УДК 510.52

Финитные задачи и логика слабого закона исключённого третьего

А. В. Чернов[1]

Идея Колмогорова из [1] об интерпретации логических связок как операций над задачами неоднократно использовалась разными исследователями для построения семантики суперинтуиционистских логик. В [2] было начато изучение подхода, основанного на идеях теории информации. В этой статье, а также в [3] изучалась интерпретация, близкая 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 альтернативной интерпретации, основанной на использовании финитных задач. Это понятие было впервые рассмотрено Медведевым в статьях [4] и [5]. 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). Поэтому естественно назвать подход, связанный с финитными задачами, комбинаторным, в отличие от алгоритмического подхода, связанного с реализуемостью.

В настоящей статье излагаются утверждения о финитных задачах, аналогичные полученным в [3] для реализуемости: формулы, для которых решение соответствующей задачи всегда можно найти в некоторой заранее выбранной небольшой совокупности, образуют логику слабого закона исключённого третьего.

[1]Работа выполнена при частичной финансовой поддержке грантов РФФИ № 03-01-00475, 02-01-22001 НЦНИ(а), гранта НШ-358.2003.1 Совета поддержки ведущих научных школ при президенте РФ и гранта SNF 200020-100259/1 (Juergen Schmidhuber, IDSIA).

Перейдём к точным определениям.

Финитной задачей называется пара множеств $\langle F, X\rangle$, 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 $A_1 = \langle F_1, X_1\rangle$ и $A_2 = \langle F_2, X_2\rangle$ — произвольные финитные задачи. Определим операции над финитными задачами, соответствующие логическим связкам.

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

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

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

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

Прежде чем двигаться дальше, отметим, что для наших целей безразлична природа элементов, из которых состоят типы рассматриваемых финитных задач, а существенна лишь мощность этих типов. Приведём формулировку утверждения, несложно доказываемого по индукции, на котором базируется корректность последующих определений.

Предложение 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 соответствующих $F_1, \ldots, F_k$, и функции $\alpha_1, \ldots, \alpha_k$ отображают их на некоторые $X'_1, \ldots, X'_k$ — подмножества $F'_1, \ldots, F'_k$, то функция α отображает множество $\chi[\Theta(\langle F_1, X_1\rangle, \ldots, \langle F_k, X_k\rangle)]$ на множество $\chi[\Theta(\langle F'_1, X'_1\rangle, \ldots, \langle F'_k, X'_k\rangle)]$.

Следующее предложение, также легко доказываемое по индукции, показывает, что в определении операции отрицания (точнее, константы $\perp$) множество $\{0\}$ можно заменить любым другим непустым конечным множеством. (Для дизъюнкции соответствующее утверждение можно сформулировать по аналогии.)

Предложение 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 $\perp$ задачи $\langle G_1, \varnothing\rangle$, а вместо переменных — задач $A_1, \ldots, A_k$. Так же обозначим через $\Theta^{(2)}(A_1, \ldots, A_k)$ результат подстановки вместо константы $\perp$ задачи $\langle G_2, \varnothing\rangle$. 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, которая отображает $\varphi[\Theta^{(1)}](F_1, \ldots, F_k)$ в $\varphi[\Theta^{(2)}](F_1, \ldots, F_k)$, и функция β, которая отображает $\varphi[\Theta^{(2)}](F_1, \ldots, F_k)$ в $\varphi[\Theta^{(1)}](F_1, \ldots, F_k)$, со свойствами: если $X_1 \subseteq F_1, \ldots, X_k \subseteq F_k$, то

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

Перейдём теперь к применению финитных задач для описания семантики пропозициональных формул.

Легко проверить, что для произвольной формулы $\Theta(t_1, \ldots, t_k)$ и произвольных финитных задач $A_1, \ldots, A_k$ множество $\chi[\Theta(A_1, \ldots, A_k)]$ непусто тогда и только тогда, когда формула Θ истинна на наборе истинностных значений $b_1, \ldots, b_k$, в котором b_i истинно в точности тогда, когда $\chi[A_i]$ непусто. Таким образом, множество формул, для которых составная задача всегда имеет решение, образует классическую логику высказываний (ср. предложение 1 в [3]).

Медведев в работах [4] и [5] 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 любых типов $F_1,\ldots,F_k$ существует такой элемент $x \in \varphi[\Theta](F_1,\ldots,F_k)$, что для любых $X_1,\ldots,X_k$

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

Следующие свойства финитно общезначимых формул были установлены Медведевым.

Предложение 3. *Если формула Θ выводима в интуиционистском исчислении высказываний, то она финитно общезначима.*

Предложение 4. *Если формула Θ позитивна, то есть не содержит отрицания и константы $\bot$, и финитно общезначима, то она выводима в интуиционистском исчислении высказываний.*

Логика всех (а не только позитивных) финитно общезначимых формул с синтаксической точки зрения устроена сложно. Она отличается как от интуиционистской логики, так и от логики реализуемости (это отметил Плиско в [6]). В [7] доказано, что логика финитно общезначимых формул не допускает конечной аксиоматизации.

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.

