УДК 510.52

Сложность множеств, полученных как значения пропозициональных формул

А. В. Чернов[1]

В классическом исчислении высказываний логические связки можно понимать как операции, позволяющие из элементарных высказываний строить более сложные составные высказывания. Формулы, для которых составное высказывание истинно независимо от истинности входящих в него элементарных высказываний, образуют классическую логику.

Для построения семантики интуиционистской логики Колмогоров в [1] предложил понимать связки как операции, которые элементарным задачам сопоставляют новые, составные задачи, например, „решить первую и вторую задачи“, „из решения первой задачи получить решение второй“. Формулы, для которых составная задача имеет хотя бы одно решение, общее для всех возможных подстановок элементарных задач, образуют исчисление задач. Колмогоров предполагал, что это исчисление совпадает с интуиционистской логикой, построенной Гейтингом.

В статье Колмогорова нет формальной интерпретации для исчисления задач (подобной булевым операциям над истинностными значениями высказываний). Впоследствии разными авторами было предложено несколько естественных уточнений идеи Колмогорова, приводящих к различным суперинтуиционистским логикам, иногда очень сложно устроенным.

В настоящей статье под *задачей* будем понимать произвольное множество двоичных слов, а под *решением задачи* — любой его элемент. Содержательно это множество можно истолковывать как список всех решений некоторой неформальной задачи; более подробная мотивировка, краткий обзор близких подходов и библиография есть в статье [2].

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

Пусть фиксировано некоторое вычислимое кодирование пар двоичных слов (а также троек, четвёрок и вообще наборов произвольной длины). Код пары слов u, v обозначается через $\langle u, v\rangle$ (соответственно, $\langle u_1, \ldots, u_k\rangle$ — код набора $u_1, \ldots, u_k$). Пусть также зафиксирована какая-нибудь главная вычислимая нумерация всех вычислимых одноместных частичных функций на множестве двоичных слов. Через $[u](v)$ обозначается результат применения функции, занумерованной словом u (которое в этом случае называется также программой), к слову v.

Операции над множествами (задачами) X и Y определяются 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 $\Phi(t_1, \ldots, t_k)$ можно по индукции определить составную задачу $\Phi(X_1, \ldots, X_k)$, получающуюся 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 $X_1, \ldots, X_k$.

Операция над множествами превращается в соответствующую той же формуле булеву функцию, если непустое множество интерпретировать как значение „истина“, а пустое — как „ложь“. Отсюда получается следующее простое утверждение (впервые этот факт отметил Плиско в [3]).

Предложение 1. *Формула выводима в классическом исчислении высказываний тогда и только тогда, когда составная задача имеет хотя бы одно решение при любой подстановке задач вместо переменных.*

Можно потребовать, чтобы задача, соответствующая формуле, не просто всегда имела решение, а имела единое решение для всех подстановок (в соответствии с идеей Колмогорова). Плиско в [4] исследовал класс предикатных формул с аналогичным свойством (он назвал их абсолютно реализуемыми). О логике пропозициональных абсолютно реализуемых формул известно довольно мало. Здесь следует упомянуть два факта. Во-первых, индукцией по интуиционистскому выводу легко доказывается следующее утверждение.

Предложение 2. *По формуле, выводимой в интуиционистском исчислении высказываний, можно эффективно построить слово, являющееся решением составной задачи при любой подстановке задач вместо переменных.*

Во-вторых, существуют абсолютно реализуемые, но интуиционистски невыводимые пропозициональные формулы, например, формула Роуза $((\neg\neg\Phi \to \Phi) \to (\neg\Phi \vee \neg\neg\Phi)) \to (\neg\Phi \vee \neg\neg\Phi)$, где $\Phi = \neg t_1 \vee \neg t_2$. Неизвестно, является ли класс всех абсолютно реализуемых пропозициональных формул разрешимым (или хотя бы перечислимым).

В статье [5] предложено более слабое условие на формулу, близкое к реализуемости: соответствующая формуле задача всегда имеет „простое“ решение. Для уточнения этой формулировки используется понятие колмогоровской сложности.

Неформально говоря, *сложностью* $K(x)$ конструктивного объекта x называется длина кратчайшей программы, порождающей x; *условной сложностью* $K(x|y)$ конструктивного объекта x при известном конструктивном объекте y называется длина кратчайшей программы, получающей на вход y и порождающей x. Точное определение и краткий список свойств можно найти в статье [2]. Здесь же необходимо только сказать, что функции $K(x)$ и $K(x|y)$ определены с точностью до аддитивной константы, то есть существуют семейство функций $K(x)$ и семейство функций $K(x|y)$ (своя функция для каждого оптимального языка программирования), и разность между любыми двумя функциями из семейства ограничена константой; поэтому некоторая аддитивная константа фигурирует во всех рассматриваемых в настоящей статье утверждениях о сложности.

