МИНИСТЕРСТВО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
им. М. В. ЛОМОНОСОВА

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

УДК 517.12 + 510.52

А. В. Чернов

ФИНИТНЫЕ ЗАДАЧИ И ЛОГИКА СЛАБОГО ЗАКОНА ИСКЛЮЧЁННОГО ТРЕТЬЕГО

МОСКВА 2003

МИНИСТЕРСТВО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
им. М. В. ЛОМОНОСОВА

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

РАЗРЕШАЮ
НА ДЕПОНИРОВАНИЕ
Зам. декана по научной работе,
профессор ________________ (*В. Н. Чубариков*)

УДК 517.12 + 510.52

А. В. Чернов

ФИНИТНЫЕ ЗАДАЧИ И ЛОГИКА СЛАБОГО ЗАКОНА ИСКЛЮЧЁННОГО ТРЕТЬЕГО

Автор: ________________________ (*А. В. Чернов*)

МОСКВА 2003

Идея Колмогорова об интерпретации логических связок как операций над задачами неоднократно использовалась разными исследователями для построения семантики суперинтуиционистских логик. В статьях [1] и [5] изучался подход, близкий к реализуемости по Клини: под задачами понимались множества конструктивных объектов (натуральных чисел и двоичных слов), а в определении операций участвовали вычислимые функции. Было получено описание логики слабого закона исключённого третьего как множества формул, для которых составная задача всегда имеет „простое“ решение.

Настоящая работа посвящена альтернативному подходу, основанному на испоьзовании финитных задач. Это понятие было впервые рассмотрено Медведевым в статьях [3] и [4]. Вместо множеств конструктивных объектов рассматриваются подмножества некоторых произвольных, но фиксированных (для каждой пропозициональной переменной) конечных множеств. При этом для интерпретации импликации вместо вычислимых частичных функций (заданных программами) используются всюду определённые функции на конечных множествах (заданные таблично). Для этого случая удаётся доказать аналогичный результат: формулы, для которых решение соответствующей задачи всегда можно найти в некоторой заранее выбранной небольшой совокупности, образуют логику слабого закона исключённого третьего.

Перейдём к точным определениям.

Финитной задачей называется пара множеств $\langle F, X\rangle$, где F конечно и непусто, а $X \subseteq F$. 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 $\chi[A]$.

Для произвольных множеств X и Y их дизъюнктное объединение $(\{0\} \times X) \cup (\{1\} \times Y)$ обозначается через $X \sqcup Y$, а множество функций из X в Y — через Y^X.

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

Работа выполнена при финансовой поддержке грантов РФФИ и Совета поддержки ведущих научных школ при президенте РФ.

логическим связкам.

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

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

Очевидно, что тип финитной задачи $\Theta(A_1, \dots, A_k)$ зависит только от типов финитных задач $A_1, \dots, A_k$, поэтому удобно ввести также соответствующую формуле Θ операцию над типами $\varphi[\Theta]$:

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

Легко проверить, что для произвольной формулы $\Theta(t_1, \dots, t_k)$ и произвольных финитных задач $A_1, \dots, A_k$ множество $\chi[\Theta(A_1, \dots, A_k)]$ непусто тогда и только тогда, когда формула Θ истинна на таком наборе истинностных значений $b_1, \dots, b_k$, что b_i истинно, в точности если $\chi[A_i]$ непусто. Таким образом, множество формул, для которых составная задача всегда имеет решение, образует классическую логику высказываний (ср. предложение 1 в [5]).

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

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

Следующие свойства финитно общезначимых формул были установлены Медведевым в [3] и [4].

Предложение 1. *Если формула Θ выводима в интуиционистском исчислении высказываний, то она финитно общезначима.*

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

Теперь 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 $X_1, \ldots, X_k$

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

Очевидно, что достаточное множество решений существует тогда и только тогда, когда формула является классической тавтологией.

Индукцией по построению формулы легко доказывается следующее утверждение.

