критерий Медведева). Первый критерий удобен для логик, заданных аксиоматически, а второй — для логик, заданных семантически.

Эти две теоремы можно использовать и как критерий того, что некоторая логика L, заданная своей семантикой, совпадает с логикой $\mathfrak{J}$. Для этого достаточно проверить, что логике L принадлежит формула $(\neg t \vee \neg\neg t)$ и не принадлежит ни одна из критических импликаций. Именно по этой схеме доказываются основные результаты диссертации.

Нам понадобится следующий более подробный вариант теоремы Медведева.

Лемма 1.4. *Если позитивная формула* $\Psi(t_1, \ldots, t_l)$ *невыводима в* $\mathfrak{Int}$, *то найдутся такое* $m > 0$ *и такие формулы* $\mathrm{T}_i(s_1, \ldots, s_m)$ *вида* $s_m \vee (\bigvee \bigwedge s_j)$, *что импликация* $\Psi(\mathrm{T}_1, \ldots, \mathrm{T}_l) \to J_m$ *выводима в* $\mathfrak{Int}$.

Доказательство леммы 1.4 будет изложено позже, поскольку оно существенно опирается на принадлежащее Скворцовым доказательство теоремы Медведева ([20]). Часть доказательства Скворцовых, необходимая для понимания конструкции, кратко пересказана здесь в виде лемм 1.5 и 1.6 (ср. леммы 1–4 в статье [20]).

Начнём с некоторых определений. Как известно (см. напр. [2]), логика $\mathfrak{Int}$ полна относительно конечных шкал Крипке, поэтому если формула Ψ невыводима в $\mathfrak{Int}$, то найдётся конечная шкала F, на которой эта формула опровергается. Для позитивных формул эту теорему можно усилить, поскольку в качестве F можно выбирать шкалы специального вида. Для произвольного непустого конечного множества F шкалой $\sigma(F)$ называется семейство $\{E \mid E \subset F\}$ собственных подмножеств F, упорядоченное по включению, с наименьшим элементом $\varnothing$. Через σ_m обозначается

$\sigma(\{1,\ldots,m\})$. Ясно, что для любого F шкала $\sigma(F)$ изоморфна σ_m, где m — количество элементов F.

Лемма 1.5. *Если* Ψ — *позитивная формула и* $\mathfrak{Int} \nvdash \Psi$, *то* $\Psi \notin L(\sigma_m)$ *для некоторого* $m > 0$.

Доказательство. Пусть F_0 — любая конечная шкала Крипке, на которой опровергается формула Ψ.

Для этого воспользуемся понятием p-морфизма. 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 $\exists v\,(u \leqslant v$ и $h(v) = w)$,

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. Очевидно, что если h есть p-морфизм F на F', то h^{-1} есть изоморфное вложение алгебры $H(F')$ в $H(F)$. Поэтому если существует p-морфизм F на F', то $L(F) \subseteq L(F')$.

Можно считать, что шкала F_0 не является линейно упорядоченной. Если это не так, добавим к ней элемент, который несравним с наибольшим и больше всех остальных. Исходная шкала будет p-морфным образом новой шкалы (при отображении, которое которое оба максимальных элемента новой шкалы переводит в наибольший элемент исходной, а остальные элементы переводит в себя), поэтому формула Ψ опровергается и в новой шкале.

Покажем, что формула Ψ опровергается также на шкале $\sigma(F_0)$. Для конечной не линейно упорядоченной шкалы Крипке F_0 рассмотрим отображение h, переводящее линейно упорядоченные подмножества F_0 в элементы F_0. Для непустых линейно упорядочен-

ных $E \subset F_0$ значение $h(E)$ равно наибольшему элементу E, и $h(\varnothing) = 0_{F_0}$.

Проверим, что h является p-морфизмом (подмножества F_0 упорядочены по включению). Отображение h сюръективно: если $u \in F_0$, то $u = h(\{u\})$. 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 $E \subseteq E'$.

Поскольку F_0 не линейно упорядочена, все её линейно упорядоченные подмножества принадлежат $\sigma(F_0)$, то есть h есть p-морфизм на шкалу F_0 шкалы $\sigma(F_0) \setminus a_0$, которая получается из $\sigma(F_0)$ отбрасыванием множества a_0, состоящего из не линейно упорядоченых подмножеств F_0, с сохранением порядка на оставшихся элементах. Таким образом, формула Ψ опровергается на шкале $\sigma(F_0) \setminus a_0$.

Учитывая то, что a_0 является открытым подмножеством $\sigma(F_0)$, для позитивной формулы $\Psi(t_1, \ldots, t_l)$ индукцией по построению легко показать, что для любых $a_1, \ldots, a_l \in H\big(\sigma(F_0) \setminus a_0\big)$ элементы $a_i \cup a_0$ открыты в $H(\sigma(F_0))$ и выполнено равенство

$$\Psi(a_1 \cup a_0, \ldots, a_l \cup a_0) = \Psi(a_1, \ldots, a_l) \cup a_0\,,$$

где значение $\Psi(a_1 \cup a_0, \ldots, a_l \cup a_0)$ вычисляется в шкале $H(\sigma(F_0))$, а $\Psi(a_1, \ldots, a_l)$ — в шкале $H\big(\sigma(F_0) \setminus a_0\big)$. Поэтому из того, что позитивная формула Ψ опровергается на шкале $\sigma(F_0) \setminus a_0$, следует, что она опровергается и на шкале $\sigma(F_0)$. □

Лемма 1.6. *Пусть $\Psi(t_1, \ldots, t_l)$ — позитивная формула, и элементы $a_1, \ldots, a_l \in H(\sigma_m)$ таковы, что $\Psi(a_1, \ldots, a_l) \neq \mathbf{1}$ в $H(\sigma_m)$. Тогда*

$$\mathfrak{Int} \vdash \Psi\big(\mathrm{T}_1(s_1, \ldots, s_m), \ldots, \mathrm{T}_l(s_1, \ldots, s_m)\big) \to J_m(s_1, \ldots, s_m)\,,$$

где $\mathrm{T}_i(s_1, \ldots, s_m) = \bigvee_{E \in a_i}\Big(\bigwedge_{j \in E} s_j\Big)$, если $a_i \neq \varnothing$ и $a_i \neq \mathbf{1}$, $\mathrm{T}_i(s_1, \ldots, s_m) = \bigwedge_{j=1}^{m} s_j$ для $a_i = \varnothing$ и $\mathrm{T}_i(s_1, \ldots, s_m) = \top$ для $a_i = \mathbf{1}$.

Доказательство. Пусть всем элементам $a \in H(\sigma_m)$ сопоставлены различные пропозициональные переменные t_a.

Докажем выводимость указанной в условии формулы в два этапа. Сначала докажем, что

$$\mathfrak{Int} \vdash \Psi(t_{a_1}, \ldots, t_{a_l}) \to \mathrm{X}_m$$

для некоторой позитивной формулы X_m с переменными t_a, где индекс a пробегает множество $H(\sigma_m)$. Затем докажем, что

$$\mathfrak{Int} \vdash \mathrm{X}'_m(s_1, \ldots, s_m) \to J_m(s_1, \ldots, s_m)\,,$$

где формула $\mathrm{X}'_m(s_1, \ldots, s_m)$, получена в результате подстановки в формулу X_m некоторых формул $\mathrm{T}_a(s_1, \ldots, s_m)$ вместо переменных t_a, $a \in H(\sigma)$. Формулы $\mathrm{T}_a(s_1, \ldots, s_m)$ определяются следующим образом:

$$\mathrm{T}_a(s_1, \ldots, s_m) = \begin{cases} \bigvee_{E \in a} \Big(\bigwedge_{j \in E} s_j \Big)\,, & \text{если } a \neq \varnothing,\ a \neq \mathbf{1}, \\ \bigwedge_{j=1}^{m} s_j\,, & \text{если } a = \varnothing, \\ \top\,, & \text{если } a = \mathbf{1}\,. \end{cases}$$

(Это соответствует определению формул $\mathrm{T}_1, \ldots, \mathrm{T}_l$ в условии леммы: $\mathrm{T}_i = \mathrm{T}_{a_i}$.)

Формула X_m имеет вид $\Delta_m \to t_\omega$, где $\omega \rightleftharpoons \sigma_m \setminus \{\varnothing\}$ — наибольший неединичный элемент алгебры $H(\sigma_m)$, а Δ_m — конъюнкция всех формул вида

$$\begin{aligned} (t_{b_1} \vee t_{b_2}) &\leftrightarrow t_{b_1 \cup b_2}, \\ (t_{b_1} \wedge t_{b_2}) &\leftrightarrow t_{b_1 \cap b_2}, \\ (t_{b_1} \to t_{b_2}) &\leftrightarrow t_{b_1 \to b_2}, \end{aligned}$$

где $b_1, b_2 \in H(\sigma_m)$.

Формула X_m является позитивной характеристической формулой шкалы σ_m (в [20] использовалось обозначение $\mathrm{X}_\Pi(\sigma_m)$). Понятие характеристической формулы было введено Янковым в статье [14].

Индукцией по построению позитивной формулы Ψ легко показать, что

$$\mathfrak{Int} \vdash \Delta_m \to (\Psi(t_{a_1}, \ldots, t_{a_l}) \leftrightarrow t_{a_0}),$$

где $a_0 = \Psi(a_1, \ldots, a_l) \neq \mathbf{1}$. Так как $a_0 \leqslant \omega$ в $H(\sigma)$, то $a_0 \to \omega = \mathbf{1} = \mathbf{1} \to \mathbf{1}$. Поэтому $\mathfrak{Int} \vdash \Delta_m \to ((t_{a_0} \to t_\omega) \leftrightarrow (t_\mathbf{1} \to t_\mathbf{1}))$ и $\mathfrak{Int} \vdash \Delta_m \to (t_{a_0} \to t_\omega)$. Следовательно,

$$\mathfrak{Int} \vdash \Psi(t_{a_1}, \ldots, t_{a_l}) \to \mathrm{X}_m$$

(не ограничивая общности, можно считать, что $t_{a_i} = t_i$ при $i \in \{1, \ldots, l\}$).

Осталось показать, что $\mathfrak{Int} \vdash \mathrm{X}'_m \to J_m$. Обозначим через Δ'_m посылку формулы X'_m, а именно, Δ'_m есть конъюнкция по всем $b_1, b_2 \in H(\sigma_m)$ формул

$$(\mathrm{T}_{b_1} \vee \mathrm{T}_{b_2}) \leftrightarrow \mathrm{T}_{b_1 \cup b_2}, \tag{1.1}$$

$$(\mathrm{T}_{b_1} \wedge \mathrm{T}_{b_2}) \leftrightarrow \mathrm{T}_{b_1 \cap b_2}, \tag{1.2}$$

$$(\mathrm{T}_{b_1} \to \mathrm{T}_{b_2}) \leftrightarrow \mathrm{T}_{b_1 \to b_2}. \tag{1.3}$$

Формула $\mathrm{T}_\omega(s_1, \ldots, s_m)$ содержит, в частности, дизъюнктивные члены $s_1, \ldots, s_m$, поэтому

$$\mathfrak{Int} \vdash \mathrm{T}_\omega(s_1, \ldots, s_m) \to \bigvee_{j=1}^{m} s_j,$$

то есть заключение формулы X'_m влечёт заключение формулы J_m. Таким образом, достаточно проверить, что из посылки J_m следует посылка X'_m, или, эквивалентно, что

$$\mathfrak{Int} \vdash \bigwedge_{\varnothing \neq E \subset \{1,\ldots,m\}} \left(\left(\bigwedge_{j \notin E} s_j \to \bigvee_{i \in E} s_i \right) \to \bigvee_{i \in E} s_i \right) \to \Gamma$$

для всех конъюнктивных членов Γ из Δ'_m.

Формулы Γ вида (1.1) непосредственно выводимы в $\mathfrak{Int}$:

$$\Big(\bigvee_{E\in b_1}\bigwedge_{j\in E} s_j\Big)\vee\Big(\bigvee_{E\in b_2}\bigwedge_{j\in E} s_j\Big)\leftrightarrow\Big(\bigvee_{E\in b_1\cup b_2}\bigwedge_{j\in E} s_j\Big)$$

(вырожденные случаи, когда b_1 или b_2 равно $\varnothing$ либо $\mathbf{1}$, нужно рассмотреть отдельно, однако они совершенно очевидны). Также легко доказывается выводимость формул вида (1.2):

$$\Big(\Big(\bigvee_{E\in b_1}\bigwedge_{j\in E} s_j\Big)\wedge\Big(\bigvee_{E'\in b_2}\bigwedge_{j\in E'} s_j\Big)\Big)\leftrightarrow$$
$$\leftrightarrow\Big(\bigvee_{E\in b_1,E'\in b_2}\Big(\bigwedge_{j\in E} s_j\Big)\wedge\Big(\bigwedge_{j\in E'} s_j\Big)\Big)\leftrightarrow\Big(\bigvee_{E\in b_1,E'\in b_2}\bigwedge_{j\in E\cup E'} s_j\Big)\leftrightarrow$$
$$\leftrightarrow\Big(\bigvee_{E\in b_1\cap b_2}\bigwedge_{j\in E} s_j\Big)$$

где для доказательства последней эквивалентности следует заметить, что если $E\in b_1$ и $E'\in b_2$, то $E\cup E'\in b_1\cap b_2$. Вырожденные случаи очевидны.

Осталось разобрать формулы вида (1.3). Введём обозначения $d_E=\{E'\mid E\subseteq E'\}$ и $h_E=\{E'\mid E\cap E'\neq\varnothing\}$ для $\varnothing\neq E\subset\{1,\dots,m\}$. Легко проверить, что интуиционистски выводимы формулы $\mathrm{T}_{d_E}\leftrightarrow\bigwedge_{j\in E}s_j$ и $\mathrm{T}_{h_E}=\bigvee_{j\in E}s_j$. Каждое b_1 из $H(\sigma_m)$, кроме $\mathbf{0}$ и $\mathbf{1}$, представимо как объединение d_E, а каждое b_2, кроме $\mathbf{1}$, представимо как пересечение $h_{E'}$ (в частности, $\varnothing=\bigcap_{i=1}^m b_{\{i\}}$). При этом, ввиду выводимости (1.1) и (1.2), формулы T_{b_1} и T_{b_2} эквивалентны в $\mathfrak{Int}$ соответственно дизъюнкции и конъюнкции формул вида T_{d_E} и $\mathrm{T}_{h_{E'}}$. Также, поскольку $\mathfrak{Int}\vdash(\vee_i\Phi_i\to\wedge_j\Psi_j)\leftrightarrow\wedge_{ij}(\Phi_i\to\Psi_j)$, формула $(\mathrm{T}_{b_1}\to\mathrm{T}_{b_2})$ эквивалентна конъюнкции формул $(\mathrm{T}_{d_E}\to\mathrm{T}_{h_{E'}})$, а множество $(b_1\to b_2)$

равно пересечению соответствующих $(d_E \to h_{E'})$, так как в алгебре $H(\sigma_m)$ выполнены все интуиционистские законы. Итак, достаточно вывести формулы (1.3) для $b_1 = d_E$, $b_2 = h_{E'}$, и проверить вырожденные случаи.

Если $E \cap E' \neq \varnothing$, то, во-первых, $\mathfrak{Int} \vdash (\mathrm{T}_{d_E} \to \mathrm{T}_{h_{E'}})$, а во-вторых, $d_E \subseteq h_{E'}$ (так как если $E'' \supseteq E$, то $E'' \cap E' \supseteq E \cap E' \neq \varnothing$), то есть $d_E \to h_{E'} = \mathbf{1}$ и $\mathrm{T}_{d_E \to h_{E'}} = \top$.

Пусть теперь $E \cap E' = \varnothing$. Тогда $d_E \to h_{E'} = h_{E'}$ в алгебре $H(\sigma_m)$. Действительно, если $E'' \notin h_{E'}$, то есть $E' \cap E'' = \varnothing$, то $(E \cup E'') \cap E' = \varnothing$, поэтому $E'' \subseteq E \cup E'' \in (d_E \setminus h_{E'})$, а значит, $E'' \notin (d_E \to h_{E'})$. Далее, посылка формулы J_m влечет формулу $\left(\bigwedge_{j \in E} s_j \to \bigvee_{i \in E'} s_i\right) \to \bigvee_{i \in E'} s_i$, так как $E \subseteq \left(\{1, \ldots, m\} \setminus E'\right)$, и следовательно,

$$\mathfrak{Int} \vdash \bigwedge_{\varnothing \neq E \subset \{1,\ldots,m\}} \left(\left(\bigwedge_{j \notin E} s_j \to \bigvee_{i \in E} s_i \right) \to \bigvee_{i \in E} s_i \right) \to \left((\mathrm{T}_{d_E} \to \mathrm{T}_{h_{E'}}) \leftrightarrow \mathrm{T}_{h_{E'}} \right).$$

Оставшиеся вырожденные случаи тривиальны. Если $b_2 = \mathbf{1}$, то $(b_1 \to b_2) = \mathbf{1}$, и $\mathrm{T}_{b_2} = \mathrm{T}_{b_1 \to b_2} = \top$. Если $b_1 = \mathbf{1}$, то $\mathrm{T}_{b_1} = \top$, $(b_1 \to b_2) = b_2$, и $\mathfrak{Int} \vdash (\top \to \mathrm{T}_{b_2}) \leftrightarrow \mathrm{T}_{b_2}$. Наконец, если $b_1 = \varnothing$, то $b_1 \to b_2 = \mathbf{1}$, и $\mathfrak{Int} \vdash \top \leftrightarrow (\bigwedge_{i=1}^{m} s_i \to \mathrm{T}_{b_2})$. □

Доказательство леммы 1.4. В соответствии с леммой 1.6, чтобы построить формулы $\mathrm{T}_i(s_1, \ldots, s_m)$ вида $s_m \vee (\bigvee \bigwedge s_j)$ достаточно найти такие элементы $a_1, \ldots, a_l \in H(\sigma_m)$, что $\Psi(a_1, \ldots, a_l) \neq \mathbf{1}$ и при всех i выполнены условия $a_i \neq \mathbf{1}$ и $\{m\} \in a_i$.

Поскольку позитивная формула $\Psi(t_1, \ldots, t_l)$ невыводима в $\mathfrak{Int}$, в силу леммы 1.5 можно выбрать такое число m и такие элементы $\tilde{a}_1, \ldots, \tilde{a}_l \in H(\sigma_{m-2})$, что $\Psi(\tilde{a}_1, \ldots, \tilde{a}_l) \neq \mathbf{1}$ в $H(\sigma_{m-2})$.

В σ_m возьмём множества $a_1, \ldots, a_l$, заданные равенствами

$$a_i = \{E \mid m \in E \subset \{1, \ldots, m\}\} \cup \{\{1, \ldots, m-1\}\} \cup \\ \cup \{\tilde{E} \cup \{m-1\} \mid \tilde{E} \in \tilde{a}_i\}$$

Заметим, что по построению $\{m\} \in a_i$ и $\varnothing \notin a_i$, следовательно, $a_i \neq \varnothing$ и $a_i \neq \mathbf{1}$.

Проверим, что множества a_i открыты в шкале σ_m. Для этого надо показать, что для любых собственных подмножеств E и E' множества $\{1, \ldots, m\}$ если $E \in a_i$ и $E \subseteq E'$, то $E' \in a_i$. Если $E = \{1, \ldots, m-1\}$, то $E' = E$, поскольку $E' \neq \{1, \ldots, m\}$. Если $m \in E$, то $m \in E'$. Осталось рассмотреть случай, когда $E = \tilde{E} \cup \{m-1\}$, где $\tilde{E} \in \tilde{a}_i$, и $E \subseteq E'$. Если $m \in E'$, то $E' \in a_i$. В противном случае $E' \subseteq \{1, \ldots, m-1\}$. Положим $\tilde{E}' = E' \setminus \{m-1\}$. Если оказалось, что $\tilde{E}' = \{1, \ldots, m-2\}$, то $E' = \{1, \ldots, m-1\} \in a_i$. Пусть $\tilde{E}' \subset \{1, \ldots, m-2\}$. Из того, что $\tilde{E} \subset E'$ и $(m-1) \notin \tilde{E}$, следует, что $\tilde{E} \subseteq \tilde{E}'$, и поэтому $\tilde{E}' \in \tilde{a}_i$ в силу открытости $\tilde{a}_i$. Таким образом, $E' = \tilde{E}' \cup \{m-1\} \in a_i$.

Осталось показать, что для выбранных $a_1, \ldots, a_l$ выполнено $\Psi(a_1, \ldots, a_l) \neq \mathbf{1}$.

Сначала заметим, что для произвольной позитивной формулы $\Theta(t_1, \ldots, t_l)$ если $m \in E \subset \{1, \ldots, m\}$ или $E = \{1, \ldots, m-1\}$, то $E \in \Theta(a_1, \ldots, a_l)$. Действительно, для переменных это выполнено по определению $a_1, \ldots, a_l$, и тривиально проверяется, что это свойство сохраняется при применении операций $\cup$, $\cap$ и $\to$.