Из предложения 1 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. (Предложение 2 показывает, что ответ не зависит от произвола в определении отрицания.)

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 5. *Пусть все рассматриваемые формулы не содержит других переменных, кроме $t_1,\ldots,t_k$. Пусть для типов $F_1,\ldots,F_k$ формула $\Psi \to \Theta$ имеет достаточное множество решений мощности M_1, а формула Ψ — мощности M_2. Тогда для типов $F_1,\ldots,F_k$ формула Θ имеет достаточное множество решений мощности не больше $M_1 \cdot M_2$.*

Индукцией по построению формулы легко доказать также следующее утверждение.

Предложение 6. *Пусть формула Θ не содержит других переменных, кроме $t_1,\ldots,t_k$. 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*

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

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 $\mathfrak{J}$ обозначим *логику слабого закона исключённого третьего.* Эта логика получает 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 $F_1,\ldots,F_k$ найдётся 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 $X_1,\ldots,X_k$

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

то

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

Доказательство. Как можно вывести из результатов статьи [8], 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 3 и 5 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 [3].

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 $\perp$.*

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 конечные множества, содержащие не менее двух элементов. Пусть множество $X\subseteq\varphi[J](G_1,\ldots,G_m)$ таково, что при всех $X_1,\ldots,X_m$*

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

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 $2mN$ каждое, и определим множества $F_1,\ldots,F_k$ при помощи равенств $F_i=\varphi[\tau_i](G_1,\ldots,G_m)$. Если $\tau_i=\perp$, то $|F_i|=1$. В противном случае τ_i есть дизъюнкция конъюнкций m переменных. Различных конъюнкций существует 2^m, в каждой не более m членов, поэтому $|F_i|\leqslant 2^m\cdot(2mN)^m=(4mN)^m$.

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 $|X_i|=2$. Аналогично оценке для $|F_i|$ получаем $|\chi[A_i]|\leqslant 2^m\cdot 2^m=4^m$. Пусть некоторое множество X содержит решения всех задач вида $\Theta(A_1,\ldots,A_k)$. Импликация

$$\Theta(\tau_1(s_1,\ldots,s_m),\ldots,\tau_k(s_1,\ldots,s_m))\to J_m(s_1,\ldots,s_m)\,.$$

интуиционистски выводима, поэтому, используя предложения 3 и 5, можно построить такое множество X', что $|X'|\leqslant|X|$ и X' содержит решения всех задач вида

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

при $|X_i|=2$. По лемме 2 получаем, что $|X|\geqslant N$. □

Доказательство леммы 2. Чтобы избежать излишней громоздкости в обозначениях, 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 $\chi[\Psi(\langle G_1,X_1\rangle,\ldots,\langle G_m,X_m\rangle)]$.

Будем считать, что $\min_i |G_i| \geqslant 3$ (если $\min_i |G_i| = 2$, заключение теоремы тривиально: $|X| \geqslant 1$).

Пусть множество G состоит из всех 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 $x_{2i-1} \neq x_{2i}$ при $i \in \{1, \ldots, m\}$.

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 равно $|G_j| - 2$, поэтому из каждой вершины первой доли исходит не меньше $(\min_i |G_i| - 2)$ 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 $\langle b_1, \ldots \langle b_{m'}, x_l^1 \rangle \ldots \rangle$ и $\langle b_1, \ldots \langle b_{m'}, x_l^2 \rangle \ldots \rangle$. Но для $i \neq l$ имеем $x_i^1 = x'_i = x_i^2$, 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 классически выводимой критической импликации для любых типов $G_1, \ldots, G_m$ есть достаточное множество решений мощности $|G_1| + \ldots + |G_m|$.

Во-вторых, для получения нижней оценки на $|X|$, вообще говоря, недостаточно выполнения условия на X для всех одноэлементных X_i. А именно, для некоторой критической импликации J существует такое $X \subseteq \varphi[J](G_1, \ldots, G_m)$, что для всех $X_1, \ldots, X_m$

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

Рассмотрим в качестве примера[2] критическую импликацию от двух переменных $((t_1 \to t_2) \to t_2) \to t_1 \vee t_2$.

Возьмём произвольные непустые конечные множества G_1 и G_2, а также любые их элементы $x_1 \in G_1$ и $x_2 \in G_2$. Покажем, как для задач $A_1 = \langle G_1, \{x_1\} \rangle$ и $A_2 = \langle G_2, \{x_2\} \rangle$ по любому элементу $g \in \chi[(A_1 \to A_2) \to A_2]$ найти либо x_1, либо x_2.

Назовём пару $\langle y_1, y_2 \rangle \in G_1 \times G_2$ *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 пара $\langle x_1, x_2 \rangle$ совместима с g. Если $\langle y'_1, y'_2 \rangle$ и $\langle y''_1, y''_2 \rangle$ — 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

[2]Приводимое рассуждение опирается на идею из примера 3 статьи [9].

$h(y_1'') = y_2''$. 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 $\langle y_1', y_2' \rangle$ и $\langle y_1'', y_2'' \rangle$, у которых $y_1' \neq y_1''$ и $y_2' \neq y_2''$.) Поскольку пара $\langle x_1, x_2 \rangle$ совместима с g, этот общий элемент есть x_1 или x_2 соответственно.