Предложение 2. *Пусть $F_1, \ldots, F_k$ — некоторые непустые конечные множества, и функции $\alpha_1, \ldots, \alpha_k$ биективно отображают соответствующие F_i на F'_i. По любой формуле $\Theta(t_1, \ldots, t_k)$ можно построить биективное отображение α множества $\varphi[\Theta](F_1, \ldots, F_k)$ на множество $\varphi[\Theta](F'_1, \ldots, F'_k)$ со следующим свойством. Если $X_1, \ldots, X_k$ — произвольные подмножества $F_1, \ldots, F_k$, а $X'_1, \ldots, X'_k$ являются образами множеств $X_1, \ldots, X_k$ при отображениях $\alpha_1, \ldots, \alpha_k$ соответственно, то множество $\chi[\Theta(\langle F'_1, X'_1\rangle, \ldots, \langle F'_k, X'_k\rangle)]$ является образом множества $\chi[\Theta(\langle F_1, X_1\rangle, \ldots, \langle F_k, X_k\rangle)]$ при отображении α.*

Отсюда, в частности, следует, что для любой формулы $\Theta(t_1, \ldots, t_k)$ ответ на вопрос о том, существует ли достаточное множество решений некоторой мощности, определяется только мощностями типов $F_1, \ldots, F_k$. Поэтому корректна следующая постановка проблемы: для каждой формулы выяснить, как минимальная мощность достаточного множества решений зависит от мощностей типов подставляемых задач.

Полезно ещё отметить, что для рассматриваемой задачи несущественен произвол, который есть в определениях финитной задачи, соответствующей константе $\perp$, и дизъюнкции финитных задач. Нетрудно проверить, что в определении $\perp$ вместо $\{0\}$ можно использовать любое непустое конечное множество, а в определении дизъюнкции вместо множеств $\{0\}$ и $\{1\}$ — любые непересекающиеся непустые конечные множества. Например, для $\perp$ достаточно доказать индукцией по построению формулы следующее утверждение (для дизъюнкции утверждение аналогично, но более громоздко).

Предложение 3. *Для любых непустых конечных множеств G_1 и G_2 и любой формулы $\Theta(t_1, \ldots, t_k)$ существует функция α со следующим свойством: для произвольных финитных задач $A_1, \ldots, A_k$*

$$\forall x \left(x \in \chi[\Theta^{(1)}(A_1, \ldots, A_k)] \Leftrightarrow \alpha(x) \in \chi[\Theta^{(2)}(A_1, \ldots, A_k)] \right),$$

где через $\Theta^{(1)}(A_1, \ldots, A_k)$ и $\Theta^{(2)}(A_1, \ldots, A_k)$ обозначены финитные задачи, полученные при подстановке задач $\langle G_1, \varnothing \rangle$ и, соответственно, $\langle G_2, \varnothing \rangle$ вместо $\perp$, а $A_1, \ldots, A_k$ — вместо переменных.

Очевидно, финитно общезначимы в точности те формулы, у которых есть одноэлементное достаточное множество решений для любых типов $F_1, \ldots, F_k$. Для дальнейшего полезно отметить ещё следующий очевидный факт.

Предложение 4. *Пусть формула $\Psi \to \Theta$ от переменных $t_1, \ldots, t_k$ финитно общезначима. Пусть для некоторых типов $F_1, \ldots, F_k$ формула Ψ имеет достаточное множество решений мощности M. Тогда для типов $F_1, \ldots, F_k$ формула Θ имеет достаточное множество решений мощности не больше M.*

Легко убедиться также в истинности следующего утверждения.

Предложение 5. *Для любой классически выводимой формулы Θ от переменных $t_1, \ldots, t_k$ и любых типов $F_1, \ldots, F_k$ существует достаточное множество решений мощности не более $(|F_1| + 1) \cdot \ldots \cdot (|F_k| + 1)$.*

Рассмотрим теперь класс формул, для которых всегда есть „небольшое“ (хотя не обязательно одноэлементное) достаточное множество решений. Теорема 1 даёт описание этого класса формул при многих возможных уточнениях слова „небольшое“.