Теперь для любой позитивной формулы $\Theta(t_1, \ldots, t_l)$ индукцией по построению покажем, что если $\tilde{E} \subset \{1, \ldots, m-2\}$, то

$$\tilde{E} \in \Theta(\tilde{a}_1, \ldots, \tilde{a}_l) \text{ в } H(\sigma_{m-2}) \Leftrightarrow \\ \Leftrightarrow (\tilde{E} \cup \{m-1\}) \in \Theta(a_1, \ldots, a_l) \text{ в } H(\sigma_m).$$

Пусть $\Theta = t_i$. Заметим, что при $\tilde{E} \subset \{1, \ldots, m-2\}$ невозможно ни $m \in \tilde{E} \cup \{m-1\}$, ни $\tilde{E} \cup \{m-1\} = \{1, \ldots, m-1\}$. Таким образом, $\tilde{E} \in \tilde{a}_i$ тогда и только тогда, когда $\tilde{E} \cup \{m-1\} \in a_i$ по определению a_i.

Пусть $\Theta = \Theta_1 \vee \Theta_2$. В этом случае

$$\begin{aligned}
&\tilde{E} \in \Theta(\tilde{a}_1, \ldots, \tilde{a}_l) \Leftrightarrow \\
&\quad \Leftrightarrow \tilde{E} \in \Theta_1(\tilde{a}_1, \ldots, \tilde{a}_l) \text{ или } \tilde{E} \in \Theta_2(\tilde{a}_1, \ldots, \tilde{a}_l) \Leftrightarrow \\
&\quad\quad \Leftrightarrow \tilde{E} \cup \{m-1\} \in \Theta_1(a_1, \ldots, a_l) \text{ или} \\
&\quad\quad\quad \tilde{E} \cup \{m-1\} \in \Theta_2(a_1, \ldots, a_l) \Leftrightarrow \\
&\quad\quad\quad\quad \Leftrightarrow \tilde{E} \cup \{m-1\} \in \Theta(a_1, \ldots, a_l)\,.
\end{aligned}$$

Пусть $\Theta = \Theta_1 \wedge \Theta_2$. В этом случае

$$\begin{aligned}
&\tilde{E} \in \Theta(\tilde{a}_1, \ldots, \tilde{a}_l) \Leftrightarrow \\
&\quad \Leftrightarrow \tilde{E} \in \Theta_1(\tilde{a}_1, \ldots, \tilde{a}_l) \text{ и } \tilde{E} \in \Theta_2(\tilde{a}_1, \ldots, \tilde{a}_l) \Leftrightarrow \\
&\quad\quad \Leftrightarrow \tilde{E} \cup \{m-1\} \in \Theta_1(a_1, \ldots, a_l) \text{ и} \\
&\quad\quad\quad \tilde{E} \cup \{m-1\} \in \Theta_2(a_1, \ldots, a_l) \Leftrightarrow \\
&\quad\quad\quad\quad \Leftrightarrow \tilde{E} \cup \{m-1\} \in \Theta(a_1, \ldots, a_l)\,.
\end{aligned}$$

Остался случай, когда $\Theta = \Theta_1 \to \Theta_2$.

Пусть $\tilde{E} \in \Theta(\tilde{a}_1, \ldots, \tilde{a}_l)$, Возьмём произвольное такое E', что $E' \subset \{1, \ldots, m\}$, $E' \supseteq \tilde{E} \cup \{m-1\}$ и $E' \in \Theta_1(a_1, \ldots, a_l)$, и покажем, что $E' \in \Theta_2(a_1, \ldots, a_l)$. Как уже известно, это выполнено при $m \in E'$. В противном случае $E' \subseteq \{1, \ldots, m-1\}$. Положим $\tilde{E}' = E' \setminus \{m-1\}$. Если оказалось, что $\tilde{E}' = \{1, \ldots, m-2\}$, то $E' = \{1, \ldots, m-1\} \in \Theta_2(a_1, \ldots, a_l)$. Пусть $\tilde{E}' \subset \{1, \ldots, m-2\}$. Так как $E' = \tilde{E}' \cup \{m-1\}$, по индуктивному предположению имеем $\tilde{E}' \in \Theta_1(\tilde{a}_1, \ldots, \tilde{a}_l)$. Поскольку $\tilde{E} \subset E'$ и $(m-1) \notin \tilde{E}$, получим $\tilde{E} \subseteq \tilde{E}'$, и по определению импликации $\tilde{E}' \in \Theta_2(\tilde{a}_1, \ldots, \tilde{a}_l)$. По индуктивному предположению получаем, что $E' \in \Theta_2(a_1, \ldots, a_l)$.

Обратно, пусть $\tilde{E} \cup \{m-1\} \in \Theta(a_1, \ldots, a_l)$. Возьмём любое такое $\tilde{E}'$, что $\tilde{E}' \subset \{1, \ldots, m-2\}$, $\tilde{E}' \supseteq \tilde{E}$ и $\tilde{E}' \in \Theta_1(\tilde{a}_1, \ldots, \tilde{a}_l)$. По предположению индукции $\tilde{E}' \cup \{m-1\} \in \Theta_1(a_1, \ldots, a_l)$, поэтому $\tilde{E}' \cup \{m-1\} \in \Theta_2(a_1, \ldots, a_l)$, так как $\tilde{E}' \cup \{m-1\} \supseteq \tilde{E} \cup \{m-1\}$. Следовательно, $\tilde{E}' \in \Theta_2(\tilde{a}_1, \ldots, \tilde{a}_l)$.

Элементы $\tilde{a}_1, \ldots, \tilde{a}_l$ выбирались так, что $\varnothing \notin \Psi(\tilde{a}_1, \ldots, \tilde{a}_l)$ в $H(\sigma_{m-2})$, поэтому $\{m-1\} \notin \Psi(a_1, \ldots, a_l)$ и $\Psi(a_1, \ldots, a_l) \neq \mathbf{1}$ в $H(\sigma_m)$, что и требовалось. □

Теперь, соединив леммы 1.3 и 1.4, можно сформулировать следующее важное свойство, которое сводит анализ формул, невыводимых в $\mathfrak{J}$, к анализу критических импликаций.

Теорема 1.3. *Пусть формула $\Phi(t_1, \ldots, t_k)$ невыводима в $\mathfrak{J}$. В этом случае можно эффективно найти такое натуральное число $m > 0$ и такие формулы $\mathrm{T}_1(s_1, \ldots, s_m), \ldots, \mathrm{T}_k(s_1, \ldots, s_m)$, что интуиционистски выводима импликация*

$$\Phi\big(\mathrm{T}_1(s_1, \ldots, s_m), \ldots, \mathrm{T}_k(s_1, \ldots, s_m)\big) \to J_m(s_1, \ldots, s_m)\,.$$

При этом можно считать, что если формула Φ позитивна, то все T_i имеют вид $s_m \vee \Upsilon(s_1, \ldots, s_m)$, где $\Upsilon(s_1, \ldots, s_m)$ есть некоторая дизъюнкция конъюнкций переменных, а если формула Φ непозитивна, то при каждом i формула T_i либо имеет указанный вид, либо является константой $\bot$.

Замечание. Если классически истинна формула $\Phi(\bot, \ldots, \bot)$, полученная подстановкой константы $\bot$ вместо всех переменных, то построенные в теореме формулы T_i не могут все быть равны $\bot$. Действительно, из классической истинности формулы $\Phi(\bot, \ldots, \bot)$ следует её выводимость в $\mathfrak{Int}$, а так как критические импликации невыводимы в $\mathfrak{Int}$, то

$$\mathfrak{Int} \nvdash \Phi(\bot, \ldots, \bot) \to J_m(s_1, \ldots, s_m)\,.$$

Лемма 1.7. *В теореме 1.3 можно считать, что* $m \leqslant 2^{N(\Phi)+4k+1}+3$, *где* $N(\Phi)$ — *количество подформул формулы* Φ.

Доказательство. Проследим, как возникает в доказательстве число m. Сначала в конструкции применяется лемма 1.3, в которой строится некоторая позитивная формула Ψ. Затем при помощи леммы 1.5 появляется число $m' = m - 2$. Число m' выбирается в этой лемме в зависимости от шкалы Крипке, на которой опровергается формула Ψ. Построим такую шкалу Крипке и оценим её мощность.

Если формула Φ невыводима в $\mathfrak{J}$, то в $\mathfrak{Int}$ невыводима формула $\Phi' = \bigwedge_{i=1}^{k}(\neg t_i \vee \neg\neg t_i) \to \Phi$. Используя одно из известных доказательств теоремы полноты для $\mathfrak{Int}$ (см. напр. [2]), можно построить конечную шкалу Крипке F, на которой опровергается формула Φ', и элементами которой являются некоторые множества подформул этой формулы. Легко видеть, что $|F| \leqslant 2^{N(\Phi)+4k+1}$.

Выберем такие элементы $a_1, \ldots, a_k$ из $H(F)$, для которых $\Phi'(a_1, \ldots, a_k) \neq \mathbf{1}$. Можно считать, что $\bigwedge_{i=1}^{k}(\neg a_i \vee \neg\neg a_i) = \mathbf{1}$ (в противном случае надо вместо шкалы F взять конус F^v в ней, где $v \in \bigwedge_{i=1}^{k}(\neg a_i \vee \neg\neg a_i)$ и $v \notin \Phi(a_1, \ldots, a_k)$), то есть для каждого i либо $\neg a_i = \mathbf{1}$, либо $\neg\neg a_i = \mathbf{1}$. Рассмотрим множество M максимальных элементов шкалы F. Из сказанного легко следует, что для каждого i либо $M \subseteq a_i$, либо $M \cap a_i = \varnothing$. Нетрудно проверить, что и для любой формулы Θ либо $M \subseteq \Theta(a_1, \ldots, a_k)$, либо $M \cap \Theta(a_1, \ldots, a_k) = \varnothing$.

Отождествив все максимальные точки шкалы F, получим шкалу $\tilde{F}$ с наибольшей точкой. Очевидно, что формула Φ опровергается и в шкале $\tilde{F}$, и $|\tilde{F}| \leqslant 2^{N(\Phi)+4k+1}$.

Теперь можно применить лемму 1.3, которая позволяет выбрать формулу Ψ таким образом, что Ψ опровергается на шкале $\tilde{F}$. В доказательстве леммы 1.5 строится шкала σ, элементами которой

являются подмножества шкалы $\tilde{F}$, к которой, возможно, добавлен один элемент (для нелинейности). Эта шкала изоморфна шкале $\sigma_{m'}$ для $m' = |\tilde{F}| + 1$. Наконец, в доказательстве леммы 1.4 возникает $m = m' + 2$. □

Полученная оценка на m верна для любой формулы. В некоторых частных случаях, конечно, можно получить более точные результаты. Докажем уточнённый вариант теоремы 1.3, в котором произвольная невыводимая формула Ф заменена произвольной критической импликацией. Это утверждение пригодится при получении одной из оценок во второй главе.

Начнём с простой леммы, из которой, в частности, следует, что критические импликации невыводимы в $\mathfrak{Int}$.

Лемма 1.8. *Пусть J — произвольная критическая импликация, содержащая только переменные $s_1, \ldots, s_m$. В алгебре $H(\sigma_m)$ возьмём множества $a_j = \{E \mid j \in E\}$. Тогда $J(a_1, \ldots, a_m) \neq \mathbf{1}$.*

Доказательство. Покажем, что для указанного набора $a_1, \ldots, a_m$ значение каждой из посылок J (вида $(P_i \to Q_i) \to Q_i$) равно $\mathbf{1}$. Для этого покажем, что $(P_i \to Q_i)(a_1, \ldots, a_m) \subseteq Q_i(a_1, \ldots, a_m)$.

Действительно, пусть $P_i = \bigwedge_{j \in E'} s_j$, $Q_i = \bigvee_{j \in E''} s_j$, $E' \cap E'' = \varnothing$, 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 $(E \cup E') \in \bigwedge_{j \in E'} a_j$, и следовательно, $E \notin (\bigwedge_{j \in E'} a_j \to \bigvee_{j \in E''} a_j)$.

Поскольку $\varnothing \notin a_j$ для всех j, любая непустая дизъюнкция элементов a_j отлична от $\mathbf{1}$. Таким образом, все посылки импликации J равны $\mathbf{1}$, а заключение отлично от $\mathbf{1}$. □

Теперь сформулируем упомянутый аналог теоремы 1.3.

Лемма 1.9. *Пусть J — произвольная критическая импликация, содержащая только переменные $s_1, \ldots, s_m$. Тогда в $\mathfrak{Int}$ выводима*

импликация

$$J\big((s_1 \wedge s_{m+1}) \vee s_{m+2}, \ldots, (s_m \wedge s_{m+1}) \vee s_{m+2}\big) \to J_{m+2}(s_1, \ldots, s_{m+2})\,.$$

Доказательство. Поскольку J опровергается на шкале σ_m, можно применить конструкцию леммы 1.4 для построения таких $a_1, \ldots, a_m$ из $H(\sigma_{m+2})$, что $J(a_1, \ldots, a_m) \neq \mathbf{1}$, $\{m+2\} \in a_j$, $a_j \neq \mathbf{1}$, $a_j \neq \varnothing$:

$$a_j = \big\{E \mid m+2 \in E\big\} \cup \big\{\{1, \ldots, m+1\}\big\} \cup \\ \cup \big\{E \cup \{m+1\} \mid j \in E \subset \{1, \ldots, m\}\big\}\,.$$

Из леммы 1.6 следует, что

$$\mathfrak{Int} \vdash J\big(\mathrm{T}_1(s_1, \ldots, s_{m+2}), \ldots, \mathrm{T}_m(s_1, \ldots, s_{m+2})\big) \to J_{m+2}(s_1, \ldots, s_{m+2})\,,$$

где $\mathrm{T}_j(s_1, \ldots, s_{m+2}) = \bigvee_{E \in a_j} \bigwedge_{l \in E} s_l$. Наконец, простая проверка показывает, что

$$\mathfrak{Int} \vdash \mathrm{T}_j(s_1, \ldots, s_{m+2}) \leftrightarrow \big(s_{m+2} \vee (s_j \wedge s_{m+1})\big)\,.$$

□

1.2. Алгоритмы и количество информации

1.2.1. Алгоритмы

Будем считать, что все алгоритмы применяются к конечным двоичным словам произвольной длины. Пустое слово будет обозначаться символом ε. Произвольные двоичные слова обозначаются строчными латинскими буквами с индексами. Длина двоичного слова x обозначается через $\ell(x)$.

Все остальные конструктивные объекты кодируются двоичными словами. В частности, будем считать, что зафиксировано

некоторое кодирование пар двоичных слов, то есть вычислимая функция, которая любым двум словам x и y ставит в соответствие некоторое слово $\langle x, y\rangle$, называемое кодом пары, и по $\langle x, y\rangle$ можно вычислимо найти x и y. (Сама пара, понимаемая в теоретико-множественном смысле, будет обозначаться $\langle\!\langle x, y\rangle\!\rangle$. Это обозначение используется в третьей главе.)

Зафиксируем также вычислимое кодирование кортежей произвольной длины: для любого натурального $n \geqslant 3$ любых двоичных слов $x_1, \ldots, x_n$ положим

$$\langle x_1, \ldots, x_n\rangle = \langle\langle x_1, \ldots, x_{n-1}\rangle, x_n\rangle\,.$$

Будем также считать, что зафиксирована некоторая главная вычислимая нумерация всех вычислимых одноместных частичных функций на множестве двоичных слов, то есть такая частичная двуместная вычислимая функция $U\colon \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$, что для любой другой двуместной частичной вычислимой функции $V\colon \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ найдётся всюду определённая вычислимая функция h, для которой $U(h(x), y) = V(x, y)$ для всех двоичных слов x и y. Запись $[x](y)$ есть другое обозначение для $U(x, y)$.

При фиксированном x выражение $[x](y)$ задаёт одноместную вычислимую функцию от y. Очевидно, что каждая одноместная вычислимая функция представима в таком виде для некоторого x. Поэтому для $[x](y)$, рассматриваемой как функция y, слово x будет называться программой для вычисления этой функции, а само значение $[x](y)$ (которое может быть и неопределено) будет также называться результатом применения программы x к слову y.

Алгоритмы и вычислимые функции будут описываться неформально, с опорой на тезис Чёрча.

1.2.2. Количество информации

В опубликованной в 1965 году статье [5] Колмогоров проанализировал три основных подхода к определению понятия количества информации. Мы будем использовать два из них, комбинаторный и алгоритмический. Хорошо известно, что многие результаты теории информации имеют две аналогичные формулировки в терминах этих двух подходов.

При комбинаторном подходе рассматриваются произвольные множества объектов с некоторым свойством. Количеством информации в элементах этого множества называется двоичный логарифм его мощности — именно столько битов нужно для указания какого-нибудь одного элемента.

При алгоритмическом подходе количество информации приписывается уже отдельным конструктивным объектам. В качестве меры количества информации берётся длина наименьшей программы, порождающей объект. Так определённая величина называется колмогоровской сложностью объекта.

Далее приводятся формальное определение и основные свойства простой колмогоровской сложности. Более подробное изложение теории сложности можно найти в обзоре [3] и монографии [17].

Пусть f — любая одноместная частичная вычислимая функция. Сложностью $K_f(x)$ слова x относительно функции f называется минимум длин таких слов y, что $f(y) = x$:

$$K_f(x) \rightleftharpoons \min\{\ell(y) \mid f(y) = x\}\,;$$

если x не принадлежит области значений функции f, его сложность относительно f бесконечна.

Функция $\mathfrak{f}$ называется *оптимальным способом описания*, если для любой другой функции g найдётся такая константа C, что $K_{\mathfrak{f}}(x) \leqslant K_g(x)+C$ для всех двоичных слов x. Теорема Колмогорова,

доказанная в [5], утверждает, что оптимальный способ описания существует.

Зафиксируем какой-нибудь оптимальный способ описания $\mathfrak{f}$. Колмогоровской сложностью слова x называется его сложность относительно этого оптимального способа описания $\mathfrak{f}$:

$$K(x) \rightleftharpoons K_{\mathfrak{f}}(x)\,.$$

Очевидно, что существует бесконечно много оптимальных способов описания, поэтому предыдущее определение содержит некоторый произвол. Однако если $\mathfrak{f}_1$ и $\mathfrak{f}_2$ — два оптимальных способа описания, то найдётся константа C, которая ограничивает разность между двумя функциями сложности:

$$\forall x \quad |K_{\mathfrak{f}_1}(x) - K_{\mathfrak{f}_2}(x)| \leqslant C\,.$$

Таким образом, все функции колмогоровской сложности отличаются не более чем на константу. Следовательно, для утверждений, в которые сложности двоичных слов входят вместе с произвольным постоянным слагаемым, выбор одного из оптимальных способов описания несущественен. Поэтому во всех дальнейших формулировках, касающихся сложности, будет фигурировать константа, зависящая только от выбора функции сложности (оптимального способа описания).

Аналогичным образом определяется функция условной колмогоровской сложности $K(x|y)$, которая выражает количество информации, необходимой для построения объекта x если объект y уже известен. Формальное определение таково.

Пусть f — любая двуместная частичная вычислимая функция. Условной сложностью $K_f(x|y)$ слова x при известном слове y относительно функции f называется минимум длин таких слов z, что $f(y,z) = x$:

$$K_f(x|y) \rightleftharpoons \min\{\ell(z) \mid f(y,z) = x\}\,;$$

если x не равен $f(y,z)$ ни при каком z, его сложность бесконечна. Функция $\mathfrak{f}$ называется *оптимальным условным способом описания*, если для любой другой функции g найдётся такая константа C, что для всех двоичных слов x и y выполнено неравенство $K_{\mathfrak{f}}(x|y) \leqslant K_g(x|y) + C$. (По теореме Колмогорова из [5] такой способ описания существует.) Зафиксируем какой-нибудь оптимальный условный способ описания $\mathfrak{f}$. Условной колмогоровской сложностью слова x при известном слове y называется его условная сложность относительно этого оптимального способа описания $\mathfrak{f}$:

$$K(x|y) \rightleftharpoons K_{\mathfrak{f}}(x|y)\,.$$

Условная сложность, как и безусловная, определена с точностью до ограниченного слагаемого.

Приведём без доказательства основные свойства колмогоровской сложности, которые будут полезны в дальнейшем.

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

2) $\exists C\,\forall x, y\; K(x|y) \leqslant K(x) + C$.

3) Для любой частичной вычислимой функции f
$\exists C\,\forall x\;\big[f(x)$ определено $\;\Rightarrow\; K(f(x)) \leqslant K(x) + C\big]$.

4) Множество $\{\langle x, n\rangle \mid K(x) < n\}$ рекурсивно перечислимо.

5) Множество $\{x \mid K(x) < n\}$ содержит не более $(2^n - 1)$ элементов.

6) $\exists C\,\forall x, y$
$K(\langle x, y\rangle) \leqslant K(x) + K(y|x) + 2\log\min\{K(x), K(y|x)\} + C$.

Глава 2.

Алгоритмические задачи

2.1. Определение и основные свойства

2.1.1. Операции над множествами

Под *алгоритмической задачей* будем понимать произвольное множество двоичных слов, а под *решением задачи* — любой его элемент.

Смысл этого определения можно пояснить следующим образом. Решение любой точно поставленной математической задачи можно записать на некотором подходящем формальном языке. Более того, такая запись должна быть конечной, чтобы её можно было использовать в математической практике. Поэтому можно считать, что любое решение любой задачи закодировано при помощи некоторого двоичного слова. С другой стороны, поскольку мы интересуемся лишь количеством информации в решениях задачи, а не содержательной её стороной, задачу естественно отождествлять с множеством её решений.