Вернёмся к минимальной мощности достаточного множества решений для произвольных формул. Полученные в теореме 1 оценки на мощность достаточного множества решений аналогичны полученным в статье [3] 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 [10].

При комбинаторном подходе под количеством информации, содержащейся в элементах некоторого множества, подразумевается двоичный логарифм его мощности. Таким образом, комбинаторной сложностью финитной задачи, соответствующей данной формуле, естественно назвать двоичный логарифм минимальной мощности достаточного множества решений. В этих терминах наличие „небольшого“ достаточного множества решений означает, что у задачи всегда есть „простое“ решение. А утверждение теоремы 1 можно переформулировать так.

Следствие 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 $F_1, \ldots, F_k$ комбинаторная сложность соответствующей задачи не превыгает 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 $\log |F_1| \leqslant \log M, \ldots, \log |F_k| \leqslant \log M$ и комбинаторная сложность соответствующей задачи больше или равна $(1/m) \log M - \log(4m)$. Отметим, что, как следует из предложения 6, эта сложность не больше $k \log(M+1)$.

Таким образом, для невыводимых в $\mathfrak{J}$ формул имеется разрыв приблизительно в km (то есть в константу) раз. При алгоритмическом подходе (теорема 1 в статье [3]) 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 [10]). Если $X = \varnothing$, то положим $Kf(\langle F, X\rangle) = \infty$. Фактически, как и в [3], 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 [3] на случай финитных задач.

Теорема 2. *Пусть формула $\Theta(t_1, \ldots, t_k)$ невыводима в логике слабого закона исключённого третьего $\mathfrak{J}$. Если при этом классически выводима формула $\Theta(\bot, \ldots, \bot)$ (вместо всех переменных подставлена* *константа* $\perp$*) 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) $Kf\Bigl(\bigwedge\limits_{\chi[A_i]\neq\varnothing} A_i\Bigr) \leqslant n + C$*;*

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 $\Theta(t_1,\ldots,t_k)$ возьмём построенные в лемме 1 формулы $\tau_1,\ldots,\tau_k$ от переменных $s_1,\ldots,s_m$ и критическую импликацию $J_m(s_1,\ldots,s_m)$. Заметим прежде всего, что если формула $\Theta(\perp,\ldots,\perp)$ выводима, то формула $\Theta(\perp,\ldots,\perp) \to J_m$ интуиционистски невыводима в силу невыводимости критических импликаций (см. [2]). Поэтому хотя бы для одного i выполнено $\tau_i \neq \perp$.

Для данного n возьмём произвольные множества $G_1,\ldots,G_m$ мощности 2^n каждое. Положим $G = \varphi[J_m](G_1,\ldots,G_m)$. 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 леммы 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 $A_i = \tau_i(B_1,\ldots,B_m)$.

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

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

Таким образом, для финитных задач имеет место классификация формул по сложности порождаемых ими задач, аналогичная построенной в [3]. А именно, с каждой формулой $\Theta(t_1,\ldots,t_k)$ свяжем функцию натурального аргумента kf_Θ:

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

Следствие 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* $\mathrm{kf}_\Theta(n) = n + O(1)$.

Автор благодарен своему научному руководителю Н. К. Верещагину за постановку задачи и постоянную помощь в работе, и признателен Ан. А. Мучнику и А. Х. Шеню за многочисленные полезные обсуждения. Ан. А. Мучник прочитал текст и сделал много ценных замечаний. Предварительный вариант статьи был депонирован в ВИНИТИ ([11]).

Литература

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

[2] Верещагин Н. К., Скворцов Д. П., Скворцова Е. З., Чернов А. В. 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.

[3] Чернов А. В. Сложность множеств, полученных как значения пропозициональных формул // Математические заметки. 2004. В печати.

[4] Медведев Ю. Т. Финитные задачи // Доклады АН СССР. 1962. Т. 142. №. 5. С. 1015–1018.

[5] Медведев Ю. Т. Об интерпретации логических формул посредством финитных задач // Доклады АН СССР. 1966. Т. 169. № 1. С. 20–24.

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

[7] Максимова Л. Л., Скворцов Д. П., Шехтман В. Б. Невозможность конечной аксиоматизации логики конечных задач Медведева // Доклады АН СССР. 1979. Т. 245, № 5, С. 1051–1054.

[8] Янков В. А. Об исчислении слабого закона исключённого третьего // Известия АН СССР. Сер. матем.. 1968. Т. 32. № 5. С. 1044–1051.

[9] Shen A., Vereshchagin N. Logical operations and Kolmogorov complexity // Theoretical Computer Science. 2002. V. 271. P. 125–129.

[10] Колмогоров А. Н. Три подхода к определению понятия „количество информации“// Проблемы передачи информации. 1965. Т. 1. № 1. С. 3–11.

[11] Чернов А. В. Финитные задачи и логика слабого закона исключённого третьего. М.: МГУ, 2003. Деп. в ВИНИТИ 03.07.2003, № 1263-В2003, 15 с.