Через $\mathfrak{J}$ обозначается *логика слабого закона исключённого третьего*, то есть суперинтуиционистская логика, которая получается добавлением аксиомы $\neg t \vee \neg\neg t$ к интуиционистскому исчислению высказываний.

Теорема 1. *Пусть формула $\Theta(t_1, \ldots, t_k)$ выводима в $\mathfrak{J}$. Тогда для любых типов $F_1, \ldots, F_k$ существует достаточное множество решений мощности не больше 2^k.*

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* $X_1, \ldots, X_k$

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

то

$$|X| \geqslant N$$

(то есть в этом случае минимальная мощность достаточного множества решений может быть сколь угодно велика).

Доказательство. Как можно вывести из результатов статьи [6], формула $\Theta(t_1, \ldots, t_k)$ выводима в логике $\mathfrak{J}$ тогда и только тогда, когда интуиционистски выводима формула $\bigwedge_{i=1}^k(\neg t_i \vee \neg\neg t_i) \to \Theta(t_1, \ldots, t_k)$. Поэтому в силу предложений 1 и 4 первое утверждение теоремы достаточно проверить только для формулы $\bigwedge_{i=1}^k(\neg t_i \vee \neg\neg t_i)$.

Пусть $A = \langle F, X\rangle$ — произвольная финитная задача. Если $X = \varnothing$, то $\neg A = \langle \{0\}^F, \{0\}^F\rangle$, а если $X \neq \varnothing$, то $\neg\neg A = \langle \{0\}^{\{0\}^F}, \{0\}^{\{0\}^F}\rangle$. Таким образом, для формулы $\neg t \vee \neg\neg t$ и для любого типа F двухэлементное множество $\chi[\neg\langle F, \varnothing\rangle \vee \neg\neg\langle F, F\rangle]$ является достаточным множеством решений. Конъюнкция k таких множеств (очевидно, имеющая мощность 2^k) будет достаточным множеством решений для формулы $\bigwedge_{i=1}^k(\neg t_i \vee \neg\neg t_i)$.

Доказательство второго утверждения теоремы опирается на свойство невыводимых в $\mathfrak{J}$ формул, вытекающее из результатов Янкова и Медведева.

Критической импликацией называется формула вида

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

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.

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

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

Следующая лемма была доказана в [5].

Лемма 1. *Если формула $\Theta(t_1, \ldots, t_k)$ невыводима в $\mathfrak{J}$, то найдутся такое m и такие формулы $\tau_1(s_1, \ldots, s_m), \ldots, \tau_k(s_1, \ldots, s_m)$, что интуиционистски выводима импликация $\Theta(\tau_1, \ldots, \tau_k) \to J_m$. При этом можно считать, что если формула Θ позитивна, то все τ_i имеют вид $s_m \vee (\bigvee \bigwedge s_j)$, а если формула Θ непозитивна, то при каждом i формула τ_i либо имеет указанный вид, либо является константой $\bot$.*

Таким образом, осталось оценить мощность достаточного множества решений для критических импликаций.

Лемма 2. *Пусть $J(s_1, \ldots, s_m)$ — критическая импликация с m переменными, а $G_1, \ldots, G_m$ — произвольные непустые конечные множества. Пусть множество $X \subseteq \varphi[J](G_1, \ldots, G_m)$ таково, что при всех $X_1, \ldots, X_m$*

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

Тогда

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

Эта лемма будет доказана ниже, а пока выведем из неё утверждение теоремы.