Пусть X и Y — произвольные множества двоичных слов. Соответствующие логическим связкам *операции над задачами* опре-

деляются следующим образом.

$$
\begin{aligned}
X \vee Y &= \{\langle 0, x\rangle \mid x \in X\} \cup \{\langle 1, y\rangle \mid y \in Y\}, \\
X \wedge Y &= \{\langle x, y\rangle \mid x \in X, y \in Y\}, \\
X \to Y &= \{p \mid \forall x\, (x \in X \Rightarrow [p](x) \text{ определено и } [p](x) \in Y)\}, \\
\bot &= \varnothing \text{ и} \\
\neg X &= X \to \bot = X \to \varnothing .
\end{aligned}
$$

Для каждой пропозициональной формулы $\Phi(t_1, \ldots, t_k)$ по индукции определяется составная задача $\Phi(X_1, \ldots, X_k)$, получающаяся при подстановке задач $X_1, \ldots, X_k$ вместо переменных $t_1, \ldots, t_k$. Таким образом, каждая формула Φ может рассматриваться как операция, сопоставляющая множество $\Phi(X_1, \ldots, X_k)$ множествам $X_1, \ldots, X_k$.

2.1.2. Интерпретация классической логики

Сначала отметим почти тривиальное свойство введённых операций, которое, однако, позволяет описать в терминах задач классическую логику и технически полезно в дальнейшем.

Сопоставим пустому множеству истинностное значение „ложь“, а всем непустым множествам — истинностное значение „истина“. Тривиально проверяется, что введённые операции над множествами $\vee$, $\wedge$, $\to$, $\neg$ при таком сопоставлении переходят в соответствующие булевские операции над истинностными значениями.

Формула, рассматриваемая как операция над множествами, превращается при этом в соответствующую той же формуле булеву функцию. Отсюда получается следующее простое утверждение (впервые этот факт отметил Плиско в [12]).

Предложение 2.1. *Формула* $\Phi(t_1, \ldots, t_k)$ *является классической тавтологией тогда и только тогда, когда* $\Phi(X_1, \ldots, X_k) \neq \varnothing$ *для любых множеств* $X_1, \ldots, X_k$.

Таким образом, классическая логика состоит из тех формул, для которых соответствующая задача всегда имеет решение.

2.1.3. Интуиционистская логика и реализуемость

По мысли Колмогорова из [16], формула должна считаться интуиционистски приемлемой, если соответствующая задача не просто всегда имеет решение, а имеет единое решение для всех подстановок элементарных задач. То есть для формулы $\Phi(t_1, \ldots, t_k)$ существует такое слово x, что $x \in \Phi(X_1, \ldots, X_k)$ для любых множеств $X_1, \ldots, X_k$. Это определение в более общей ситуации (для предикатных, а не пропозициональных формул) впервые исследовал Плиско в [11], назвавший такие формулы *абсолютно реализуемыми*. Этот вариант реализуемости был введён с целью приспособить реализуемость по Клини (см. [15] и [4, § 82]) для описания конструктивной логики в наиболее общей форме. Очевидно, что всякая абсолютно реализуемая формула реализуема по Клини.

Неизвестно, совпадают ли классы реализуемых и абсолютно реализуемых пропозициональных формул (пример реализуемой, но не абсолютно реализуемой предикатной формулы построил Плиско в [11].) Тем не менее, основные факты о реализуемых формулах, доказанные в работах Клини ([4, § 82]) и Роуза ([18]), переносятся и на случай абсолютной реализуемости.

Следующий факт является аналогом теоремы Нельсона из [4] и точно так же доказывается индукцией по выводу.

Предложение 2.2. *По каждой формуле* $\Phi(t_1, \ldots, t_k)$, *выводимой в* $\mathfrak{Int}$, *можно эффективно построить такое слово* x, *что*

$x \in \Phi(X_1, \ldots, X_k)$ *для любых множеств* $X_1, \ldots, X_k$.

Множество реализуемых формул содержит логику $\mathfrak{Int}$, но не исчерпывается ей. Примером абсолютно реализуемой, но интуиционистски невыводимой пропозициональной формулы служит формула Роуза $\big((\neg\neg\Phi \to \Phi) \to (\neg\Phi \vee \neg\neg\Phi)\big) \to (\neg\Phi \vee \neg\neg\Phi)$, где $\Phi = \neg t_1 \vee \neg t_2$ (её абсолютная реализуемость доказывается точно так же, как её реализуемость в статье Роуза [18]). Неизвестно, является ли класс всех абсолютно реализуемых пропозициональных формул разрешимым (или хотя бы перечислимым).

2.1.4. Сложность алгоритмических задач

Перейдём, наконец, к рассмотрению модифицированного подхода к реализуемости, основанного понятии количества информации.

Сложностью $Ks(X)$ множества двоичных слов X называется минимум колмогоровских сложностей его элементов, то есть $Ks(X) = \min\{K(x) \mid x \in X\}$; сложность пустого множества бесконечно велика: $Ks(\varnothing) = \infty$. Таким образом, сложностью задачи называется сложность её простейшего решения.

Докажем два несложных, но фундаментальных неравенства между сложностями задач, соответствующих формулам.

Предложение 2.3. *Пусть* $\Phi(t_1, \ldots, t_k)$ — *произвольная пропозициональная формула. Существует такая константа* C_Φ, *что для любых множеств* $X_1, \ldots, X_k$, *если* $\Phi(X_1, \ldots, X_k) \neq \varnothing$, *то*

$$Ks\big(\Phi(X_1, \ldots, X_k)\big) \leqslant Ks\Big(\bigwedge_{X_i \neq \varnothing} X_i\Big) + C_\Phi\,.$$

Константа C_Φ *зависит только от вида формулы* Φ, *количества переменных* k *и выбора оптимального способа описания. (Если все* X_i *пусты, можно считать, что в правой части есть только* C_Φ.)

Доказательство. Чтобы доказать неравенство, мы предъявим вычислимую функцию, которая по любому элементу множества $\bigwedge_{X_i \neq \varnothing} X_i$ строит элемент множества $\Phi(X_1, \ldots, X_k)$, и применим свойство 3 колмогоровской сложности, приведённое на странице 32.

Сначала для каждой формулы $\Psi(t_1, \ldots, t_k)$ мы построим вычислимую функцию f_Ψ, которая получает в качестве аргументов k двоичных слов, и обладает следующим свойством. Пусть $X_1, \ldots, X_k$ — произвольные множества, а слова $y_1, \ldots, y_k$ таковы, что для каждого i выполнено одно из двух: либо $y_i = 0x_i$ и $x_i \in X_i$, либо $y_i = 1$ и $X_i = \varnothing$. Тогда если $\Psi(X_1, \ldots, X_k) \neq \varnothing$, то $f_\Psi(y_1, \ldots, y_k) = 0x$ и $x \in \Psi(X_1, \ldots, X_k)$, а если $\Psi(X_1, \ldots, X_k) = \varnothing$, то $f_\Psi(y_1, \ldots, y_k) = 1$.

Функцию f_Ψ определим индукцией по построению формулы Ψ.

1) $\Psi(t_1, \ldots, t_k) = t_i$. Положим $f_\Psi(y_1, \ldots, y_k) = y_i$.

2) $\Psi(t_1, \ldots, t_k) = \bot$. Положим $f_\Psi(y_1, \ldots, y_k) = 1$.

3) $\Psi(t_1, \ldots, t_k) = \Psi_1(t_1, \ldots, t_k) \wedge \Psi_2(t_1, \ldots, t_k)$.
Если $f_{\Psi_1}(y_1, \ldots, y_k) = 0x_1$ и $f_{\Psi_2}(y_1, \ldots, y_k) = 0x_2$, то положим $f_\Psi(y_1, \ldots, y_k) = 0\langle x_1, x_2\rangle$, иначе $f_\Psi(y_1, \ldots, y_k) = 1$.

4) $\Psi(t_1, \ldots, t_k) = \Psi_1(t_1, \ldots, t_k) \vee \Psi_2(t_1, \ldots, t_k)$.
Если $f_{\Psi_1}(y_1, \ldots, y_k) = 0x_1$, то $f_\Psi((y_1, \ldots, y_k)) = 0\langle 0, x_1\rangle$. Иначе если $f_{\Psi_2}(y_1, \ldots, y_k) = 0x_2$, то $f_\Psi(y_1, \ldots, y_k) = 0\langle 1, x_2\rangle$; в оставшемся случае $f_\Psi(y_1, \ldots, y_k) = 1$.

5) $\Psi(t_1, \ldots, t_k) = \Psi_1(t_1, \ldots, t_k) \to \Psi_2(t_1, \ldots, t_k)$.
Если $f_{\Psi_2}(y_1, \ldots, y_k) = 0x_2$, то $f_\Psi(y_1, \ldots, y_k) = 0\lambda z.x_2$. Если $f_{\Psi_1}(y_1, \ldots, y_k) = 0x_1$ и $f_{\Psi_2}(y_1, \ldots, y_k) = 1$, то $f_\Psi(y_1, \ldots, y_k) = 1$. Если же, наконец, $f_{\Psi_1}(y_1, \ldots, y_k) = f_{\Psi_2}(y_1, \ldots, y_k) = 1$, то

$f_\Psi(y_1, \ldots, y_k) = 0\lambda z.0$. (Здесь через $\lambda z.x$ обозначена программа, вычисляющая функцию, тождественно равную x).

Пусть дан элемент множества $\bigwedge_{X_i \neq \varnothing} X_i$. Зная, какие из X_i пусты, можно построить кортеж $y_1, \ldots, y_k$ с требуемым свойством (для каждого i выполнено одно из двух: либо $y_i = 0x_i$ и $x_i \in X_i$, либо $y_i = 1$ и $X_i = \varnothing$). Теперь, используя функцию f_Φ, можно построить элемент множества $\Phi(X_1, \ldots, X_k)$.

В построенном вычислимом отображении использовалась только информация о виде формулы Φ, и k битов, сообщающих, пусто ли соответствующее X_i. □

Предложение 2.4. *Для произвольных множеств X и Y имеет место неравенство*

$$Ks(Y) \leqslant Ks(X \to Y) + Ks(X) + 2\log\min\{Ks(X), Ks(X \to Y)\} + C\,,$$

где константа C зависит только от выбора оптимального способа описания.

Доказательство. Если множество X или множество $X \to Y$ пусто, то правая часть неравенства бесконечна, и поэтому оно выполнено.

Пусть множества X и $X \to Y$ непусты. Заметим, что в этом случае Y тоже непусто. Возьмём элементы $p \in X \to Y$ и $x \in X$, на которых достигается минимум в определении сложности множества, то есть такие, что $K(p) = Ks(X \to Y)$ и $K(x) = Ks(X)$. По определению импликации значение $[p](x)$ определено и принадлежит Y, поэтому $Ks(Y) \leqslant K\big([p](x)\big) \leqslant K(\langle p, x\rangle) + C' \leqslant$ $\leqslant K(p) + K(x) + 2\log\min\{K(p), K(x)\} + C$, где последнее неравенство следует из свойств 2 и 6 колмогоровской сложности, а предпоследнее — из свойства 3, применённого к вычислимой функции $f(\langle p, x\rangle) = [p](x)$. □

2.1.5. Простейшие логические свойства

Предложение 2.1 можно переформулировать в терминах сложности: формула $\Phi(t_1, \ldots, t_k)$ является классической тавтологией тогда и только тогда, когда $Ks(\Phi(X_1, \ldots, X_k))$ конечна для любых множеств $X_1, \ldots, X_k$. Таким образом, классическая логика описывает тривиальное понимание „малости“ количества информации, достаточной для решения задачи — конечная величина мала по сравнению с бесконечной.

Другой крайний вариант понимания „малости“ — сложность всех задач, соответствующих данной формуле, ограничена некоторой константой. То есть рассматривается множество $\mathfrak{L}_{\mathrm{K}}$ таких формул $\Phi(t_1, \ldots, t_k)$, для которых найдётся такая константа C, что для любых множеств $X_1, \ldots, X_k$

$$Ks(\Phi(X_1, \ldots, X_k)) \leqslant C\,.$$

Определение множества $\mathfrak{L}_{\mathrm{K}}$ можно переформулировать и без использования понятия колмогоровской сложности, в духе обычного определения реализуемости. Формула $\Phi(t_1, \ldots, t_k)$ принадлежит множеству $\mathfrak{L}_{\mathrm{K}}$, если найдутся такие слова $x_1, \ldots, x_l$ (их количество может зависеть от формулы), что для любых множеств $X_1, \ldots, X_k$

$$\exists i \in \{1, \ldots, l\} \quad x_i \in \Phi(X_1, \ldots, X_k)$$

(определение абсолютной реализуемости получится, если потребовать $l = 1$).

Эквивалентность этих двух определений очевидна. Если для некоторой формулы Φ сложность $Ks(\Phi(X_1, \ldots, X_k))$ всегда меньше C, то в качестве $x_1, \ldots, x_l$ можно взять все элементы множества $\{x \mid K(x) \leqslant C\}$ (в силу свойства 5 колмогоровской сложности l оказывается меньше 2^C). Наоборот, если множеству $\Phi(X_1, \ldots, X_k)$ все-

гда принадлежит одно из значений $x_1, \ldots, x_l$, то в качестве оценки сложности можно взять $C = \max\{K(x_1), \ldots, K(x_l)\}$.

Столь же легко убедиться, что $\mathfrak{L}_{\mathrm{K}}$ является суперинтуиционистской логикой. Как очевидно из второго варианта определения, множество $\mathfrak{L}_{\mathrm{K}}$ содержит все абсолютно реализуемые формулы, а значит, и $\mathfrak{Int}$. Если $Ks(\Phi(X_1, \ldots, X_k)) \leqslant C$ для любых множеств $X_1, \ldots, X_k$, то это, в частности, выполнено, и для множеств вида $\Psi(Y_1, \ldots, Y_m)$, и $Ks\big(\Phi\big(\Psi_1(Y_1, \ldots, Y_m), \ldots, \Psi_k(Y_1, \ldots, Y_m)\big)\big) \leqslant C$. Таким образом, $\mathfrak{L}_{\mathrm{K}}$ замкнуто относительно подстановок. Если $Ks(\Phi(X_1, \ldots, X_k)) \leqslant C_1$ и $Ks((\Phi \to \Psi)(X_1, \ldots, X_k)) \leqslant C_2$, то в соответствии с предложением 2.4 $Ks(\Psi(X_1, \ldots, X_k)) \leqslant C$ для некоторой константы C, зависящей только от C_1 и C_2. Поэтому $\mathfrak{L}_{\mathrm{K}}$ замкнуто относительно правила *modus ponens*.

Нетрудно проверить, что $\mathfrak{L}_{\mathrm{K}}$ содержит логику $\mathfrak{J}$. Верно даже следующее более сильное утверждение.

Лемма 2.5. *По формуле $\Phi(t_1, \ldots, t_k)$, выводимой в $\mathfrak{J}$, можно эффективно построить такие слова $x_1, \ldots, x_l$, где $l \leqslant 2^k$, что для любых множеств $X_1, \ldots, X_k$*

$$\exists i \in \{1, \ldots, l\} \quad x_i \in \Phi(X_1, \ldots, X_k)\,.$$

Доказательство. Заметим, что множество $Y_1 = \{\langle 0,0\rangle, \langle 1,0\rangle\}$ содержит решение задачи $(\neg X \vee \neg\neg X)$ для любого X, причём $\langle 0,0\rangle \in \neg X \vee \neg\neg X$, если множество X пусто, и $\langle 1,0\rangle \in \neg X \vee \neg\neg X$, если множество X непусто. Поэтому множество $Y_k = \bigwedge_{i=1}^{k} Y_1$ (k-ая степень множества Y_1) содержит решение задачи $\bigwedge_{i=1}^{k}(\neg X_i \vee \neg\neg X_i)$ для любых $X_1, \ldots, X_k$, и каждый элемент множества Y_k является решением этой задачи при некоторых $X_1, \ldots, X_k$.

Поскольку формула $\Phi(t_1, \ldots, t_k)$ выводима в логике $\mathfrak{J}$, из лем-

мы 1.2 следует, что формула

$$\Phi'(t_1,\ldots,t_k) = \bigwedge_{i=1}^{k}(\neg t_i \vee \neg\neg t_i) \to \Phi(t_1,\ldots,t_k)$$

выводима в $\mathfrak{Int}$. Пользуясь предложением 2.2, можно построить такое слово r, что $r \in \Phi'(X_1,\ldots,X_k)$ для любых $X_1,\ldots,X_k$. Множество $Z = \{[r](y) \mid y \in Y_k\}$ будет искомым. Действительно, поскольку все элементы множества Y_k бывают элементами множества $\bigwedge_{i=1}^{k}(\neg X_i \vee \neg\neg X_i)$ при некоторых $X_1,\ldots,X_k$, значения $[r](y)$ определены для всех $y \in Y_k$, поэтому множество Z строится эффективно. Ясно также, что при любых $X_1,\ldots,X_k$ найдётся такое $y \in Y_k$, что $[r](y) \in \Phi(X_1,\ldots,X_k)$. Наконец, $|Z| \leqslant |Y_k| = 2^k$. □

Помимо логики $\mathfrak{L}_{\mathrm{K}}$ можно рассмотреть и логики, порождённые другими ограничениями на сложность задачи, соответствующей формуле. Предложение 2.3 показывает, что естественно сравнить сложность задачи $Ks(\Phi(X_1,\ldots,X_k))$ с величиной $Ks(\bigwedge_{X_i\neq\varnothing} X_i)$. Это соотношение должно быть асимптотическим, чтобы обеспечить инвариантность определения относительно выбора различных оптимальных способов описания.

С каждой формулой $\Phi(t_1,\ldots,t_k)$ свяжем функцию натурального аргумента ka_Φ:

$$\mathrm{ka}_\Phi(n) = \max\Big\{ Ks(\Phi(X_1,\ldots,X_k)) \Big| (\exists i\, X_i \neq \varnothing) \Rightarrow Ks\Big(\bigwedge_{X_i\neq\varnothing} X_i\Big) \leqslant n \Big\}.$$

Из предложения 2.3 следует, что для классически истинных формул $\mathrm{ka}_\Phi(n) \leqslant n + O(1)$.

Логика $\mathfrak{L}_{\mathrm{K}}$ была определена как множество формул, для которых $\mathrm{ka}_\Phi(n) = O(1)$ при $n \to \infty$. Однако можно дать аналогичные определения и для промежуточных границ скорости роста ka_Φ, например, рассмотреть множества таких формул, что

$\mathrm{ka}_\Phi(n) = O(\log n)$, $\mathrm{ka}_\Phi(n) = O(\sqrt{n})$ или $\mathrm{ka}_\Phi(n) = o(n)$. Столь же просто, как и для $\mathfrak{L}_\mathrm{K}$ доказывается, что все эти множества являются суперинтуиционистскими логиками. Неожиданный и нетривиальный факт заключается в том, что эти логики совпадают между собой и с логикой $\mathfrak{J}$. Это утверждение доказывается в следующем разделе.

2.2. Оценки на сложность задач

Лемма 2.5 в некотором смысле полностью описывает сложность задач, соответствующих выводимым в $\mathfrak{J}$ формулам, поскольку сама сложность определена с точностью до ограниченного слагаемого. В этом разделе будут даны точные оценки на максимальную сложность задач, соответствующих формулам, невыводимым в $\mathfrak{J}$.

2.2.1. Нижняя оценка для критических импликаций

Как показано в главе 1, критические импликации занимают особое место среди формул, невыводимых в $\mathfrak{Int}$ и $\mathfrak{J}$. Замечательно, что для них удаётся оценить сложность соответствующей задачи при подстановке одноэлементных множеств.

Теорема 2.1. *Для любой критической импликации $J(s_1, \ldots, s_m)$ найдётся такая константа C, что для произвольных двоичных слов $x_1, \ldots, x_m$ имеет место неравенство*

$$Ks(J(\{x_1\}, \ldots, \{x_m\})) \geqslant \min_j K(x_j | x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m) - C\,.$$

Доказательство. Пусть J — произвольная критическая импликация от m переменных, а $x_1, \ldots, x_m$ — произвольные двоичные слова.

Для упрощения обозначений отождествим в этом доказательстве натуральное число j и его двоичную запись.

Определим вспомогательную m-местную операцию Λ_m над множествами $Y_1, \ldots, Y_m$:

$$\Lambda_m(Y_1, \ldots, Y_m) = \{\langle y_1, \ldots, y_m, q\rangle \mid \forall j\ (y_j \notin Y_j \Rightarrow [q](\varepsilon) = j)\}$$

(иначе говоря, в наборе $y_1, \ldots, y_m$ все слова, за исключением, быть может, одного, принадлежат соответствующим множествам $Y_1, \ldots, Y_m$, а „ошибочное“ слово, если оно есть, будет рано или поздно указано программой q, запущенной на пустом слове).

Лемма 2.6. *Пусть P — непустая конъюнкция, а Q — непустая дизъюнкция некоторых из переменных $s_1, \ldots, s_m$, причём общих переменных у P и Q нет. Тогда найдётся такая константа C_1, что для любых двоичных слов $x_1, \ldots, x_m$*

$$Ks\big(\Lambda_m(\{x_1\}, \ldots, \{x_m\}) \to ((\bar{P} \to \bar{Q}) \to \bar{Q})\big) \leqslant C_1\,,$$

где $\bar{P}$ и $\bar{Q}$ есть результат подстановки одноэлементных множеств $\{x_1\}, \ldots, \{x_m\}$ вместо переменных $s_1, \ldots, s_m$ в P и Q соответственно, а константа C_1 зависит только от формул P, Q и от выбора оптимального способа описания.

Доказательство. Следующий алгоритм находит некоторый элемент из множества $\bar{Q}$ по любому набору $\langle x'_1, \ldots, x'_m, q\rangle$ из множества $\Lambda_m(\{x_1\}, \ldots, \{x_m\})$ и любой программе r, отображающей множество $\bar{P}$ в множество $\bar{Q}$.

Запустим параллельно вычисление q на пустом слове и вычисление r на единственном элементе множества $P(\{x'_1\}, \ldots, \{x'_m\})$. Будем дожидаться наступления первого из следующих двух событий.

1) *Программа r завершила работу и результат принадлежит множеству $Q(\{x'_1\},\ldots,\{x'_m\})$.*

   Тогда выдаём этот результат.

2) *Программы q завершила работу.*

   Пусть результат равен j. Если переменная s_j входит в конъюнкцию P, то выдаём любой элемент из $Q(\{x'_1\},\ldots,\{x'_m\})$, а иначе дожидаемся результата работы r и выдаём его.

Проверим корректность алгоритма.

Если значение q на пустом слове неопределено, то $x'_1 = x_1$, ..., $x'_m = x_m$, $P(\{x'_1\},\ldots,\{x'_m\}) = \bar{P}$, $Q(\{x'_1\},\ldots,\{x'_m\}) = \bar{Q}$, и очевидно, что при работе алгоритма произойдёт первое событие и результат принадлежит $\bar{Q}$.

Пусть значение q на пустом слове определено и равно j. Формулы P и Q не имеют общих переменных, поэтому если переменная s_j входит в конъюнкцию P, то она не входит в дизъюнкцию Q и потому $Q(\{x'_1\},\ldots,\{x'_m\}) = \bar{Q}$, а в противном случае $P(\{x'_1\},\ldots,\{x'_m\}) = \bar{P}$. Таким образом, если раньше наступило второе событие, то алгоритм выдаёт либо элемент из $\bar{Q}$, либо значение r на единственном элементе множества $\bar{P}$ (очевидно, это значение определено). Если же раньше наступило первое событие, то результат верен либо потому, что он принадлежит $\bar{Q}$, либо потому, что он вычислен по элементу множества $\bar{P}$.

Очевидно, что для задания алгоритма достаточно знать только формулы P и Q, а также число m. □

Лемма 2.7. *Для каждого m найдётся такая константа C_2, что*

для любых слов $x_1, \ldots, x_m$

$$Ks(\Lambda_m(\{x_1\}, \ldots, \{x_m\}) \to (\{x_1\} \vee \{x_2\} \vee \ldots \vee \{x_m\})) \geqslant$$
$$\geqslant \min_j \{K(x_j | x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m)\} - C_2 .$$

Доказательство. Каждому двоичному слову u вычислимым образом поставим в соответствие какую-нибудь программу q_u, для которой $[q_u](\varepsilon) = [u](u)$.

Возьмём любой элемент p из множества $\Lambda_m(\{x_1\}, \ldots, \{x_m\}) \to (\{x_1\} \vee \{x_2\} \vee \ldots \vee \{x_m\})$. Рассмотрим значения программы p на аргументах вида $\langle x_1, \ldots, x_m, q_u \rangle \in \Lambda_m(\{x_1\}, \ldots, \{x_m\})$ при всевозможных u. Можно считать, что эти значения при подходящем перекодировании имеют вид $\langle j, x_j \rangle$, где $j \in \{1, \ldots, m\}$. Очевидно, что это j является всюду определённой вычислимой функцией u. Поэтому найдётся такое слово u_0 (а именно, программа этой функции j), что $[u_0](u_0) = j(u_0)$. Обозначим значение $j(u_0)$ через j_0.

Покажем теперь, что зная программу p и число j_0, можно по набору $x_1, \ldots, x_{j_0-1}, x_{j_0+1}, \ldots, x_m$ эффективно построить x_{j_0}. Параллельно для всех пар $\langle u, v \rangle$ будем проверять следующее свойство:

$$[u](u) = j_0 \quad \text{(иначе говоря, } [q_u](\varepsilon) = j_0\text{)}$$

и

$$[p](\langle x_1, \ldots, x_{j_0-1}, v, x_{j_0+1}, \ldots, x_m, q_u \rangle) \text{ имеет вид } \langle j_0, w \rangle$$

(где w — некоторое слово). Возьмём любую пару $\langle u, v \rangle$ с этим свойством (такая обязательно найдётся, например, $u = u_0$ и $v = x_{j_0}$) и рассмотрим соответствующее w. Заметим, что если $[u](u) = j_0$, то при всяком v набор $\langle x_1, \ldots, x_{j_0-1}, v, x_{j_0+1}, \ldots, x_m, q_u \rangle$ принадлежит множеству $\Lambda_m(\{x_1\}, \ldots, \{x_m\})$. Поэтому $w = x_{j_0}$.

Таким образом, $K(x_{j_0} | x_1, \ldots, x_{j_0-1}, x_{j_0+1}, \ldots, x_m) \leqslant K(p) + C_2$, где константа C_2 зависит только от выбора функции K и числа j_0. $\square$

Пусть p' — элемент множества $J(\{x_1\},\ldots,\{x_m\})$. Используя лемму 2.6, нетрудно по программе p' эффективно построить программу p, принадлежащую множеству $\Lambda_m(\{x_1\},\ldots,\{x_m\}) \to (\{x_1\} \vee \ldots \vee \{x_m\})$ (программа p, получив на вход элемент множества $\Lambda_m(\{x_1\},\ldots,\{x_m\})$, строит элементы каждой из посылок $(\bar{P}_i \to \bar{Q}_i) \to \bar{Q}_i$ критической импликации J, а затем применяет к составленному из них кортежу программу p'). Поскольку $K(p) \leqslant K(p') + O(1)$, из леммы 2.7 следует утверждение теоремы. □

Замечание. Доказательство теоремы 2.1 обобщает рассуждение из примера 6 в статье [19]. Чтобы сделать изложение более ясным, здесь введена операция Λ_m, а само доказательство разбито на две леммы.

2.2.2. Классификация формул по сложности порождаемых алгоритмических задач

Из оценки для критических импликаций можно получить общее утверждение для произвольных невыводимых в $\mathfrak{J}$ формул.

Теорема 2.2. *Пусть формула $\Phi(t_1,\ldots,t_k)$ невыводима в логике $\mathfrak{J}$. Если при этом классически истинна формула $\Phi(\bot,\ldots,\bot)$ (вместо всех переменных подставлена константа $\bot$) или формула $\Phi(t_1,\ldots,t_k)$ позитивна, то существует такая константа C, что для любого числа n найдутся конечные множества $X_1,\ldots,X_k$ со свойствами:*

1) среди $X_1,\ldots,X_k$ есть непустые;

2) $Ks\Big(\bigwedge\limits_{X_i\neq\varnothing} X_i\Big) \leqslant n + C$;

3) $Ks(\Phi(X_1,\ldots,X_k)) \geqslant n - C$.

Если формула $\Phi(t_1, \ldots, t_k)$ *позитивна, то можно выбрать непустыми все множества* $X_1, \ldots, X_k$.

Доказательство. Для невыводимой в $\mathfrak{J}$ формулы Φ возьмём число m и формулы $\mathrm{T}_1, \ldots, \mathrm{T}_k$, построенные в теореме 1.3. В силу замечания после теоремы, не все T_i есть $\bot$.

Для данного n выберем какие-нибудь двоичные слова $x_1, \ldots, x_m$ длины n, для которых при всех j выполнено неравенство

$$K(x_j | x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m) \geqslant n - \log_2 m\,.$$

Такие слова обязательно найдутся. Действительно, количество слов, условная сложность которых при фиксированном условии меньше $n - \log_2 m$, не больше $2^n/m - 1$. Количество различных условий вида $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m$ не превышает $2^{n(m-1)}$. Поэтому количество наборов из m двоичных слов длины n, не удовлетворяющих хотя бы одному из m указанных неравенств, не больше $m(2^n/m - 1)2^{n(m-1)} < 2^{nm}$ (где 2^{nm} — количество всех наборов).

Отметим, что для каждого из построенных слов $x_1, \ldots, x_m$ сложность $K(x_i) \leqslant n + C'$ для некоторой константы C', зависящей только от выбора функции K.

Положим $X_i = \mathrm{T}_i(\{x_1\}, \ldots, \{x_m\})$. Отметим, что если $\mathrm{T}_i \neq \bot$, то $X_i = \{x_m\} \vee \ldots$, а иначе X_i пусто. Проверим, что множества X_i имеют требуемые свойства.

Во-первых, поскольку не все T_i есть $\bot$, некоторые из X_i непусты.

Во-вторых, все непустые X_i содержат элемент $\langle 0, x_m \rangle$, следовательно,

$$Ks\Big(\bigwedge_{X_i \neq \varnothing} X_i\Big) \leqslant K(\langle 0, x_m \rangle) \leqslant n + C$$

для некоторой константы C, зависящей только от чисел k и m и выбора функции K.

Наконец, поскольку импликация $\Phi(\mathrm{T}_1, \ldots, \mathrm{T}_k) \to J_m$ выводима в $\mathfrak{Int}$, из предложения 2.2 вытекает, что для любых множеств $Y_1, \ldots, Y_m$

$$Ks\big(\Phi(\mathrm{T}_1(Y_1, \ldots, Y_m), \ldots, \mathrm{T}_k(Y_1, \ldots, Y_m)) \to J_m(Y_1, \ldots, Y_m)\big) \leqslant O(1)\,.$$

Поэтому из предложения 2.4 следует, что

$$Ks(J_m(\{x_1\}, \ldots, \{x_m\})) \leqslant Ks(\Phi(X_1, \ldots, X_k)) + C'\,,$$

где константа C' зависит только от формулы Φ и выбора функции K. Отсюда и из полученной в теореме 2.1 оценки на сложность критической импликации J_m получаем, что

$$Ks(\Phi(X_1, \ldots, X_m)) \geqslant n - C\,.$$

□

Из доказанной теоремы, в частности, вытекает, что $\mathfrak{L}_{\mathrm{K}} = \mathfrak{J}$.

Лемма 2.5, предложение 2.1 (точнее, его переформулировка из раздела 2.1.5) и теорема 2.2 вместе с неравенством из предложения 2.3 дают точную оценку на скорость роста максимальной достижимой сложности составной задачи в зависимости от сложностей подставленных задач. Более строго это можно сформулировать в терминах описания асимптотического поведения функции ka_Φ при $n \to \infty$ для всех возможных формул Φ.

Следствие 2.1.

Если Φ *не выводится в классической логике, то* $\mathrm{ka}_\Phi(n) = \infty$ *при достаточно больших* n.

Если Φ *выводится в* $\mathfrak{J}$, *то* $\mathrm{ka}_\Phi(n) = O(1)$.

Если Φ *не выводится в* $\mathfrak{J}$, *но выводится в классической логике, то* $\mathrm{ka}_\Phi(n) = n + O(1)$.

2.2.3. Верхние оценки для критических импликаций

В статье [19] рассматривалась также следующая задача. Пусть даны двоичные слова $x_1, \ldots, x_k$. Подставим одноэлементные множества $\{x_1\}, \ldots, \{x_k\}$ в формулу $\Phi(t_1, \ldots, t_k)$. В [19] для нескольких формул были найдены равенства (с точностью до константы и до логарифма), которые связывают сложность получающегося множества со сложностями слов $x_1, \ldots, x_k$ и их условными сложностями относительно друг друга.

В частности, это было сделано для критической импликации $((s_1 \to s_2) \to s_2) \to s_1 \vee s_2$. Обобщение использованного там метода позволило доказать нижнюю оценку сложности задач, получающихся при подстановке одноэлементных множеств в произвольную критическую импликацию (теорема 2.1). Для многих (хотя не для всех) критических импликаций удаётся доказать и соответствующую верхнюю оценку.

В частности, доказанная оценка точна, если заключение критической импликации имеет вид $\bigvee_{i=1}^{m} s_i$, а слова $x_1, \ldots, x_m$ независимы (то есть сложность любого из них не уменьшится, если станут известны все остальные; именно такие слова использованы в доказательстве теоремы 2.2):

$$\begin{aligned} Ks(J(\{x_1\}, \ldots, \{x_m\})) \leqslant \\ \leqslant Ks(\{x_1\} \vee \ldots \vee \{x_m\}) + O(1) = \min_j K(x_j) + O(1) = \\ = \min_j K(x_j | x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m) + O(1) \end{aligned}$$

Почти так же легко убедиться, что эта оценка верна для критической импликации J_m и произвольных $x_1, \ldots, x_m$.

Лемма 2.8. *Для каждого m существует такая константа C,*

что для произвольных слов $x_1, \ldots, x_m$ *верна оценка*

$$Ks(J_m(\{x_1\}, \ldots, \{x_m\})) \leqslant \\ \leqslant \min_j K(x_j | x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m) + C\,.$$

Доказательство. Зафиксируем какое-нибудь $j \in \{1, \ldots, m\}$ и докажем, что

$$Ks(J_m(\{x_1\}, \ldots, \{x_m\})) \leqslant K(x_j | x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m) + C\,.$$

Очевидно, отсюда будет следовать утверждение леммы.

Пусть слово y позволяет найти x_j при известных остальных словах $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m$. Очевидно, по y можно построить программу $f \in (\bigwedge_{i \neq j} x_i \to x_j)$, и $K(f) \leqslant K(y) + O(1)$, где слагаемое $O(1)$ зависит только от выбора функции K.

Для f построим следующую программу $p_f \in J_m(\{x_1\}, \ldots, \{x_m\})$. Эта программа получает на вход кортеж элементов, принадлежащих посылкам критической импликации J_m. Заметим, что среди этих посылок есть формула $((\bigwedge_{i \neq j} s_i) \to s_j) \to s_j$. Обозначим через r тот элемент входного кортежа, который соответствует этой посылке (для корректных входов он принадлежит множеству $((\bigwedge_{i \neq j} \{x_i\}) \to \{x_j\}) \to \{x_j\})$. Программа p_f выдаёт значение $\langle j, [r](f) \rangle$ (если оно определено).

Очевидно, что $Ks(J_m(\{x_1\}, \ldots, \{x_m\})) \leqslant K(p_f) \leqslant K(f) + O(1) \leqslant$ $\leqslant K(y) + O(1)$. С другой стороны, можно выбрать y так, что $K(y) \leqslant K(x_j | x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m) + O(1)$. □

Очевидно, что доказательство изложенной леммы проходит для любой критической импликации от переменных $s_1, \ldots, s_m$, у которой заключение имеет вид $\bigvee_{i=1}^m s_i$, а среди посылок есть формулы $((\bigwedge_{i \neq j} s_i) \to s_j) \to s_j$ для всех $j \in \{1, \ldots, m\}$. Однако и в том случае, если для какого-то одного j посылка указанного вида отсут-

ствует, утверждение остаётся верным, хотя с меньшей точностью, а доказательство становится существенно сложнее.

Теорема 2.3. *Пусть $J(s_1, \ldots, s_m)$ — критическая импликация, $m \geqslant 2$. Пусть существует такое l, что для всех $j \in \{1, \ldots, m\}$, $j \neq l$ среди посылок J есть формула $((\bigwedge_{i \neq j} s_i) \to s_j) \to s_j$. Тогда существует такая константа C, что для произвольных слов $x_1, \ldots, x_m$ верна оценка*

$$Ks(J(\{x_1\}, \ldots, \{x_m\})) \leqslant \\ \leqslant \min_{j \in V} K(x_j | x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m) + 2 \log \max_j K(x_j) + C\,,$$

где V — множество индексов тех переменных, которые входят в дизъюнкцию R, являющуюся заключением критической импликации.

Доказательство. Для упрощения обозначений будем считать, что $l = m$. Если это не так, переименуем переменные, это приведёт только к замене формулы J на другую критическую импликацию с указанными в условии свойствами.

Доказательство разобьём на две леммы. Их можно назвать обратными к леммам из доказательства теоремы 2.1. Используемая здесь операция Λ_m определена на странице 43.

Начнём с более простой леммы, обратной к лемме 2.7.

Лемма 2.9. *Для всякого m существует такая константа C', что для любого $j \in \{1, \ldots, m\}$*

$$Ks(\Lambda_m(\{x_1\} \ldots \{x_m\}) \to \{x_j\}) \leqslant \\ \leqslant K(x_j | x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m) + C'\,.$$

Доказательство. Для данного j возьмём формулы $P = \bigwedge_{i \neq j} s_i$ и $Q = s_j$ и рассмотрим соответствующие множества $\bar{P} = \bigwedge_{i \neq j} \{x_i\}$ и

$\bar{Q} = \{x_j\}$. В силу леммы 2.6

$$Ks\big(\Lambda_m(\{x_1\},\ldots,\{x_m\}) \to ((\bar{P} \to \bar{Q}) \to \bar{Q})\big) \leqslant O(1)\,.$$

Отсюда, пользуясь выводимой в $\mathfrak{Int}$ формулой $(t_1 \to (t_2 \to t_3)) \leftrightarrow (t_2 \to (t_1 \to t_3))$ и предложениями 2.2 и 2.4, получаем

$$Ks(\Lambda_m(\{x_1\},\ldots,\{x_m\}) \to \bar{Q}) \leqslant Ks(\bar{P} \to \bar{Q}) + O(1)\,.$$

Осталось заметить (фактически это уже использовалось в лемме 2.8), что

$$Ks(\bigwedge_{i\neq j}\{x_i\} \to \{x_j\}) \leqslant K(x_j|x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_m) + O(1)$$

□

Следующее утверждение в основном доказано в статье [19] (пример 3), хотя в несколько иной формулировке.

Лемма 2.10. *Существует такая константа C, что для любых двоичных слов x и y, если $N \geqslant \max\{K(x), K(y)\}$, то*

$$Ks((((\{x\} \to \{y\}) \to \{y\}) \to \Lambda_2(\{x\},\{y\})) \leqslant K(N) + C\,.$$

Доказательство. Опишем алгоритм, который по любой программе $r \in ((\{x\} \to \{y\}) \to \{y\})$ строит такие слова x', y', что либо $x' = x$, либо $y' = y$, и программу q со свойством: если $x' \neq x$, то $[q](\varepsilon) = 1$, а если $y' \neq y$, то $[q](\varepsilon) = 2$. Сначала будем считать, что число N больше *длин* слов x и y. Потом объясним, как изменить алгоритм для случая, указанного в условии, когда N больше сложностей этих слов.

Пусть A_N — множество слов длины не больше N. Каждой конечной функции, отображающей множество A_N в себя, вычислимым образом поставим в соответствие некоторую программу, её

вычисляющую. Для краткости отождествим функции с соответствующими программами.

Назовём пару $\langle x', y' \rangle \in A_N \times A_N$ *совместимой* с программой $r \in ((\{x\} \to \{y\}) \to \{y\})$, если для всякой функции $g\colon A_N \to A_N$ такой, что $g(x') = y'$, значение $[r](g)$ определено и равно y'. Очевидно, что пара $\langle x, y \rangle$ совместима с r. Очевидно также, что множество пар, совместимых с r, можно перечислить по данному r.

Строим $\langle x', y', q \rangle$. Перечисляем совместимые с r пары, первую найденную и назовём $\langle x', y' \rangle$. Программа q на входе ε работает так. Она тоже перечисляет совместимые с r пары, но не останавливается, найдя $\langle x', y' \rangle$, а продолжает перечисление. Если будет найдена другая пара $\langle x'', y'' \rangle$, программа q останаваливается и выдаёт 1 при $x' \neq x''$, а при $x' = x''$ выдаёт 2. Описание алгоритма завершено.

Докажем его корректность. Существует по крайней мере одна пара, совместимая с r (а именно, $\langle x, y \rangle$), поэтому какая-то пара $\langle x', y' \rangle$ будет найдена.

Заметим теперь, что если $\langle x_1, y_1 \rangle$ и $\langle x_2, y_2 \rangle$ — различные совместимые с r пары, то либо $x_1 = x_2$, либо $y_1 = y_2$. Действительно, пусть $x_1 \neq x_2$, тогда существует функция g, для которой $g(x_1) = y_1$ и $g(x_2) = y_2$. В силу совместимости с r имеем $[r](g) = y_1$ и $[r](g) = y_2$, то есть $y_1 = y_2$.

Отсюда следует, что для найденной алгоритмом пары $\langle x', y' \rangle$ либо $x = x'$, либо $y = y'$ (возможно, выполнены оба равенства). Осталось проверить правильность работы q. Пусть, например, $x \neq x'$ (и $y = y'$). Тогда существуют по меньшей мере две пары, совместимые с r, и q завершит работу. Если $x' \neq x''$, то $[q](\varepsilon) = 1$, что правильно. Противоположный случай, то есть $x' = x''$ и $y' \neq y''$, невозможен: тогда $x \neq x''$, $y \neq y''$, то есть у двух совместимых с r пар $\langle x, y \rangle$ и $\langle x'', y'' \rangle$ обе компоненты различны. Корректность алго-

ритма доказана. Очевидно, что для его задания достаточно знать число N.