Для формулы $\Theta(t_1, \ldots, t_k)$ возьмём построенные в лемме 1 формулы $\tau_1, \ldots, \tau_k$ от переменных $s_1, \ldots, s_m$. Для данного N возьмём любые множества $G_1, \ldots, G_m$ мощности $2mN$, и определим множества $F_1, \ldots, F_k$ при помощи равенств $F_i = \varphi[\tau_i](G_1, \ldots, G_m)$. Если $\tau_i = \bot$, то $|F_i| = 1$, а иначе $|F_i| \leqslant 2^m \cdot (2mN)^m$.

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

$$A_i = \tau_i(\langle G_1, X_1\rangle, \ldots, \langle G_m, X_m\rangle)\,,$$

где $|X_i| = 2$. Очевидно, что для них $|\chi[A_i]| \leqslant 4^m$. Пусть некоторое множество X содержит решения всех задач вида $\Theta(A_1, \ldots, A_k)$. Тогда, в частности, оно содержит и решения всех задач вида

$$\Theta(\tau_1(\langle G_1, X_1\rangle, \ldots, \langle G_m, X_m\rangle), \ldots, \tau_k(\langle G_1, X_1\rangle, \ldots, \langle G_m, X_m\rangle)\,.$$

Поэтому из лемм 1 и 2 и предложений 1 и 4 получаем $|X| \geqslant N$. $\square$

Доказательство леммы 2. 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 $\Psi(X_1, \ldots, X_m)$ является сокращением для $\chi[\Psi(\langle G_1, X_1\rangle, \ldots, \langle G_m, X_m\rangle)]$.

Пусть G — множество таких наборов $\langle x_1, \ldots, x_{2m}\rangle \in G_1 \times G_1 \times G_2 \times G_2 \times \ldots \times G_m \times G_m$, 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 $X_i(\vec{x}) = \{x_{2i-1}, x_{2i}\} \subset G_i$.

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 $\bigwedge \Psi_i(s_1, \ldots, s_m) \to \bigvee s_j$. 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 $Q(\vec{x}) = Q(X_1(\vec{x}), \ldots, X_m(\vec{x}))$. 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 $f_{\vec{x}}$ принадлежит 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 $\bigvee_j X_j(\vec{x})$ (дизъюнкция берётся по j из заключения критической импликации) и имеет вид $\langle b_1, \ldots \langle b_{m'}, x_c\rangle \ldots\rangle$, 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 не меньше $|G_j| - 2$, 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 значения $\vec{x}^1$ и $\vec{x}^2$, что p на кортежах функций вида $f_{\vec{x}^1}$ и $f_{\vec{x}^2}$ выдаёт соответственно $\langle b_1, \ldots \langle b_{m'}, x^1_l\rangle \ldots\rangle$ и $\langle b_1, \ldots \langle b_{m'}, x^2_l\rangle \ldots\rangle$. 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. $\square$

Отметим, что утверждение леммы 2 почти оптимально по следующим двум параметрам. Во-первых, очевидно, что у любой критической импликации есть достаточное множество решений мощности не более $|G_1| + \ldots + |G_m|$. Во-вторых, для получения нижней оценки на $|X|$, вообще говоря, недостаточно выполнения условия леммы для всех одноэлементных X_i. В качестве примера[2], рассмотрим критическую импли-

[2] Приводимое рассуждение опирается на идею из примера 3 статьи [7].

кацию $((t_1 \to t_2) \to t_2) \to t_1 \vee t_2$, произвольные непустые конечные множества G_1 и G_2, любые их элементы $x_1 \in G_1$ и $x_2 \in G_2$. Для задач $A_1 = \langle G_1, \{x_1\}\rangle$ и $A_2 = \langle G_2, \{x_2\}\rangle$ можно по любому элементу $g \in \chi[(A_1 \to A_2) \to A_2]$ найти либо x_1, либо x_2. Для этого рассмотрим такие пары $\langle y_1, y_2\rangle \in G_1 \times G_2$, что для любой функции $h\colon G_1 \to G_2$, такой что $h(y_1) = y_2$, выполнено $g(h) \in \{\langle 0, y_1\rangle, \langle 1, y_2\rangle\}$. Теперь для нахождения x_1 или x_2 достаточно воспользоваться тем, что либо для всех таких пар $y_1 = x_1$, либо для всех таких пар $y_2 = x_2$. Последнее утверждение легко доказывается от противного: пусть это неверно, тогда найдутся две такие пары, что $y_1 \neq y_1'$ и $y_2 \neq y_2'$; но тогда существует такая функция h, что $h(y_1) = y_2$ и $h(y_1') = y_2'$, и $g(h) \in \{\langle 0, y_1\rangle, \langle 1, y_2\rangle\} \cap \{\langle 0, y_1'\rangle, \langle 1, y_2'\rangle\} = \varnothing$, противоречие.