Опишем теперь, как надо изменить алгоритм, если N — не оценка на длины x и y, а оценка на их сложности. Для этого перейдём от самих слов к их описаниям.

Пусть $\mathfrak{f}$ — оптимальный способ описания, соответствующий используемой функции сложности K. Обозначим через $\mathfrak{f}^{-1}$ вычислимую функцию, которая устроена следующим образом: получив на вход слово z, она начинает параллельно на всех элементах множества A_N вычислять функцию $\mathfrak{f}$, пока для какого-нибудь c не обнаружится $\mathfrak{f}(c) = z$; это c выдаётся в качестве значения $\mathfrak{f}^{-1}$ на слове z (если такого c не найдётся, то $\mathfrak{f}^{-1}$ не определена на z). Заметим, что $\mathfrak{f}^{-1}$ определена на x и y, поскольку у них есть описания длины не больше N. Обозначим $a = \mathfrak{f}^{-1}(x)$, $b = \mathfrak{f}^{-1}(y)$.

Теперь по программе $r \in ((\{x\} \to \{y\}) \to \{y\})$ построим программу $\tilde{r} \in ((\{a\} \to \{b\}) \to \{b\})$. Тогда, применив к $\tilde{r}$ ранее описанный алгоритм, можно найти $\langle a', b', q\rangle$. Положим $x' = \mathfrak{f}(a')$, $y' = \mathfrak{f}(b')$ (для $\tilde{r}$, которое строится далее, значения $\mathfrak{f}(a')$ и $\mathfrak{f}(b')$ определены). Очевидно, что набор $\langle x', y', q\rangle$ — искомый.

Программа $\tilde{r}$ действует следующим образом: получив на вход программу $\tilde{g}$, она преобразует её в программу $g = \mathfrak{f} \circ \tilde{g} \circ \mathfrak{f}^{-1}$ (здесь $\circ$ обозначает композицию программ), применяет к g программу r, и затем к результату применяет $\mathfrak{f}^{-1}$; результат последнего действия выдаётся в качестве ответа. Схема преобразования функций $\tilde{g}$ в g и r в $\tilde{r}$ наглядно показана на диаграмме.

$$\begin{array}{ccc} a & \xrightarrow{\tilde{g}} & b \\ {\scriptstyle \mathfrak{f}^{-1}}\uparrow & & \downarrow{\scriptstyle \mathfrak{f}} \\ x & \xrightarrow[g]{} & y \end{array} \qquad\qquad \begin{array}{ccc} \tilde{g} & \xrightarrow{\tilde{r}} & b \\ \downarrow & & \uparrow{\scriptstyle \mathfrak{f}^{-1}} \\ g & \xrightarrow[r]{} & y \end{array}$$

Очевидно, что преобразование r в $\tilde{r}$ вычислимо. Покажем, что

если $r \in ((\{x\} \to \{y\}) \to \{y\})$, то $\tilde{r} \in ((\{a\} \to \{b\}) \to \{b\})$. Заметим, что если $\tilde{g} \in (\{a\} \to \{b\})$, то $g \in (\{x\} \to \{y\})$, так как $\mathfrak{f}^{-1}(x) = a$, $\tilde{g}(a) = b$ и $\mathfrak{f}(b) = y$. Теперь для любого $\tilde{g} \in (\{a\} \to \{b\})$ имеем $[r](g) = y$, $\mathfrak{f}^{-1}(y) = b$, то есть $\tilde{r} \in ((\{a\} \to \{b\}) \to \{b\})$. $\square$

Теперь можно доказать утверждение, парное к лемме 2.6. Оно обобщает предыдущую лемму на случай $m > 2$.

Лемма 2.11. *Существует такая константа C, что для любых двоичных слов $x_1, \ldots, x_m$ выполнено неравенство*

$$Ks\Big(\bigwedge_{j=1}^{m-1} \big((\bigwedge_{i\neq j} \{x_i\} \to \{x_j\}) \to \{x_j\}\big) \to \Lambda_m(\{x_1\} \ldots \{x_m\})\Big) \leqslant$$

$$\leqslant \log \max_j K(x_j) + C\,.$$

Доказательство. Опишем алгоритм, который по любому набору таких элементов $r_1, \ldots, r_{m-1}$, что $r_j \in (\bigwedge_{i\neq j}\{x_i\} \to \{x_j\}) \to \{x_j\}$, строит слова $x'_1, \ldots, x'_m$ и программу q со свойствами: неравенство $x'_i \neq x_i$ возможно не более чем для одного j, и если $x'_i \neq x_i$, то $[q](\varepsilon) = i$.

Отметим, что

$$\bigwedge_{i\neq j}\{x_i\} = \{\langle x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m\rangle\}\,.$$

Таким образом, каждое из r_j принадлежит соответствующему множеству вида $(\{z\} \to \{x_j\}) \to \{x_j\}$. Пользуясь леммой 2.10, для каждого $j \in \{1, \ldots, m-1\}$ преобразуем r_j в слово

$$\big\langle \big\langle x_1^{(j)}, \ldots, x_{j-1}^{(j)}, x_{j+1}^{(j)}, \ldots, x_m^{(j)}\big\rangle, x_j^{(j)}, q^{(j)}\big\rangle\,,$$

которое (для корректных r_j) принадлежит множеству

$$\Lambda_2(\langle x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m\rangle, x_j)\,,$$

и дальше будем работать только с набором этих слов. Для сокращения записи введём обозначение

$$\vec{x}^{\,(j)} = \langle x_1^{(j)}, \ldots, x_m^{(j)} \rangle .$$

Запустим параллельно для всех $j \in \{1, \ldots, m-1\}$ вычисление $[q^{(j)}](\varepsilon)$. Для каждого шага вычисления будем называть j определившимся, если вычисление $[q^{(j)}](\varepsilon)$ завершилось к этому шагу, а прочие будем называть неопределившимися.

Если на некотором шаге для какого-то определившегося j обнаружено, что $[q^{(j)}](\varepsilon) = 2$, то алгоритм выдаёт $\langle x_1^{(j)}, \ldots, x_m^{(j)}, q \rangle$, где q — программа, которая на пустом слове останавливается и выдаёт j; работа алгоритма на этом завершается.

Пусть на некотором шаге для всех неопределившихся j наборы $\vec{x}^{\,(j)}$ совпадают между собой и равны некоторому $\langle y_1, \ldots, y_m \rangle$ (в частности, это выполнено, если осталось только одно неопределившееся j).

Если для какого-то из уже определившихся j_0 выполнено неравенство $y_{j_0} \neq x_{j_0}^{(j_0)}$, то алгоритм выдаёт $\langle x_1^{(1)}, \ldots, x_{m-1}^{(m-1)}, \varepsilon, q \rangle$, где q — программа, которая на пустом слове останавливается и выдаёт m; работа алгоритма на этом завершается.

В противном случае, то есть если для всех уже определившихся j выполнены равенства $y_j = x_j^{(j)}$, алгоритм выдаёт $\langle y_1, \ldots, y_m, q \rangle$ и завершает работу. При этом q — программа, на пустом слове работающая следующим образом. Она запускает параллельное вычисление $[q^{(j)}](\varepsilon)$. Если для какого-нибудь j обнаружилось $[q^{(j)}](\varepsilon) = 2$, она выдаёт j. Если для всех $j \in \{1, \ldots, m-1\}$ обнаружилось $[q^{(j)}](\varepsilon) = 1$, она выдаёт m.

Описание алгоритма завершено. Докажем его корректность.

Сначала заметим, что если для какого-то j обнаружено, что $[q^{(j)}](\varepsilon) = 2$, то в соответствии с определением операции Λ_2 это

означает, что

$$\langle x_1^{(j)}, \ldots, x_{j-1}^{(j)}, x_{j+1}^{(j)}, \ldots, x_m^{(j)} \rangle = \langle x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m \rangle ,$$

и очевидно, что в этом случае результат работы алгоритма правилен.

Пусть к некоторому шагу для определившихся j обнаружено, что $[q^{(j)}](\varepsilon) = 1$ (и следовательно, $x_j^{(j)} = x_j$), а для остальных j все наборы $\vec{x}^{\,(j)}$ равны $y_1, \ldots, y_m$.

Если для какого-то из уже определившихся j_0 выполнено неравенство $y_{j_0} \neq x_{j_0}^{(j_0)}$, то $y_{j_0} \neq x_{j_0}$. Следовательно, для всех неопределившихся j (заметим, что они не равны j_0) выполнено

$$\langle x_1^{(j)}, \ldots, x_{j-1}^{(j)}, x_{j+1}^{(j)}, \ldots, x_m^{(j)} \rangle \neq \langle x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m \rangle ,$$

и в соответствии с определением операции Λ_2 это означает, что $x_j^{(j)} = x_j$. Таким образом, $x_j^{(j)} = x_j$ для всех $j \in \{1, \ldots, m-1\}$, и опять очевидно, что результат работы алгоритма правилен и этом случае.

Докажем, что результат верен и в последнем оставшемся случае, когда для всех уже определившихся j выполнены равенства $y_j = x_j^{(j)}$. Если хотя бы для одного j вычисление $[q^{(j)}](\varepsilon)$ не останавливается (заметим, что это j не могло быть определившимся к моменту завершения работы алгоритма), то для этого j имеем $\langle x_1^{(j)}, \ldots, x_{j-1}^{(j)}, x_{j+1}^{(j)}, \ldots, x_m^{(j)} \rangle = \langle x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m \rangle$ и $x_j^{(j)} = x_j$, поэтому $y_i = x_i^{(j)} = x_i$ для всех i. Если для какого-нибудь j обнаруживается, что $[q^{(j)}](\varepsilon) = 2$ (опять-таки, это j не могло быть определившимся к моменту завершения работы алгоритма), то $y_i = x_i^{(j)} = x_i$ для всех $i \neq j$. Если же для всех $j \in \{1, \ldots, m-1\}$ обнаруживается $[q^{(j)}](\varepsilon) = 1$, то $y_i = x_i^{(i)} = x_i$ для всех $i \neq m$.

Осталось объяснить, почему алгоритм всегда заканчивает работу. Если алгоритм работает бесконечно, это означает, что по

крайней мере для двух значений j, во-первых, не останавливаются $[q^{(j)}](\varepsilon)$, а во-вторых, среди наборов $\vec{x}^{\,(j)}$ есть различные. Но, как уже было отмечено, из первого условия следует, что $x_i^{(j)} = x_i$ для всех i. Поэтому все наборы $\vec{x}^{\,(j)}$ должны совпадать между собой, поскольку они равны $\langle x_1, \ldots, x_m \rangle$.

Очевидно, что для осуществления описанного алгоритма достаточно знать лишь число $\max_j K(x_j)$ (или любое большее), нужное для применения леммы 2.10. □

Итак, для всякого $j_0 \in \{1, \ldots, m\}$

$$Ks\Big(\bigwedge_{j=1}^{m-1}\big((\bigwedge_{i\neq j}\{x_i\}\to\{x_j\})\to\{x_j\}\big)\to\{x_{j_0}\}\Big)\leqslant$$
$$\leqslant K(x_{j_0}|x_1,\ldots,x_{j_0-1},x_{j_0+1},\ldots,x_m)+2\log\max_j K(x_j)+C\,.$$

Для доказательства достаточно дважды применить предложение 2.4, сначала к интуиционистской тавтологии $(t_1 \to t_2) \to ((t_2 \to t_3) \to (t_1 \to t_3))$ и формуле из леммы 2.11, а затем к результату предыдущего шага и формуле из леммы 2.9. Возникающее при этом слагаемое вида $2\log\log\max_j K(x_j)$ оценим величиной $\log\max_j K(x_j) + O(1)$.

Если в заключении внешней импликации из левой части неравенства добавить несколько дизъюнктивных членов (чтобы получилась дизъюнкция R из заключения рассматриваемой критической импликации J), то сложность в левой части не увеличится. Если в посылке добавить конъюнктивные члены (в соответствии со структурой J), сложность опять-таки не увеличится. Таким образом, имеем для всякого j_0 — индекса переменной из дизъюнкции

R:

$$Ks(J(\{x_1\},\ldots,\{x_m\})) \leqslant$$
$$\leqslant K(x_{j_0}|x_1,\ldots,x_{j_0-1},x_{j_0+1},\ldots,x_m) + 2\log\max_j K(x_j) + C\,.$$

Взяв минимум из величин в правой части, получим утверждение теоремы. □

2.2.4. О мощности множеств, на которых достигается нижняя оценка сложности

В теореме 2.2 построены конечные множества, на которых достигается максимум из определения функции ka_Φ со стр. 41. Представляет некоторый интерес вопрос о возможной мощности таких множеств. Ограничимся здесь только непустыми множествами (поскольку только для непустых множеств утверждения о сложности являются содержательными) и позитивными формулами.

Начнём с рассмотрения простого примера. Формула $\Phi(t,s) = ((t \to s) \to t) \to t$ известна в классической логике как закон Пирса. Она невыводима в $\mathfrak{J}$. В примере 5 из статьи [19] показано, что для любых двоичных слов x и y имеет место неравенство

$$Ks(\Phi(\{x\},\{y\})) \leqslant O(\log(K(x)+K(y)))$$

(метод доказательства то же, что и в лемме 2.10).

С другой стороны, интуиционистски выводима импликация $\Phi(t \vee s, s) \to J_2(t,s)$, поэтому для множеств $X = \{x,y\}$ и $Y = \{y\}$ из теоремы 2.1 следует, что

$$\Phi(X,Y) \geqslant \min\{K(x|y), K(y|x)\} - O(1)\,,$$

а действуя, как в теореме 2.2, можно взять x и y длины n, у которых $\min\{K(x|y), K(y|x)\} \geqslant n-1$.

Таким образом, для закона Пирса максимальное значение функции ka_Φ может быть достигнуто на множествах, в которых не более двух элементов, но не на одноэлементных множествах.

Доказательство теоремы 2.2 позволяет получить оценку мощности подставляемых множеств, для которых сложность составной задачи достигает n. Эти подставляемые множества имеют вид дизъюнкции конъюнкций некоторых из m одноэлементных множеств. Количество различных конъюнкций, очевидно, не превышает 2^m, а каждая конъюнкция одноэлементных множеств сама состоит ровно из одного элемента. Таким образом, подставляемые множества имеют мощность не более 2^m. Число m зависит только от формулы Φ, и оценка на него даётся леммой 1.7: $m \leqslant 2^{N(\Phi)+4k+1} + 3$, где $N(\Phi)$ — количество всех подформул формулы Φ. Таким образом, мощности подставляемых множеств ограничены величиной, не зависящей от требуемой сложности составной задачи. (А колмогоровская сложность любого элемента этих множеств ограничена линейной функцией от требуемой сложности составной задачи.)

Для каждой позитивной формулы, невыводимой в $\mathfrak{Int}$ можно поставить вопрос о наименьшей константе $S = S(\Phi)$, для которой функция

$$f_{\Phi,S}(n) = \max\left\{ Ks(\Phi(X_1,\ldots,X_k)) \,\middle|\, Ks\left(\bigwedge_{i=1}^{k} X_i\right) \leqslant n \& \forall i\ 0 < |X_i| \leqslant S \right\}$$

асимптотически равна $n + O(1)$.

Рассмотрим один пример вычисления $S(\Phi)$. Для произвольной критической импликации J с m переменными воспользуемся подстановкой из леммы 1.9 в доказательстве теоремы 2.2. Получим набор множеств $X_i = \{x_{m+2}, \langle x_i, x_{m+1}\rangle\}$, что даёт оценку $S(J) \leqslant 2$. Нетрудно убедиться, что $S(J_m) = 2$ при $m \geqslant 2$.

Действительно, предположим, что $S(J_m) = 1$, то есть для всякого n существуют множества $X_1 = \{x_1\}, \ldots, X_m = \{x_m\}$, для которых $Ks(J_m(X_1, \ldots, X_m)) \geqslant n - O(1)$ и $Ks(\bigwedge_{i=1}^m X_i) \leqslant n + O(1)$. Как показывает лемма 2.8,

$$Ks(J_m(X_1, \ldots, X_m)) \leqslant \min_j K(x_j | x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m) + O(1)\,.$$

Несколько раз применяя свойство 6 колмогоровской сложности, получим цепочку неравенств

$$\begin{aligned} Ks(\bigwedge_{i=1}^m X_i) &= K(\langle x_1, \ldots, x_m \rangle) \geqslant \\ &\geqslant K(x_m | x_1, \ldots, x_{m-1}) + K(\langle x_1, \ldots, x_{m-1} \rangle) - O(\log n) \geqslant \\ &\geqslant K(x_m | x_1, \ldots, x_{m-1}) + K(x_{m-1} | x_1, \ldots, x_{m-2}) + \\ &\qquad + K(\langle x_1, \ldots, x_{m-2} \rangle) - O(\log n) \geqslant \\ &\qquad \ldots \\ &\qquad \geqslant \sum_{j=1}^m K(x_j | x_1, \ldots, x_{j-1}) - O(\log n)\,. \end{aligned}$$

Так как для любого $j \in \{1, \ldots, m\}$

$$\begin{aligned} K(x_j | x_1, \ldots, x_{j-1}) &\geqslant K(x_j | x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m) - O(1) \geqslant \\ &\geqslant \min_j K(x_j | x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m) - O(1)\,, \end{aligned}$$

получаем, что

$$\min_j \{K(x_j | x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m)\} \leqslant n/m + O(\log n)\,,$$

поэтому $f_{J_m,1}(n) \leqslant n/m + O(\log n) \ll n + O(1)$. Противоречие.

Применяя теорему 2.3, можно показать, что $S(J) \neq 1$ и для некоторых других критических импликаций.

Глава 3.

Финитные задачи

Ю. Т. Медведев в статье [7] рассмотрел формализацию идеи Колмогорова об операциях над задачами, существенно отличающуюся от реализуемости. Эта формализация использует не алгоритмические, а чисто комбинаторные понятия. Основой её служат задачи, названные Медведевым финитными.

Содержательно под финитной задачей понимается всякая задача, решение которой является элементом некоторого заданного заранее непустого класса. Например, каждому высказыванию можно сопоставить задачу определения того, истинно оно или ложно. Возможными решениями таких задач являются два значения — истина и ложь, а множество правильных каждой такой задачи решений состоит ровно из одного значения.

Формально финитная задача полностью задаётся двумя множествами — множеством решений, возможных априори, и множеством правильных решений.

Операции над финитными задачами определяются, в терминах действий над конечными множествами. Существенное отличие интерпретации с помощью финитных задач от реализуемости заключается в определении импликации. В случае реализуе-

мости импликация интерпретируется вычислимыми частичными функциями, которые заданы своими программами. В определении импликации финитных задач используются функции, определённые на всех элементах конечного множества воможных решений. Эти функции заданы как множество пар, состоящих из аргумента функции и её значения на этом аргументе.

3.1. Основные свойства финитных задач

3.1.1. Определение

Для произвольных множеств X и Y обозначим $X \times Y$ их декартово произведение. Пары, являющиеся его элементами будем обозначать $\langle\!\langle x, y \rangle\!\rangle$ (чтобы отличать их от кодов пар двоичных слов, обозначенных $\langle x, y \rangle$). Через $X \sqcup Y$ обозначим дизъюнктное объединение $(\{0\} \times X) \cup (\{1\} \times Y)$. Через Y^X обозначим множество функций из X в Y (функция рассматривается как подмножество декартова произведения $X \times Y$).

Финитной задачей называется пара множеств $\langle\!\langle F, X \rangle\!\rangle$, где F — произвольное конечное непустое множество, а X — произвольное подмножество F (возможно, пустое или совпадающее со всем F). Множество F будет далее называться *типом* задачи, а X — множеством её решений. Для финитной задачи A её тип обозначается через $\varphi[A]$, а множество решений — через $\chi[A]$.

Пусть $A_1 = \langle\!\langle F_1, X_1 \rangle\!\rangle$ и $A_2 = \langle\!\langle F_2, X_2 \rangle\!\rangle$ — произвольные финитные задачи. Определим операции над финитными задачами, соот-

ветствующие логическим связкам.

$$\begin{aligned} A_1 \wedge A_2 &= \langle\!\langle F_1 \times F_2, X_1 \times X_2 \rangle\!\rangle ; \\ A_1 \vee A_2 &= \langle\!\langle F_1 \sqcup F_2, X_1 \sqcup X_2 \rangle\!\rangle ; \\ A_1 \to A_2 &= \langle\!\langle F_2^{F_1}, \{ f \in F_2^{F_1} \mid \forall x \, (x \in X_1 \Rightarrow f(x) \in X_2) \} \rangle\!\rangle ; \\ \bot &= \langle\!\langle \{0\}, \varnothing \rangle\!\rangle , \\ \neg A_1 &= A_1 \to \bot . \end{aligned}$$

Для любой пропозициональной формулы $\Theta(t_1, \ldots, t_k)$ и любых финитных задач $A_1, \ldots, A_k$ финитная задача $\Theta(A_1, \ldots, A_k)$ определяется индукцией по построению формулы Θ.

Из определения очевидно следует, что тип финитной задачи $\Theta(A_1, \ldots, A_k)$ зависит только от типов финитных задач $A_1, \ldots, A_k$, поэтому удобно наряду с операцией над финитными задачами ввести также соответствующую формуле Θ операцию над типами $\varphi[\Theta]$. Для любых финитных задач $A_1, \ldots, A_k$ при этом выполнено

$$\varphi[\Theta](\varphi[A_1], \ldots, \varphi[A_k]) = \varphi[\Theta(A_1, \ldots, A_k)] .$$

3.1.2. Утверждения о корректности

Интуитивно понятно, что неважно, из каких именно элементов состоит некоторый тип, а существенные для логики свойства финитных задач определяются лишь мощностями типов. Для обоснования коррекности последующих определений полезна следующая формализация этого утверждения.

Предложение 3.1. *Пусть $F_1, \ldots, F_k$ — некоторые непустые конечные множества. Пусть $F'_1, \ldots, F'_k$ — равномощные им множества, и функции $\alpha_1, \ldots, \alpha_k$ осуществляют биекцию F_i на F'_i. Тогда по любой формуле $\Theta(t_1, \ldots, t_k)$ можно построить биективную функцию α, которая отображает множество $\varphi[\Theta](F_1, \ldots, F_k)$ на*

множество $\varphi[\Theta](F'_1, \ldots, F'_k)$ *и имеет следующее свойство. Если* $X_1, \ldots, X_k$ *— произвольные подмножества* $F_1, \ldots, F_k$*, и функции* $\alpha_1, \ldots, \alpha_k$ *отображают их на соответствующие* $X'_1, \ldots, X'_k$ *— подмножества* $F'_1, \ldots, F'_k$*, то функция* α *отображает множество* $\chi[\Theta(\langle\!\langle F_1, X_1\rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k\rangle\!\rangle)]$ *на* $\chi[\Theta(\langle\!\langle F'_1, X'_1\rangle\!\rangle, \ldots, \langle\!\langle F'_k, X'_k\rangle\!\rangle)]$.

Доказательство. Для каждой формулы Θ, все переменные которой содержатся среди $t_1, \ldots, t_k$, индукцией построим функцию α_Θ.

1) $\Theta = t_i$.
   Положим $\alpha_\Theta = \alpha_i$.

2) $\Theta = \bot$.
   В качестве α_Θ возьмём тождественную функцию на множестве $\{0\}$.

3) $\Theta = \Theta_1 \vee \Theta_2$.
   Положим $\alpha_\Theta(\langle\!\langle 0, x\rangle\!\rangle) = \langle\!\langle 0, \alpha_{\Theta_1}(x)\rangle\!\rangle$, а $\alpha_\Theta(\langle\!\langle 1, y\rangle\!\rangle) = \langle\!\langle 1, \alpha_{\Theta_2}(y)\rangle\!\rangle$.

4) $\Theta = \Theta_1 \wedge \Theta_2$.
   Положим $\alpha_\Theta(\langle\!\langle x, y\rangle\!\rangle) = \langle\!\langle \alpha_{\Theta_1}(x), \alpha_{\Theta_2}(y)\rangle\!\rangle$.

5) $\Theta = \Theta_1 \to \Theta_2$.
   Положим $\alpha_\Theta(f) = \alpha_{\Theta_2} \circ f \circ \alpha_{\Theta_1}^{-1}$, где $\circ$ обозначает композицию функций; поскольку α_{Θ_1} — биекция, обратное отображение определено однозначно.

Легко проверить, что построенная функция обладает требуемыми свойствами. □

В определениях финитной задачи, соответствующей константе $\bot$, и дизъюнкции финитных задач, есть некоторый произвол — там встречаются множества $\{0\}$ и $\{1\}$. Понятно, что использование именно этих множеств не обусловлено содержательно, и для $\bot$

вместо $\{0\}$ можно использовать любое непустое конечное множество, а для дизъюнкции вместо множеств $\{0\}$ и $\{1\}$ можно использовать любые непересекающиеся непустые конечные множества. Следующие два предложения формализуют это наблюдение.

Предложение 3.2. *Пусть G_1 и G_2 — непустые конечные множества. Для произвольной формулы $\Theta(t_1, \ldots, t_k)$ и финитных задач $A_1, \ldots, A_k$ обозначим через $\Theta^{(1)}(A_1, \ldots, A_k)$ финитную задачу, полученную в результате подстановки вместо константы $\bot$ задачи $\langle\!\langle G_1, \varnothing \rangle\!\rangle$, а вместо переменных — задач $A_1, \ldots, A_k$. Аналогично через $\Theta^{(2)}(A_1, \ldots, A_k)$ обозначим результат подстановки вместо константы $\bot$ задачи $\langle\!\langle G_2, \varnothing \rangle\!\rangle$. Также аналогично определяются операции над типами $\varphi[\Theta^{(1)}]$ и $\varphi[\Theta^{(2)}]$.*

Для любых непустых конечных множеств G_1 и G_2, любой формулы $\Theta(t_1, \ldots, t_k)$ и любых типов $F_1, \ldots, F_k$ найдутся функция α, отображающая множество $\varphi[\Theta^{(1)}](F_1, \ldots, F_k)$ в $\varphi[\Theta^{(2)}](F_1, \ldots, F_k)$, и функция β, отображающая множество $\varphi[\Theta^{(2)}](F_1, \ldots, F_k)$ в $\varphi[\Theta^{(1)}](F_1, \ldots, F_k)$, со свойством: если $X_1 \subseteq F_1, \ldots, X_k \subseteq F_k$, то

$$\begin{aligned}
&\forall x \, \big(x \in \chi[\Theta^{(1)}(\langle\!\langle F_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k \rangle\!\rangle)] \Rightarrow \\
&\qquad\qquad \Rightarrow \alpha(x) \in \chi[\Theta^{(2)}(\langle\!\langle F_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k \rangle\!\rangle)] \big), \\
&\forall x \, \big(x \in \chi[\Theta^{(2)}(\langle\!\langle F_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k \rangle\!\rangle)] \Rightarrow \\
&\qquad\qquad \Rightarrow \beta(x) \in \chi[\Theta^{(1)}(\langle\!\langle F_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k \rangle\!\rangle)] \big).
\end{aligned}$$

Доказательство. Зафиксируем некоторые множества G_1 и G_2 и типы $F_1, \ldots, F_k$. Функции α и β будем строить индукцией по Θ, обозначая их α_Θ и β_Θ соответственно.

1) $\Theta = t_i$.

Положим $\alpha_\Theta(x) = x$, $\beta_\Theta(x) = x$.

2) $\Theta = \bot$.
Так как множества G_1 и G_2 непусты, существуют элементы $y \in G_1$ и $z \in G_2$. Положим $\alpha_\Theta(x) = z$ и $\beta_\Theta(x) = y$.

3) $\Theta = \Theta_1 \vee \Theta_2$.
Если $x = \langle\!\langle 0, y \rangle\!\rangle$ для некоторого y, то положим $\alpha_\Theta(x) = \langle\!\langle 0, \alpha_{\Theta_1}(y) \rangle\!\rangle$, $\beta_\Theta(x) = \langle\!\langle 0, \beta_{\Theta_1}(y) \rangle\!\rangle$. Если $x = \langle\!\langle 1, y \rangle\!\rangle$ для некоторого y, то положим $\alpha_\Theta(x) = \langle\!\langle 1, \alpha_{\Theta_2}(y) \rangle\!\rangle$, $\beta_\Theta(x) = \langle\!\langle 1, \beta_{\Theta_2}(y) \rangle\!\rangle$.

4) $\Theta = \Theta_1 \wedge \Theta_2$.
Любой x из областей определения α_Θ и β_Θ имеет вид $\langle\!\langle y, z \rangle\!\rangle$ для некоторых y и z. Положим $\alpha_\Theta(x) = \langle\!\langle \alpha_{\Theta_1}(y), \alpha_{\Theta_2}(z) \rangle\!\rangle$, $\beta_\Theta(x) = \langle\!\langle \beta_{\Theta_1}(y), \beta_{\Theta_2}(z) \rangle\!\rangle$.

5) $\Theta = \Theta_1 \to \Theta_2$.
Возьмём в качестве $\alpha_\Theta(x)$ функцию из $\varphi[\Theta^{(2)}](F_1, \ldots, F_k)$, которая произвольный элемент $y \in \varphi[\Theta_1^{(2)}](F_1, \ldots, F_k)$ отображает в элемент $\alpha_{\Theta_2}\Big(x\big(\beta_{\Theta_1}(y)\big)\Big)$. Аналогично, возьмём в качестве $\beta_\Theta(x)$ функцию из $\varphi[\Theta^{(1)}](F_1, \ldots, F_k)$, которая произвольный элемент $y \in \varphi[\Theta_1^{(1)}](F_1, \ldots, F_k)$ отображает в элемент $\beta_{\Theta_2}\Big(x\big(\alpha_{\Theta_1}(y)\big)\Big)$.

Индукцией по построению формулы Θ докажем, что для функций α_Θ и β_Θ выполнено указанное свойство. Чтобы не загромождать текст, ограничимся только частью, касающейся функции α_Θ, опустив аналогичное рассмотрение функции β_Θ. Для краткости не будем писать аргументы $\langle\!\langle F_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k \rangle\!\rangle$ у $\Theta^{(1)}$ и $\Theta^{(2)}$.

1) $\Theta = t_i$.
В этом случае $\Theta^{(1)} = \Theta^{(2)}$, и $\alpha_\Theta(x) = x$ очевидно обладает нужным свойством.

2) $\Theta = \bot$. В этом случае $\Theta^{(1)} = \langle\!\langle G_1, \varnothing \rangle\!\rangle$, $\Theta^{(2)} = \langle\!\langle G_2, \varnothing \rangle\!\rangle$. Поэтому $x \notin \chi[\Theta^{(1)}]$ и $\alpha(x) \notin \chi[\Theta^{(2)}]$ при любом x.

3) $\Theta = \Theta_1 \vee \Theta_2$.
Пусть $x \in \chi[\Theta^{(1)}]$. Если $x = \langle\!\langle 0, y \rangle\!\rangle$ для некоторого y, то $y \in \chi[\Theta_1^{(1)}]$, по индуктивному предположению $\alpha_{\Theta_1}(y) \in \chi[\Theta_1^{(2)}]$, поэтому $\alpha(x) \in \chi[\Theta^{(2)}]$. Случай, когда $x = \langle\!\langle 1, z \rangle\!\rangle$, аналогичен.

4) $\Theta = \Theta_1 \wedge \Theta_2$. Аналогично предыдущему.

5) $\Theta = \Theta_1 \to \Theta_2$.
Пусть $x \in \chi[\Theta^{(1)}]$. Тогда образ функции x на множестве $\chi[\Theta_1^{(1)}]$ вложен в множество $\chi[\Theta_2^{(1)}]$. Докажем, что функция $\alpha_\Theta(x)$ принадлежит $\chi[\Theta^{(2)}]$. Пусть $y \in \chi[\Theta_1^{(2)}]$. Тогда по предположению индукции $\beta_{\Theta_1}(y) \in \chi[\Theta_1^{(1)}]$, поэтому $x\big(\beta_{\Theta_1}(y)\big) \in \chi[\Theta_2^{(1)}]$, и снова по предположению индукции $\big(\alpha_\Theta(x)\big)(y) = \alpha_{\Theta_2}\Big(x\big(\beta_{\Theta_1}(y)\big)\Big) \in \chi[\Theta_2^{(2)}]$.

□

Предложение 3.3. *Пусть G_1, H_1, G_2, H_2 — непустые конечные множества, $G_1 \cap H_1 = \varnothing$ и $G_2 \cap H_2 = \varnothing$. Для произвольной формулы $\Theta(t_1, \ldots, t_k)$ и финитных задач $A_1, \ldots, A_k$ обозначим через $\Theta^{(1)}(A_1, \ldots, A_k)$ финитную задачу, полученную в результате подстановки вместо переменных задач $A_1, \ldots, A_k$, где дизъюнкция $\vee$ определяется как*

$$\langle\!\langle F_1, X_1 \rangle\!\rangle \vee^{(1)} \langle\!\langle F_2, X_2 \rangle\!\rangle = \\ = \langle\!\langle (G_1 \times F_1) \cup (H_1 \times F_2), (G_1 \times X_1) \cup (H_1 \times X_2) \rangle\!\rangle .$$

Аналогично через $\Theta^{(2)}(A_1, \ldots, A_k)$ обозначим задачу, где дизъюнк-

ция $\vee$ *определяется как*

$$\langle\!\langle F_1, X_1 \rangle\!\rangle \vee^{(2)} \langle\!\langle F_2, X_2 \rangle\!\rangle = \\ = \langle\!\langle (G_2 \times F_1) \cup (H_2 \times F_2), (G_2 \times X_1) \cup (H_2 \times X_2) \rangle\!\rangle .$$

Также аналогично определяются операции над типами $\varphi[\Theta^{(1)}]$ *и* $\varphi[\Theta^{(2)}]$.

Для любых таких множеств G_1, H_1, G_2 *и* H_2, *любой формулы* $\Theta(t_1, \ldots, t_k)$ *и любых типов* $F_1, \ldots, F_k$ *найдутся функция* α, *отображающая множество* $\varphi[\Theta^{(1)}](F_1, \ldots, F_k)$ *в* $\varphi[\Theta^{(2)}](F_1, \ldots, F_k)$, *и функция* β, *отображающая множество* $\varphi[\Theta^{(2)}](F_1, \ldots, F_k)$ *в* $\varphi[\Theta^{(1)}](F_1, \ldots, F_k)$, *со свойством: если* $X_1 \subseteq F_1, \ldots, X_k \subseteq F_k$, *то*

$$\forall x \, \big(x \in \chi[\Theta^{(1)}(\langle\!\langle F_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k \rangle\!\rangle)] \Rightarrow \\ \Rightarrow \alpha(x) \in \chi[\Theta^{(2)}(\langle\!\langle F_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k \rangle\!\rangle)] \big) , \\ \forall x \, \big(x \in \chi[\Theta^{(2)}(\langle\!\langle F_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k \rangle\!\rangle)] \Rightarrow \\ \Rightarrow \beta(x) \in \chi[\Theta^{(1)}(\langle\!\langle F_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k \rangle\!\rangle)] \big) .$$

Доказательство предложения 3.3 совершенно аналогично доказательству предложения 3.2. Эти два предложения, конечно, можно соединить в одно.

3.1.3. Финитные задачи и логика

Как и алгоритмические задачи, финитные задачи можно использовать для интерпретации классической логики.

Сопоставим финитным задачам с пустым множеством решений булево значение **Л** („ложь“), а финитным задачам с непустым множеством решений — булево значение **И** („истина“). Легко проверяется, что операции над финитными задачами $\vee$, $\wedge$, $\rightarrow$, $\neg$ при таком сопоставлении переходят в соответствующие булевские операции над значениями **Л** и **И**.

Отсюда получается аналог предложения 2.1.

Предложение 3.4. *Формула* $\Theta(t_1, \ldots, t_k)$ *является классической тавтологией тогда и только тогда, когда для любых финитных задач* $A_1, \ldots, A_k$ *множество возможных решений составной задачи* $\chi[\Theta(A_1, \ldots, A_k)]$ *непусто.*

Медведев в работах [7]–[9] ввёл и исследовал понятие финитной общезначимости, которое естественно считать аналогом реализуемости для финитных задач.

Формула $\Theta(t_1, \ldots, t_k)$ называется *финитно общезначимой*, если для произвольных типов $F_1, \ldots, F_k$ существует такой элемент $x \in \varphi[\Theta](F_1, \ldots, F_k)$, что для любых $X_1, \ldots, X_k$

$$X_1 \subseteq F_1, \ldots, X_k \subseteq F_k \quad \Rightarrow \quad x \in \chi[\Theta(\langle\!\langle F_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k \rangle\!\rangle)]\,.$$

Медведевым были установлены следующие свойства финитно общезначимых формул.

Предложение 3.5. *Если формула* Θ *выводима в интуиционистском исчислении высказываний, то она финитно общезначима.*

Теорема 3.1. *Если формула* Θ *позитивна, то есть не содержит отрицания и константы* $\bot$*, и финитно общезначима, то она выводима в интуиционистском исчислении высказываний.*

Именно для доказательства последней теоремы Медведевым было введено понятие критической импликации.

Логика всех (а не только позитивных) финитно общезначимых формул с синтаксической точки зрения устроена сложно. Она отличается как от интуиционистской логики (как и в случае реализуемости, можно рассмотреть формулу Роуза), так и от логики реализуемости (это отметил Плиско в [10]). В [6] доказано, что логика финитно общезначимых формул не допускает конечной аксиоматизации.

3.2. Достаточное множество решений

3.2.1. Определение и простейшие свойства

Введём новое понятие, характеризующее финитную задачу.

Для формулы $\Theta(t_1, \ldots, t_k)$ и для произвольных типов $F_1, \ldots, F_k$ множество $X \subseteq \varphi[\Theta](F_1, \ldots, F_k)$ назовём *достаточным множеством решений*, если для любых $X_1, \ldots, X_k$

$$X_1 \subseteq F_1, \ldots, X_k \subseteq F_k \quad \Rightarrow \quad X \cap \chi[\Theta(\langle\!\langle F_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k \rangle\!\rangle)] \neq \varnothing\,.$$

Если для некоторой формулы $\Theta(t_1, \ldots, t_k)$ всегда (то есть для любых типов $F_1, \ldots, F_k$) существует достаточное множество решений, то, в частности, для любых задач $A_1, \ldots, A_k$ множество $\chi[\Theta(A_1, \ldots, A_k)]$ непусто. И наоборот, если для любых задач $A_1, \ldots, A_k$ множество $\chi[\Theta(A_1, \ldots, A_k)]$ непусто, то для данных типов $F_1, \ldots, F_k$ объединение множеств $\chi[\Theta(A_1, \ldots, A_k)]$ по всем задачам данных типов будет достаточным множеством решений. Поэтому из предложением 3.4 получаем, что для формулы $\Theta(t_1, \ldots, t_k)$ всегда существует достаточное множество решений тогда и только тогда, когда Θ является классической тавтологией.

Если для некоторых типов $F_1, \ldots, F_k$ достаточное множество решений существует, можно поставить вопрос о его минимальной возможной мощности. Предложение 3.1 показывает, что ответ на этот вопрос зависит только от мощностей типов $F_1, \ldots, F_k$. Предложения 3.2 и 3.3 показывают, что на минимальную мощность достаточного множества решений не влияет произвол, присутствующий в определении операции $\vee$ и константы $\bot$.

Логарифм мощности достаточного множества решений является комбинаторной мерой количества информации. Нижеследующие результаты сформулированы в терминах мощностей, но перейдя

к логарифмам, легко увидеть, что они чрезвычайно близки соответствующим результатам для алгоритмических задач.

Из определения очевидно, что финитно общезначимы в точности те формулы, у которых есть одноэлементное достаточное множество решений для любых типов $F_1, \ldots, F_k$.

Следущие два свойства являются аналогами предложений 2.4 и 2.3 соответственно.

Предложение 3.6. *Пусть все рассматриваемые формулы содержат только переменные $t_1, \ldots, t_k$. Пусть для некоторых типов $F_1, \ldots, F_k$ для формулы $\Psi \to \Theta$ есть достаточное множество решений мощности M_1, а для формулы Ψ — мощности M_2. Тогда для типов $F_1, \ldots, F_k$ формула Θ имеет достаточное множество решений мощности не больше $M_1 \cdot M_2$.*

Доказательство. В качестве достаточного множества решений можно взять множество всех значений функций из достаточного множества решений для $\Psi \to \Theta$ на всех элементах достаточного множества решений для Ψ. □

Предложение 3.7. *Пусть формула Θ содержит только переменные $t_1, \ldots, t_k$. Для любых типов $F_1, \ldots, F_k$ существует такое множество X мощности не более $(|F_1| + 1) \cdot \ldots \cdot (|F_k| + 1)$, что для любых таких множеств $X_1, \ldots, X_k$, что $X_1 \subseteq F_1$, …, $X_k \subseteq F_k$, выполнено*

$$\chi[\Theta(\langle\!\langle F_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k \rangle\!\rangle)] \neq \varnothing \quad \Rightarrow \\ \Rightarrow \quad X \cap \chi[\Theta(\langle\!\langle F_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k \rangle\!\rangle)] \neq \varnothing .$$

Доказательство. Назовём элемент x *псевдорешением* финитной задачи A, если либо $x \in \chi[A]$, либо $\chi[A] = \varnothing$ и $x \notin \varphi[A]$ (иными словами, если x — псевдорешение задачи A, то из $x \in \varphi[A]$ следует $x \in \chi[A]$, а из $x \notin \varphi[A]$ следует $\chi[A] = \varnothing$).