Полученные в теореме 1 оценки на мощность достаточного множества решений аналогичны полученным в статье [5] оценкам сложности составных алгоритмических задач. Эта аналогия лежит в русле общего параллелизма между комбинаторным и алгоритмическим подходами к понятию „количество информации“, отмеченного в статье Колмогорова [2].

При комбинаторном подходе под количеством информации, содержащейся в элементах некоторого множества, подразумевается двоичный логарифм его мощности. В этих терминах наличие „небольшого“ достаточного множества решений означает, что у задачи всегда есть „простое“ решение. А утверждение теоремы 1 можно переформулировать так. Если формула выводима в $\mathfrak{J}$, то количество информации, достаточное для решения соответствущей задачи, ограничено константой, зависящей только от формулы. Если формула невыводима в $\mathfrak{J}$, то для любого n количество информации, необходимое для решения соответствущей задачи, может быть больше n при подстановке вместо переменных задач из некоторого класса L. При этом информация, достаточная для решения задачи, соответствующей классически выводимой формуле, когда переменные пробегают L, не превышает $km \cdot n + km \log_2(4m) + k$ (что следует из предложения 5).

Таким образом, для невыводимых в $\mathfrak{J}$ формул не исключено, что количество информации, необходимое для решения соответствующей задачи, будет меньше известной оценки на достаточное количество информации в km (то есть в константу) раз. При алгоритмическом подходе (теорема 1 в статье [5]) этот разрыв отсутствует.

Разница в полученных результатах обусловлена способом измерения количества информации в подставляемых задачах, который не учитывает возможности их взаимосвязи. Устранить этот недостаток можно, применив к финитным задачам элементы алгоритмического подхода.

Будем рассматривать только те финитные задачи, тип которых состоит из конструктивных объектов (двоичных слов, натуральных чисел и т. п.). В силу конечности сам тип тоже будет конструктивным объектом. Очевидно, что операции над финитными задачами эффективны. Отметим ещё, что по формуле $\Theta(t_1, \ldots, t_k)$ без фиктивных переменных и типу $\varphi[\Theta](F_1, \ldots, F_k)$ можно восстановить типы $F_1, \ldots, F_k$.

Назовём величину

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

колмогоровской сложностью финитной задачи $\langle F, X\rangle$ (где $K(x|F)$ — условная колмогоровская сложность — означает длину кратчайшего описания конструктивного объекта x при известном конструктивном объекте F; точное определение можно найти в [2]). Фактически, как и в [5], сложностью задачи объявлена минимальная сложность её решений.

Нетрудно убедиться, что для любой формулы $\Theta(t_1, \ldots, t_k)$ и любых финитных задач $A_1, \ldots, A_k$ из $\chi[\Theta(A_1, \ldots, A_k)] \neq \varnothing$ следует оценка

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

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

Если формула $\Theta(t_1, \ldots, t_k)$ выводима в $\mathfrak{J}$, то для неё всегда есть достаточное множество решений мощности 2^k, при известных типах это множество может быть найдено перебором, а любой его элемент задаётся своим номером в нём, поэтому для любых задач $A_1, \ldots, A_k$ верна оценка $Kf(\Theta(A_1, \ldots, A_k)) \leqslant C_\Theta$, где константа C_Θ зависит только от формулы Θ и выбора оптимального способа описания.