Для формулы Θ, содержащей только переменные $t_1, \ldots, t_k$, и типов $F_1, \ldots, F_k$ построим функцию f_Θ со следующим свойством: если $x_1, \ldots, x_k$ — псевдорешения финитных задач $\langle\!\langle F_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k \rangle\!\rangle$ соответственно, то $f_\Theta(x_1, \ldots, x_k)$ — псевдорешение финитной задачи $\Theta(\langle\!\langle F_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k \rangle\!\rangle)$. (Область определения функции f_Θ можно выбирать достатчно произвольно. Для дальнейшего необходимо, чтобы среди допустимых значений i-го аргумента были все элементы множества F_i и какой-нибудь элемент не из F_i.)

Функцию f_Θ определим индукцией по построению формулы.

1) $\Theta = t_i$.
   Положим $f_\Theta(x_1, \ldots, x_k) = x_i$.

2) $\Theta = \bot$.
   Положим $f_\Theta(x_1, \ldots, x_k) = 1$ (напомним, что константе $\bot$ сопоставлена финитная задача $\langle\!\langle \{0\}, \varnothing \rangle\!\rangle$).

3) $\Theta = \Theta_1 \vee \Theta_2$.
   Если $f_{\Theta_1}(x_1, \ldots, x_k) \in \varphi[\Theta_1](F_1, \ldots, F_k)$, то $f_\Theta(x_1, \ldots, x_k) = \langle\!\langle 0, f_{\Theta_1}(x_1, \ldots, x_k) \rangle\!\rangle$, а в противном случае $f_\Theta(x_1, \ldots, x_k) = \langle\!\langle 1, f_{\Theta_2}(x_1, \ldots, x_k) \rangle\!\rangle$.

4) $\Theta = \Theta_1 \wedge \Theta_2$.
   Положим $f_\Theta(x_1, \ldots, x_k) = \langle\!\langle f_{\Theta_1}(x_1, \ldots, x_k), f_{\Theta_2}(x_1, \ldots, x_k) \rangle\!\rangle$.

5) $\Theta = \Theta_1 \to \Theta_2$.
   Если $f_{\Theta_1}(x_1, \ldots, x_k) \notin \varphi[\Theta_1](F_1, \ldots, F_k)$, то возьмём в качестве $f_\Theta(x_1, \ldots, x_k)$ любую функцию из $\varphi[\Theta](F_1, \ldots, F_k)$, а в противном случае — функцию, тождественно равную $f_{\Theta_2}(x_1, \ldots, x_k)$.

Пусть $x_1, \ldots, x_k$ — псевдорешения финитных задач $A_1, \ldots, A_k$ (типов $F_1, \ldots, F_k$). Докажем по индукции, что $f_\Theta(x_1, \ldots, x_k)$ — псевдорешение финитной задачи $\Theta(A_1, \ldots, A_k)$.

1) $\Theta = t_i$. Тривиально.

2) $\Theta = \bot$. Тривиально.

3) $\Theta = \Theta_1 \vee \Theta_2$.
По предположению индукции $f_{\Theta_1}(x_1, \ldots, x_k)$ и $f_{\Theta_2}(x_1, \ldots, x_k)$ есть псевдорешения задач $\Theta_1(A_1, \ldots, A_k)$ и $\Theta_2(A_1, \ldots, A_k)$ соответственно. Если множество $\chi[\Theta_1(A_1, \ldots, A_k)]$ непусто, то $f_{\Theta_1}(x_1, \ldots, x_k) \in \chi[\Theta_1(A_1, \ldots, A_k)]$ и поэтому

$$f_\Theta(x_1, \ldots, x_k) = \langle\!\langle 0, f_{\Theta_1}(x_1, \ldots, x_k) \rangle\!\rangle \in \chi[\Theta(A_1, \ldots, A_k)]\,.$$

Аналогично рассматривается случай $\chi[\Theta_2(A_1, \ldots, A_k)]$. Наконец, если $\chi[\Theta_1(A_1, \ldots, A_k)]$ и $\chi[\Theta_2(A_1, \ldots, A_k)]$ пусты, то $\chi[\Theta(A_1, \ldots, A_k)]$ тоже пусто, и в то же время

$$f_\Theta(x_1, \ldots, x_k) = \langle\!\langle 1, f_{\Theta_2}(x_1, \ldots, x_k) \rangle\!\rangle \notin \varphi[\Theta(A_1, \ldots, A_k)]\,.$$

4) $\Theta = \Theta_1 \wedge \Theta_2$. Этот пункт рассматривается аналогично.

5) $\Theta = \Theta_1 \to \Theta_2$.
Если множество $\chi[\Theta_1(F_1, \ldots, F_k)]$ пусто, то $\chi[\Theta(F_1, \ldots, F_k)] = \varphi[\Theta(F_1, \ldots, F_k)]$. Пусть $\chi[\Theta_1(F_1, \ldots, F_k)]$ непусто. Если множество $\chi[\Theta_2(F_1, \ldots, F_k]$ непусто, то элемент $f_{\Theta_2}(x_1, \ldots, x_k)$ ему принадлежит, и тождественно равная этому элементу функция лежит в $\chi[\Theta(F_1, \ldots, F_k)]$. В противном случае эта функция не лежит $\varphi[\Theta(F_1, \ldots, F_k)]$, а множество $\chi[\Theta(F_1, \ldots, F_k)]$ пусто.

Теперь заметим, что если F — конечное множество, $x \notin F$, то множество $F \cup \{x\}$ содержит хотя бы одно псевдорешение любой финитной задачи $\langle\!\langle F, X \rangle\!\rangle$. Выберем $x_i \notin F_i$ для каждого из множеств $F_1, \ldots, F_k$ и положим

$$X = \{f_\Theta(y_1, \ldots, y_k) \mid \forall i\ (y_i \in F_i \text{ или } y_i = x_i)\}\,.$$

Очевидно, что $|X|$ не превосходит $(|F_1|+1)\cdot\ldots\cdot(|F_k|+1)$, и для любых $X_i \subseteq F_i$ множество X содержит псевдорешение задачи $\Theta(\langle\!\langle F_1, X_1\rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k\rangle\!\rangle)$ (поскольку хотя бы в одном из наборов аргументов функции f_Θ каждый y_i является псевдорешением соответствующей задачи $\langle\!\langle F_i, X_i\rangle\!\rangle$). □

Следующая лемма является аналогом леммы 2.5.

Лемма 3.8. *Пусть формула Θ, содержащая только переменные $t_1, \ldots, t_k$ выводима в $\mathfrak{J}$. Тогда для любых типов $F_1, \ldots, F_k$ найдётся достаточное множество решений мощности не больше 2^k.*

Доказательство. Пусть $A = \langle\!\langle F, X\rangle\!\rangle$ — произвольная финитная задача. Если $X = \varnothing$, то $\neg A = \langle\!\langle \{0\}^F, \{0\}^F\rangle\!\rangle$, а если $X \neq \varnothing$, то $\neg\neg A = \langle\!\langle \{0\}^{\{0\}^F}, \{0\}^{\{0\}^F}\rangle\!\rangle$. Таким образом, для формулы $(\neg t \vee \neg\neg t)$ и любого типа F множество $\chi[\neg\langle\!\langle F, \varnothing\rangle\!\rangle \vee \neg\neg\langle\!\langle F, F\rangle\!\rangle]$, содержащее два элемента, является достаточным множеством решений. Для формулы $\bigwedge_{i=1}^k(\neg t_i \vee \neg\neg t_i)$ и типов $F_1, \ldots, F_k$ достаточным множеством решений будет

$$\chi\Big[\bigwedge_{i=1}^{k}(\neg\langle\!\langle F_i, \varnothing\rangle\!\rangle \vee \neg\neg\langle\!\langle F_i, F_i\rangle\!\rangle)\Big].$$

Очевидно, мощность этого множества равна 2^k.

Поскольку формула $\Theta(t_1, \ldots, t_k)$ выводима в логике $\mathfrak{J}$, из леммы 1.2 следует, что формула

$$\Theta'(t_1, \ldots, t_k) = \bigwedge_{i=1}^{k}(\neg t_i \vee \neg\neg t_i) \to \Theta(t_1, \ldots, t_k)$$

выводима в $\mathfrak{Int}$. Поэтому из предложений 3.5 и 3.6 получаем утверждение леммы. □

3.2.2. Нижняя оценка для критических импликаций

Следующая теорема является аналогом теоремы 2.1.

Теорема 3.2. *Пусть $J(s_1,\ldots,s_m)$ — критическая импликация с m переменными, а $G_1,\ldots,G_m$ — произвольные конечные множества, содержащие по крайней мере два элемента. Пусть множество $X\subseteq\varphi[J](G_1,\ldots,G_m)$ таково, что при всех $X_1,\ldots,X_m$*

$$\forall i(X_i\subseteq G_i\&|X_i|=2)\quad\Rightarrow\quad X\cap\chi[J(\langle\!\langle G_1,X_1\rangle\!\rangle,\ldots,\langle\!\langle G_m,X_m\rangle\!\rangle)]\neq\varnothing\,.$$

Тогда

$$|X|\geqslant\min_i|G_i|/(2m)\,.$$

Доказательство. Чтобы избежать громоздких обозначений, всюду в этом доказательстве будем считать, что $\varphi[\Psi]$ есть тип, который получается в результате подстановки в некоторую формулу Ψ типов $G_1,\ldots,G_m$ вместо переменных $s_1,\ldots,s_m$, а $\Psi(X_1,\ldots,X_m)$ — сокращение для $\chi[\Psi(\langle\!\langle G_1,X_1\rangle\!\rangle,\ldots,\langle\!\langle G_m,X_m\rangle\!\rangle)]$.

Пусть G — множество таких наборов $\langle\!\langle x_1,\ldots,x_{2m}\rangle\!\rangle\in G_1\times G_1\times\times G_2\times G_2\times\ldots\times G_m\times G_m$, что $x_{2i-1}\neq x_{2i}$ для любых $i\in\{1,\ldots,m\}$.

Каждому набору $\vec{x}\in G$ поставим в соответствие двухэлементные множества $X_i(\vec{x})=\{x_{2i-1},x_{2i}\}\subseteq G_i$.

Скажем, что элемент p, принадлежащий типу $\varphi[J]$, является решением для набора $\vec{x}\in G$, если $p\in J(X_1,\ldots,X_m)$ для $X_i=X_i(\vec{x})$.

Мы покажем, что любое p является решением только для небольшой доли всех наборов из G. С этой целью для каждого p рассмотрим двудольный граф, вершинами которого являются элементы множества G. Элементы, для которых p является решением, принадлежат первой доле, все остальные — второй. Условие, при котором две вершины соединены ребром, будет сформулировано ниже. При этом будет обеспечено следующее свойство графа: из

каждой вершины первой доли исходит не меньше $(\min_i |G_i| - 2)$ рёбер, а из каждой вершины второй доли исходит не больше $2m$ рёбер.

Пусть в первой доле M_1 вершин, а во второй доле M_2 вершин. Оценим число рёбер графа: с одной стороны, из первой доли исходит не меньше $(\min_i |G_i| - 2)M_1$ рёбер, а с другой стороны, из второй доли исходит не больше $2mM_2$ рёбер. Из соотношений $M_1 + M_2 = |G|$ и $(\min_i |G_i| - 2)M_1 \leqslant 2mM_2$ получаем, что $M_1 \leqslant |G| \cdot 2m/(\min_i |G_i| + 2m - 2)$, то есть не более чем для такого количества наборов из G элемент p является решением. Множество X с указанным в условии свойством должно для каждого набора из G содержать решение p, поэтому $|X| \cdot |G| \cdot 2m/(\min_i |G_i| + 2m - 2) \geqslant |G|$, то есть $|X| \geqslant \min_i |G_i|/(2m) + 1 - 1/m$, что и требовалось.

Осталось объяснить, как следует провести рёбра в графе, соответствующем p.

Критическая импликация J имеет вид $\bigwedge_i \Psi_i(s_1, \ldots, s_m) \to \bigvee s_j$. Элемент p типа $\varphi[J]$ является функцией, определенной на кортеже элементов типа $\varphi[\Psi_i]$. Формулы Ψ_i имеют вид $(P \to Q) \to Q$, где P — непустая конъюнкция, а Q — непустая дизъюнкция некоторых из $s_1, \ldots, s_m$, причём общих переменных у них нет.

Пусть Ψ — формула описанного вида. Для каждого набора $\vec{x} \in G$ определим функцию $f_{\vec{x}} \in \varphi[\Psi]$. Пусть $P^1(\vec{x})$ — единственный элемент множества $P(\{x_1\}, \{x_3\}, \ldots, \{x_{2m-1}\})$, $P^2(\vec{x})$ — единственный элемент множества $P(\{x_2\}, \{x_4\}, \ldots, \{x_{2m}\})$, и наконец, $Q(\vec{x}) = Q(X_1(\vec{x}), \ldots, X_m(\vec{x}))$. Значение функции $f_{\vec{x}}$ на элементе $r \in \varphi[(P \to Q)]$ определяется так:

$$f_{\vec{x}}(r) = \begin{cases} r(P^1(\vec{x})), & \text{если } r(P^1(\vec{x})) \in Q(\vec{x}), \\ r(P^2(\vec{x})), & \text{в противном случае.} \end{cases}$$

Очевидно, что $f_{\vec{x}} \in \Psi(X_1(\vec{x}), \ldots, X_m(\vec{x}))$. Однако $f_{\vec{x}}$ принадле-

жит также множеству $\Psi(X_1(\vec{x}'), \ldots, X_m(\vec{x}'))$ для таких $\vec{x}' \in G$, которые отличаются от $\vec{x}$ только в одной координате, то есть $x_i = x'_i$ для всех i, кроме одного.

Действительно, пусть $r \in (P \to Q)(X_1(\vec{x}'), \ldots, X_m(\vec{x}'))$. Тогда по определению $r(P^1(\vec{x}')) \in Q(\vec{x}')$ и $r(P^2(\vec{x}')) \in Q(\vec{x}')$. Поскольку формулы P и Q не имеют общих переменных, замена $\vec{x}'$ на $\vec{x}$ может повлиять либо на значение P^1, либо на значение P^2, либо на значение Q, но не на какие два из них сразу, то есть возможны три случая.

1) $P^1(\vec{x}) \neq P^1(\vec{x}')$, $P^2(\vec{x}) = P^2(\vec{x}')$, $Q(\vec{x}) = Q(\vec{x}')$.

   Тогда значение $f_{\vec{x}}(r)$ либо равно $r(P^2(\vec{x})) = r(P^2(\vec{x}'))$, либо принадлежит $Q(\vec{x}) = Q(\vec{x}')$.

2) $P^2(\vec{x}) \neq P^2(\vec{x}')$, $P^1(\vec{x}) = P^1(\vec{x}')$, $Q(\vec{x}) = Q(\vec{x}')$.

   Тогда $r(P^1(\vec{x})) = r(P^1(\vec{x}')) \in Q(\vec{x}') = Q(\vec{x})$, поэтому значение $f_{\vec{x}}(r)$ равно $r(P^1(\vec{x}))$.

3) $Q(\vec{x}) \neq Q(\vec{x}')$, $P^1(\vec{x}) = P^1(\vec{x}')$, $P^2(\vec{x}) = P^2(\vec{x}')$.

   Тогда значение $f_{\vec{x}}(r)$ равно либо $r(P^1(\vec{x})) = r(P^1(\vec{x}'))$, либо $r(P^2(\vec{x})) = r(P^2(\vec{x}'))$.

Таким образом, во всех случаях $f_{\vec{x}}(r) \in Q(\vec{x}')$.

Пусть p является решением для некоторого набора $\vec{x}$. Рассмотрим значение p на кортеже тех $f_{\vec{x}}$, которые соответствуют формулам Ψ_i из посылки критической импликации. Это значение принадлежит множеству $\bigvee_j X_j(\vec{x})$ (где дизъюнкция берётся по всем j из заключения критической импликации) и имеет вид $\langle\!\langle b_1, \ldots \langle\!\langle b_{m'}, x_c \rangle\!\rangle \ldots \rangle\!\rangle$, где $b_1, \ldots, b_{m'} \in \{0, 1\}$ и однозначно определяются по c. В графе, соответствующем p, вершину $\vec{x}$ соединим рёбрами со всеми такими $\vec{x}'$, что $x_i = x'_i$ при $i \neq c$ и $x_c \neq x'_c$.

Покажем, что $\vec{x}$ и $\vec{x}'$ лежат в разных долях графа. Действительно, возьмём $j = \lceil c/2 \rceil$ — номер того множества из дизъюнкции, которому должен принадлежать элемент x_c. Одно из чисел $2j-1$ и $2j$ равно c, второе обозначим через d, и рассмотрим множество $X_j(\vec{x}') = \{x'_c, x'_d\}$. Элемент x_c не принадлежит этому множеству, поскольку $x'_c \neq x_c$ и $x'_d = x_d \neq x_c$ (напомним, что рассматриваются только такие $\vec{x}$, у которых $x_{2i-1} \neq x_{2i}$). Поэтому в силу отмеченного свойства функций $f_{\vec{x}}$ элемент p, являясь решением для $\vec{x}$, не может быть решением для $\vec{x}'$.

Количество элементов $\vec{x}'$ рассматриваемого вида равно $|G_j|-2$, поэтому из каждой вершины первой доли исходит по крайней мере $(\min_i |G_i| - 2)$ рёбер.

Предположим, что из какой-то вершины $\vec{x}'$ второй доли исходит больше $2m$ рёбер. Тогда некоторые две вершины из первой доли отличаются от $\vec{x}'$ в одной и той же координате, то есть найдутся два таких набора $\vec{x}^1$ и $\vec{x}^2$, что p на кортежах функций вида $f_{\vec{x}^1}$ и $f_{\vec{x}^2}$ выдаёт соответственно $\langle\!\langle b_1, \ldots \langle\!\langle b_{m'}, x^1_l \rangle\!\rangle \ldots \rangle\!\rangle$ и $\langle\!\langle b_1, \ldots \langle\!\langle b_{m'}, x^2_l \rangle\!\rangle \ldots \rangle\!\rangle$. Но для $i \neq l$ имеем $x^1_i = x'_i = x^2_i$, поэтому $\vec{x}^1$ и $\vec{x}^2$ должны находиться в разных долях; противоречие. □

3.2.3. Классификация формул по мощности достаточного множества решений

Наконец, можно доказать аналог теоремы 2.2.

Теорема 3.3. *Пусть формула $\Theta(t_1, \ldots, t_k)$ невыводима в $\mathfrak{J}$. Тогда найдётся такое m, что для любого N существуют такие типы $F_1, \ldots, F_k$, что их мощности не превышают $(4mN)^m$ и для любого множества $X \subseteq \varphi[\Theta](F_1, \ldots, F_k)$ выполнено следующее: если при любых $X_1, \ldots, X_k$*

$$\forall i (X_i \subseteq F_i \& |X_i| \leqslant 4^m) \quad \Rightarrow \quad X \cap \chi[\Theta(\langle\!\langle F_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle F_k, X_k \rangle\!\rangle)] \neq \varnothing\,,$$

то

$$|X| \geqslant N\,.$$

Доказательство. Для невыводимой в $\mathfrak{J}$ формулы Θ возьмём число m и формулы $\mathrm{T}_1, \ldots, \mathrm{T}_k$, построенные в теореме 1.3.

Для данного N возьмём любые множества $G_1, \ldots, G_m$ мощности $2mN$ каждое, и определим множества $F_1, \ldots, F_k$ посредством равенств $F_i = \varphi[\mathrm{T}_i](G_1, \ldots, G_m)$.

Если $\mathrm{T}_i = \bot$, то $|F_i| = 1$. В противном случае T_i является дизъюнкцией некоторых конъюнкций переменных $s_1, \ldots, s_m$. Конъюнкция не более чем m множеств мощности $2mN$ каждое имеет мощность не более $(2mN)^m$, различных таких конъюнкций тоже существует не более 2^m, поэтому $|F_i| \leqslant 2^m \cdot (2mN)^m = (4mN)^m$.

Рассмотрим все финитные задачи $A_1, \ldots, A_k$ вида

$$A_i = \mathrm{T}_i(\langle\!\langle G_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle G_m, X_m \rangle\!\rangle)\,,$$

где $|X_i| = 2$.

Если $\mathrm{T}_i = \bot$, то $|\chi[A_i]| = 0$. В противном случае, аналогично оценке для $|F_i|$, получаем, что $|\chi[A_i]| \leqslant 2^m \cdot 2^m = 4^m$.

Пусть некоторое множество X содержит решения всех задач $\Theta(A_1, \ldots, A_k)$ для $A_1, \ldots, A_k$ из рассматриваемого класса.

По теореме 1.3 импликация

$$\Theta(\mathrm{T}_1(s_1, \ldots, s_m), \ldots, \mathrm{T}_k(s_1, \ldots, s_m)) \to J_m(s_1, \ldots, s_m)\,.$$

выводима в $\mathfrak{Int}$, и в силу предложения 3.5 для неё существует элемент f, являющийся решением соответствующей финитной задачи при любой подстановке финитных задач вида $\langle\!\langle G_i, X_i \rangle\!\rangle$.

Применив f ко всем элементам множества X, получим множество X', которое содержит решения всех задач вида

$$J_m(\langle\!\langle G_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle G_m, X_m \rangle\!\rangle)$$

для $|X_i| = 2$, и $|X| \geqslant |X'|$.

В силу теоремы 3.2 $|X'| \geqslant N$, и поэтому $|X| \geqslant N$. □

Предложение 3.4, лемма 3.8 и теорема 3.3 позволяют сделать следующие выводы о достаточном множестве решений в зависимости от выводимости формулы.

Следствие 3.1.

Если формула Θ *не выводится в классической логике, то достаточного множества решений не существует.*

Если формула Θ *выводится в* $\mathfrak{J}$*, то для любых типов* $F_1, \ldots, F_k$ *есть достаточное множество решений мощности не более* 2^k*.*

Если формула Θ *не выводится в* $\mathfrak{J}$*, но выводится в классической логике, то существует такая константа* m*, зависящая только от* Θ*, что для любого числа* M *существуют типы* $F_1, \ldots, F_k$*, для которых* $|F_1| \leqslant M, \ldots, |F_k| \leqslant M$ *и мощность любого достаточного множества решений больше или равна* $M^{1/m}/(4m)$*.*

Переформулируем последнее утверждение в терминах (комбинаторного) количества информации и сравним со следствием 2.1. Смысл первых двух пунктов ясен: для классически невыводимой формулы у соответствующей задачи может вообще не быть решений, а для решения задачи, соответствующей выводимой в $\mathfrak{J}$ формуле, всегда достаточно ограниченного количества дополнительной информации. Разберём подробнее последний пункт, говорящий о классически истинных, но невыводимых в $\mathfrak{J}$ формулах. Подставляемые в формулу задачи таковы, что для решения получающейся составной задачи, в силу предложения 3.7, достаточно информации в количестве

$$n = \log_2\bigl((|F_1| + 1) \cdot \ldots \cdot (|F_k| + 1)\bigr) = k \log_2(M + 1)\,.$$

Однако при некоторой подстановке может быть недостаточно информации в количестве

$$\log_2(M^{1/m}/(4m)) \geqslant \frac{1}{km}\, n - \log_2(8m)\,.$$

Таким образом, количество информации, минимально достаточное для решения составной задачи, растёт линейно с ростом количества информации в подставляемых задачах.

В отличие от алгоритмического подхода, в данном случае сохраняется разница (в константу раз) между верхней и нижней оценкой скорости роста количества информации. В разделе 3.3 изложен достаточно естественный способ измерения сложности финитной задачи, для которого удаётся получить верхнюю и нижнюю оценки, отличающиеся только *аддитивной* константой.

3.2.4. Об оптимальности оценки для критических импликаций

Теорема 3.2 даёт нижнюю оценку на мощность достаточного множества решений. Покажем, что эта оценка не может быть существенно усилена.

Лемма 3.9. *Для любой классически выводимой критической импликации $J(s_1, \ldots, s_m)$ и любых типов $G_1, \ldots, G_m$ существует достаточное множество решений, мощность которого не превосходит $|G_1| + \ldots + |G_m|$.*

Замечание. Классически невыводимые критические импликации действительно существуют, например, $((s_1 \to s_2) \to s_2) \to s_3$. Однако легко убедиться, что критические импликации J_m классически выводимы для $m \geqslant 2$. Классически выводимы и те критические импликации, о которых идёт речь в теореме 2.3.

Доказательство. Пусть $R(s_1, \ldots, s_m)$ — дизъюнкция переменных, стоящая в заключении критической импликации. Для каждого элемента из $\varphi[R](G_1, \ldots, G_m)$ построим функцию из $\varphi[J](G_1, \ldots, G_m)$, тождественно равную этому элементу. Множество таких функций и будет достаточным множеством решений.

Действительно, рассмотрим произвольные задачи $A_1, \ldots, A_m$ типов $G_1, \ldots, G_m$. Если $\chi[R(A_1, \ldots, A_m)]$ непусто, то оно содержит некоторый элемент x, и функция, тождественно равная x, принадлежит $\chi[J(A_1, \ldots, A_m)]$. Если $\chi[R(A_1, \ldots, A_m)]$ пусто, то в силу классической выводимости критической импликации J, задача, соответствующая её посылке, тоже должна иметь пустое множество решений, поэтому любая функция из $\varphi[J](G_1, \ldots, G_m)$ принадлежит $\chi[J(A_1, \ldots, A_m)]$.

Очевидно, что мощность построенного множества равна

$$|\varphi[R](G_1, \ldots, G_m)| \leqslant |G_1| + \ldots + |G_m| .$$

□

Таким образом, если $|G_1| = \ldots = |G_m| = M$, то мы имеем две оценки на мощность достаточного множества решений для критической импликации: нижнюю $M/(2m)$ и верхнюю $m \cdot M$. После логарифмирования получим две оценки на количество информации, различающиеся на константу, как и в случае алгоритмических задач.

Разберём теперь ещё один вопрос, связанный с теоремой 3.2. Её доказательство существенно отличается от доказательства аналогичной теоремы 2.1, и это неслучайно.

В теореме 2.1 рассматривались подстановки в формулу одноэлементных множеств. В случае финитных задач это соответствует следующему условию на множество $X \subseteq \varphi[J](G_1, \ldots, G_m)$: для

всех $X_1, \ldots, X_m$

$$\forall i(X_i \subseteq G_i \& |X_i| = 1) \quad \Rightarrow \quad X \cap \chi[J(\langle\!\langle G_1, X_1 \rangle\!\rangle, \ldots, \langle\!\langle G_m, X_m \rangle\!\rangle)] \neq \varnothing .$$

Однако в этом случае для некоторых критических импликаций X может быть одноэлементным. Это показывает следующая лемма (рассуждение опирается на идею из примера 3 статьи [19], использованную также в лемме 2.10).

Лемма 3.10. *Пусть G_1 и G_2 — любые типы. Для критической импликации $J = ((s_1 \to s_2) \to s_2) \to (s_1 \vee s_2)$ существует такой элемент $f \in \varphi[J](G_1, G_2)$, что $f \in \chi[J(A_1, A_2)]$ для любых финитных задач $A_1 = \langle\!\langle G_1, \{x_1\} \rangle\!\rangle$ и $A_2 = \langle\!\langle G_2, \{x_2\} \rangle\!\rangle$, где $x_1 \in G_1$ и $x_2 \in G_2$.*

Доказательство. Элемент f является функцией, отображающей множество $G_2^{G_2^{G_1}}$ в $G_1 \sqcup G_2$. Опишем, как элементу g сопоставить некоторый элемент z так, чтобы если для каких-то x_1 и x_2 выполнено $g \in \chi[(\langle\!\langle G_1, \{x_1\} \rangle\!\rangle \to \langle\!\langle G_2, \{x_2\} \rangle\!\rangle) \to \langle\!\langle G_2, \{x_2\} \rangle\!\rangle]$, то $z = \langle\!\langle 0, x_1 \rangle\!\rangle$ или $z = \langle\!\langle 1, x_2 \rangle\!\rangle$.

Назовём пару $\langle\!\langle y_1, y_2 \rangle\!\rangle \in G_1 \times G_2$ *совместимой* с g, если для любой функции $h\colon G_1 \to G_2$, из $h(y_1) = y_2$ следует $g(h) = y_2$. Отметим, что при $g \in \chi[(\langle\!\langle G_1, \{x_1\} \rangle\!\rangle \to \langle\!\langle G_2, \{x_2\} \rangle\!\rangle) \to \langle\!\langle G_2, \{x_2\} \rangle\!\rangle]$ пара $\langle\!\langle x_1, x_2 \rangle\!\rangle$ совместима с g.

Заметим, что если $\langle\!\langle y_1', y_2' \rangle\!\rangle$ и $\langle\!\langle y_1'', y_2'' \rangle\!\rangle$ — различные совместимые с g пары, то либо $y_1' = y_1''$, либо $y_2' = y_2''$. Действительно, пусть $y_1' \neq y_1''$, тогда существует функция h, для которой $h(y_1') = y_2'$ и $h(y_1'') = y_2''$. В силу совместимости с g имеем $g(h) = y_2'$ и $g(h) = y_2''$, то есть $y_2' = y_2''$.

Рассмотрим теперь множество пар из $G_1 \times G_2$, совместимых с g. В этом множестве либо все пары имеют одинаковый первый

элемент, либо все пары имеют одинаковый второй элемент. (В противном случае найдутся пары $\langle\!\langle y'_1, y'_2 \rangle\!\rangle$ и $\langle\!\langle y''_1, y''_2 \rangle\!\rangle$, у которых $y'_1 \neq y''_1$ и $y'_2 \neq y''_2$. Действительно, возьмём две пары, различающиеся первым элементом. Если второй элемент у этих пар одинаков, возьмём третью пару с отличным вторым элементом. Первым элементом третья пара отличается хотя бы от одной из двух пар.) Поскольку пара $\langle\!\langle x_1, x_2 \rangle\!\rangle$ совместима с g, этот общий элемент есть x_1 или x_2 соответственно. □

Таким образом, теорему 3.2 нельзя доказать так же, как теорему 2.1. Отметим, однако, что тем же методом, что и в теореме 3.2, можно доказать аналогичное ей утверждение для алгоритмических задач, которого достаточно для доказательства теоремы 2.2.

3.3. Колмогоровская сложность финитных задач

3.3.1. Определение и простейшие свойства

Колмогоровская сложность является алгоритмической характеристикой, и может применяться только к ограниченному классу объектов, а именно, к так называемым конструктивным объектам, то есть объектам, с которыми могут работать алгоритмы. Поэтому в этом разделе типы рассматриваемых финитных задач уже не будут произвольными конечными множествами.

В первом приближении можно сказать, что теперь все типы будут состоять из двоичных слов. Однако логические операции над типами приводят к появлению элементов нового сорта — пар и конечных функций. Конечно, их тоже можно закодировать двоичными словами, но это потребует изменить определение операций

над финитными задачами. Вместо этого расширим то универсальное множество, подмножествами которого являются все типы.

Обозначим через $\mathfrak{U}$ наименьшее множество, которое содержит все двоичные слова, и для которого выполнены следующие два свойства. Если x и y принадлежат $\mathfrak{U}$, то пара $\langle\!\langle x, y \rangle\!\rangle$ тоже принадлежит $\mathfrak{U}$. Если X и Y — конечные подмножества $\mathfrak{U}$, то множество функций X^Y тоже является подмножеством $\mathfrak{U}$.

Нетрудно проверить, что множество $\mathfrak{U}$ существует и счётно. Элементы множества $\mathfrak{U}$ можно закодировать двоичными словами так, что по кодам двух элементов вычислимо находится код их пары и наоборот, а также по набору кодов аргументов и значений функции вычислимо находится код самой функции и наоборот. Будем считать, что конечное множество F элементов $\mathfrak{U}$ кодируется двоичным словом, соответствующим кортежу кодов всех элементов множества F в лексикографическом порядке.

Далее в этом разделе будем считать, что все типы финитных задач являются непустыми конечными подмножествами множества $\mathfrak{U}$. Предложение 3.1 показывает, что такое ограничение несущественно. В тех случаях, когда будут рассматриваться алгоритмические преобразования типов или их элементов (в частности, в определении колмогоровской сложности финитной задачи), будем считать, что речь идёт о вычислимых преобразованиях соответствующих кодов.

Очевидно, что по формуле $\Theta(t_1, \ldots, t_k)$ и типам $F_1, \ldots, F_k$ можно эффективно найти тип $\varphi[\Theta](F_1, \ldots, F_k)$. С другой стороны, по формуле $\Theta(t_1, \ldots, t_k)$ без фиктивных переменных и типу $\varphi[\Theta](F_1, \ldots, F_k)$ можно эффективно восстановить типы $F_1, \ldots, F_k$.

Колмогоровской сложностью финитной задачи $\langle\!\langle F, X \rangle\!\rangle$ назовём величину

$$Kf(\langle\!\langle F, X \rangle\!\rangle) = \min_{x \in X} K(x|F),$$

где F в условии понимается как код множества F (а не как произвольный его элемент, например). Если $X = \varnothing$, то $Kf(\langle\!\langle F, X \rangle\!\rangle) = \infty$. Неформально говоря, сложностью задачи объявлена минимальная сложность её решений (как и в случае алгоритмических задач).

Перенесём на случай сложности финитных задач результаты, доказанные в главе 2 для сложности алгоритмических задач.

Предложение 3.11. *Для любой формулы $\Theta(t_1, \ldots, t_k)$ и любых финитных задач $A_1, \ldots, A_k$ если $\chi[\Theta(A_1, \ldots, A_k)] \neq \varnothing$, то*

$$Kf(\Theta(A_1, \ldots, A_k)) \leqslant Kf\Big(\bigwedge_{\chi[A_i]\neq\varnothing} A_i\Big) + O(1)\,,$$

где член $O(1)$ зависит только от формулы Θ и выбора оптимального способа описания.

Доказательство. Зная тип $\varphi[\Theta(A_1, \ldots, A_k)]$, можно алгоритмически найти типы $\varphi[A_1], \ldots, \varphi[A_k]$ и построить функцию f_Θ из доказательства предложения 3.7.

Теперь для построения элемента из множества $\chi[\Theta(A_1, \ldots, A_k)]$ достаточно знать, какие из множеств $\chi[A_i]$ непусты, и знать по элементу из каждого непустого множества. □

Лемма 3.12. *Если формула $\Theta(t_1, \ldots, t_k)$ выводима в $\mathfrak{J}$, то найдётся такая константа C, что для любых финитных задач $A_1, \ldots, A_k$*

$$Kf(\Theta(A_1, \ldots, A_k)) \leqslant C\,.$$

Доказательство. По лемме 3.8, если формула $\Theta(t_1, \ldots, t_k)$ выводима в $\mathfrak{J}$, то для любых типов $F_1, \ldots, F_k$ у неё есть достаточное множество решений мощности 2^k. Зная тип $\varphi[\Theta(A_1, \ldots, A_k)]$, можно алгоритмически восстановить типы $\varphi[A_1], \ldots, \varphi[A_k]$ и перебором найти указанное достаточное множество решений. Любой элемент

этого множества задаётся своим номером в нём. Для построения элемента из $\chi[\Theta(A_1,\ldots,A_k)]$ при известном типе $\varphi[\Theta(A_1,\ldots,A_k)]$ достаточно знать только этот номер. □

3.3.2. Классификация формул по сложности порождаемых финитных задач

Наконец, следующая теорема дословно переносит утверждение теоремы 2.2 на случай финитных задач.

Теорема 3.4. *Пусть формула $\Theta(t_1,\ldots,t_k)$ невыводима в логике $\mathfrak{J}$. Если при этом классически истинна формула $\Theta(\bot,\ldots,\bot)$ (вместо всех переменных подставлена константа $\bot$) или формула $\Theta(t_1,\ldots,t_k)$ позитивна, то существует такая константа C, что для любого числа n найдутся финитные задачи $A_1,\ldots,A_k$ со свойствами:*

1) *среди множеств $\chi[A_1],\ldots,\chi[A_k]$ есть непустые;*

2) $Kf\Big(\bigwedge\limits_{\chi[A_i]\neq\varnothing} A_i\Big) \leqslant n + C;$

3) $Kf(\Theta(A_1,\ldots,A_k)) \geqslant n - C.$

Если формула $\Theta(t_1,\ldots,t_k)$ позитивна, то можно выбрать финитные задачи $A_1,\ldots,A_k$ так, что все множества $\chi[A_1],\ldots,\chi[A_k]$ непусты.

Доказательство. Для невыводимой в $\mathfrak{J}$ формулы Θ возьмём число m и формулы $\mathrm{T}_1,\ldots,\mathrm{T}_k$, построенные в теореме 1.3. В силу замечания после теоремы, не все T_i равны константе $\bot$ (а для позитивной Θ — все не равны).

Для данного n возьмём произвольные множества $G_1,\ldots,G_m$ мощности 2^n. Пусть $G = \varphi[J_m](G_1,\ldots,G_m)$. Рассмотрим множество $X = \{p \in G \mid K(p|G) < n - \log_2(2m)\}$. Мощность множества

X не превышает $2^{n-\log_2(2m)} - 1 = 2^n/(2m) - 1$, поэтому в силу теоремы 3.2 оно не является достаточным множеством решений для J_m и типов $G_1, \ldots, G_m$. Таким образом, найдутся финитные задачи $B_1, \ldots, B_m$, для которых $Kf(J_m(B_1, \ldots, B_m)) \geqslant n - \log_2(2m)$ (и $|\chi[B_i]| = 2$ для $i \in \{1, \ldots, m\}$).

Поскольку любой элемент множества G_i можно задать его номером, $Kf(B_i) \leqslant \log_2 |G_i| + C' = n + C'$, где константа C' зависит только от выбора оптимального способа описания.

Определим задачи $A_1, \ldots, A_k$ равенствами $A_i = \mathrm{T}_i(B_1, \ldots, B_m)$.

Если $\mathrm{T}_i \neq \bot$, то $\{0\} \times \chi[B_m] \subseteq \chi[A_i]$ (и поэтому $\chi[A_i] \neq \varnothing$). Следовательно,

$$Kf\Big(\bigwedge_{\chi[A_i]\neq\varnothing} A_i\Big) \leqslant Kf(B_m) + C'' \leqslant n + C\,,$$

где константы C'' и C зависят только от формулы Θ и выбора оптимального способа описания.

Поскольку формула $\Theta(\mathrm{T}_1, \ldots, \mathrm{T}_k) \to J_m$ интуиционистски выводима, по предложению 3.5 она финитно общезначима. Зная типы финитных задач, подставленных вместо переменных $s_1, \ldots, s_m$ (а для этого достаточно знать тип задачи, получившейся после подстановки), общее решение можно найти перебором. Поэтому

$$Kf(J_m(B_1, \ldots, B_m)) \leqslant \\ \leqslant Kf(\Theta(\mathrm{T}_1(B_1, \ldots, B_m), \ldots, \mathrm{T}_k(B_1, \ldots, B_m))) + C_\Theta\,,$$

где константа C_Θ зависит только от формулы Θ и выбора оптимального способа описания. Таким образом, $Kf(\Theta(A_1, \ldots, A_k)) \geqslant$ $\geqslant Kf(J_m(B_1, \ldots, B_m)) - C_\Theta \geqslant n - \log_2(2m) - C_\Theta \geqslant n - C$. □

Таким образом, для финитных задач имеет место та же классификация формул по сложности порождаемых ими задач, что и для алгоритмических.

А именно, с каждой формулой $\Theta(t_1, \ldots, t_k)$ свяжем функцию натурального аргумента kf_Θ:

$$\mathrm{kf}_\Theta(n) = \\ = \max\Big\{ Kf(\Theta(A_1, \ldots, A_k)) \Big| (\exists i\, \chi[A_i] \neq \varnothing) \Rightarrow Kf\Big(\bigwedge_{\chi[A_i]\neq\varnothing} A_i \Big) \leqslant n \Big\}.$$

Предложения 3.4 и 3.11, лемма 3.12 и теорема 3.4 дают следующее описание сложности финитных задач в зависимости от формулы Θ.

Следствие 3.2.

Если Θ *не выводится в классической логике, то* $\mathrm{kf}_\Theta(n) = \infty$ *при достаточно больших* n.

Если Θ *выводится в* $\mathfrak{J}$, *то* $\mathrm{kf}_\Theta(n) = O(1)$.

Если Θ *не выводится в* $\mathfrak{J}$, *но выводится в классической логике, то* $\mathrm{kf}_\Theta(n) = n + O(1)$.

Литература

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

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

[3] А. К. Звонкин, Л. А. Левин. Сложность конечных объектов и обоснование теории информации и случайности с помощью теории алгоритмов. *Успехи математических наук*, 1970, т. 25, № 6, с. 85–127.

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

[5] А. Н. Колмогоров. Три подхода к определению понятия „количество информации“. *Проблемы передачи информации*, 1965, т. 1, № 1, с. 3–11.

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

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

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

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

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

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

[12] В. Е. Плиско. О языках с конструктивными логическими связками *Доклады АН СССР*, 1987, т. 296, вып. 1, с. 35–38.

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

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

[15] S. C. Kleene. On the interpretation of intuitionistic number theory. *Journal of Symbolic Logic*, 1945, v. 10, pp. 109–124.

[16] A. Kolmogoroff. Zur Deutung der intuitionistishen Logik. *Mathematische Zeitschrift*, 1932, Bd. 35, H. 1, S. 58–65.

[17] M. Li, P. Vitányi. *An Introduction to Kolmogorov Complexity and Its Applications.* New York, Springer-Verlag, 1997.

[18] G. F. Rose. Propositional calculus and realizability. *Transactions of the American Mathematical Society*, 1953, v. 75, № 1, pp. 1–19.

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

Работы автора по теме диссертации

[20] Н. К. Верещагин, Д. П. Скворцов, Е. З. Скворцова, А. В. Чернов. Варианты понятия реализуемости для пропозициональных формул, приводящие к логике слабого закона исключённого третьего. *Математическая логика и алгебра*, Труды Математического института им. В. А. Стеклова, 2003, т. 242, с. 77–97.

[21] А. В. Чернов. Финитные задачи и логика слабого закона исключённого третьего. Рукопись депонирована в ВИНИТИ 03.07.2003, № 1263-В2003, 15 с.

[22] A. V. Chernov, D. P. Skvortsov, E. Z. Skvortsova, N. K. Vereshchagin. Variants of Realizability for Propositional Formulas and the Logic of the Weak Law of Excluded Middle. *Proceedings of Computer Science Logic'02*, Lecture Notes in Computer Science, 2002, v. 2471, pp. 74–88.