Следующая теорема дословно переносит утверждение теоремы 1 статьи [5] на случай финитных задач.

Теорема 2. *Пусть формула $\Theta(t_1, \dots, t_k)$ невыводима в логике слабого закона исключённого третьего $\mathfrak{J}$. Если при этом формула Θ позитивна или формула $\Theta(\bot, \dots, \bot)$ выводима, то существует такая константа C, что для любого числа n найдутся финитные задачи $A_1, \dots, A_k$ со свойствами:*

1. *не все $A_1, \dots, A_k$ равны $\bot$;*
2. $Kf\Big(\bigwedge\limits_{\chi[A_i]\neq\varnothing} A_i\Big) \leqslant n + C$;
3. $Kf(\Theta(A_1, \dots, A_k)) \geqslant n - C$.

Доказательство. Для невыводимой в $\mathfrak{J}$ формулы $\Theta(t_1, \dots, t_k)$ возьмём построенные в лемме 1 формулы $\tau_1, \dots, \tau_k$ от переменных $s_1, \dots, s_m$ и критическую импликацию $J_m(s_1, \dots, s_m)$. Заметим сначала, что если формула $\Theta(\bot, \dots, \bot)$ выводима, то формула $\Theta(\bot, \dots, \bot) \to J_m$ интуиционистски невыводима в силу невыводимости критических импликаций (см. [1]). Поэтому хотя бы для одного i выполнено $\tau_i \neq \bot$.

Для данного n возьмём произвольные множества $G_1, \dots, G_m$ мощности 2^n. Пусть $G = \varphi[J_m](G_1, \dots, G_m)$. Рассмотрим множество $X = \{p \in G | K(p|G) < n - \log_2(2m)\}$. Мощность множества X не превышает $2^{n-\log_2(2m)} - 1 = 2^n/(2m) - 1$, поэтому в силу леммы 2 оно не является достаточным множеством решений для J_m и типов $G_1, \dots, G_m$. Таким образом, найдутся финитные задачи $B_1, \dots, B_m$, для которых $Kf(J_m(B_1, \dots, B_m)) \geqslant n - \log_2(2m)$ (и $|\chi[B_i]| = 2$ для $i \in \{1, \dots, m\}$). 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 $A_1, \dots, A_k$ равенствами $A_i = \tau_i(B_1, \dots, B_m)$.

Если $\tau_i \neq \bot$, то $\{0\} \times \chi[B_m] \subseteq A_i$. Следовательно, $Kf\Big(\bigwedge\limits_{\chi[A_i]\neq\varnothing} A_i\Big) \leqslant Kf(B_m) + C'' \leqslant n + C$, где константы C'' и C зависят только от формулы Θ и выбора оптимального способа описания.

Поскольку формула $\Theta(\tau_1, \dots, \tau_k) \to J_m$ интуиционистски выводима, она финитно общезначима, и при известных типах общее решение может быть найдено перебором. Поэтому $Kf(J_m(B_1, \dots, B_m)) \leqslant Kf(\Theta(\tau_1(B_1, \dots, B_m), \dots, \tau_k(B_1, \dots, B_m))) + C_\Theta$, где константа C_Θ зависит только от формулы Θ и выбора оптимального способа описания. Таким образом, $Kf(\Theta(A_1, \dots, A_k)) \geqslant Kf(J_m(B_1, \dots, B_m)) - C_\Theta \geqslant n - \log_2(2m) - C_\Theta \geqslant n - C$. $\square$

Список литературы

[1] 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, в печати.

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

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

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

[5] А. В. Чернов. Сложность множеств, полученных как значения пропозициональных формул. *Математические заметки*, принято к печати.

[6] В. А. Янков. Об исчислении слабого закона исключённого третьего. *Известия АН СССР, сер. матем.*, 1968, т. 32, № 5, сс. 1044–1051.

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