Сложностью множества двоичных слов (задачи) X называется минимум колмогоровских сложностей его элементов (решений задачи), то есть $K(X) = \min\{K(x)|x \in X\}$; сложность пустого множества (задачи, не имеющей решений) бесконечна: $K(\varnothing) = \infty$. Рассматриваются формулы, для которых сложность соответствующей составной задачи мала по сравнению со сложностями подставленных задач. В статье [2] показано, что такие формулы образуют логику $\mathfrak{J}$ слабого закона исключённого третьего, которая получается из интуиционистского исчисления высказываний добавлением аксиомы $(\neg t \vee \neg\neg t)$.

Предложение 3. *По формуле, выводимой в $\mathfrak{J}$, можно эффективно построить конечное множество слов, в котором для любой подстановки задач вместо переменных найдётся решение составной задачи.*

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 $Y_k = \bigwedge_{i=1}^{k} Y_1$ 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 некоторой подстановке.

Как показано в статье [6], формула $\Phi(t_1, \ldots, t_k)$ выводима в логике $\mathfrak{J}$ тогда и только тогда, когда интуиционистски выводима формула $\Phi'(t_1, \ldots, t_k) = \bigwedge_{i=1}^{k}(\neg t_i \vee \neg\neg t_i) \to \Phi(t_1, \ldots, t_k)$. Пользуясь предложением 2, для выводимой в $\mathfrak{J}$ формулы Φ можно построить такое слово r, что $r \in \Phi'(X_1, \ldots, X_k)$ для любых $X_1, \ldots, X_k$. Очевидно, что множество $\{[r](y) \mid y \in Y_k\}$ будет искомым (из сказанного выше следует, что программа r определена на всех элементах множества Y_k). $\square$

Из предложения 3, в частности, вытекает, что для любой выводимой в $\mathfrak{J}$ формулы $\Phi(t_1, \ldots, t_k)$ найдётся такая константа C, что $K(\Phi(X_1, \ldots, X_k)) \leqslant C$ для любых $X_1, \ldots, X_k$. В [2] доказано и обратное утверждение, а именно, показано, что для невыводимых в $\mathfrak{J}$ формул сложность соответствующей задачи может расти как линейная функция сложностей подставленных задач. Основной целью настоящей статьи является изложение более простого доказательства следующего более сильного утверждения.

Теорема 1. *Пусть формула $\Phi(t_1, \ldots, t_k)$ невыводима в логике слабого закона исключённого третьего $\mathfrak{J}$. Если при этом $\Phi(\bot, \ldots, \bot) \neq \bot$, 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) $K\Big(\bigwedge\limits_{X_i \neq \varnothing} X_i\Big) \leqslant n + C$;

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

Если формула Φ позитивна, то есть не содержит отрицания и константы $\bot$, то условие $\Phi(\bot, \ldots, \bot) \neq \bot$ можно опустить.

Замечание. Нетрудно показать (см. [2]), что при $\Phi(X_1, \dots, X_k) \neq \varnothing$ верно неравенство

$$K(\Phi(X_1, \dots, X_k)) \leqslant K(\bigwedge_{X_i \neq \varnothing} X_i) + C_\Phi$$

(константа C_Φ зависит только от формулы Φ и выбора функции K), поэтому теорема даёт точную оценку на скорость роста максимальной достижимой сложности составной задачи в зависимости от сложностей подставленных задач.

Доказательство теоремы использует понятие, введённое Медведевым в работе [7]. *Критической импликацией* называется формула вида

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

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

Известно, что ни одна критическая импликация невыводима интуиционистски.

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

$$J_m = \bigwedge_{\varnothing \neq E \subset \{1,\dots,m\}} \Big(\Big(\bigwedge_{j \notin E} s_j \to \bigvee_{i \in E} s_i \Big) \to \bigvee_{i \in E} s_i \Big) \to \bigvee_{i=1}^{m} s_i\,.$$

Пользуясь результатами Медведева и Янкова (см. [7], [6]), можно доказать следующую лемму.

Лемма 1. *Если формула $\Phi(t_1, \dots, t_k)$ невыводима в $\mathfrak{J}$, то найдутся такое $m > 0$ и такие формулы $\tau_1(s_1, \dots, s_m), \dots, \tau_k(s_1, \dots, s_m)$, что интуиционистски выводима импликация $\Phi(\tau_1, \dots, \tau_k) \to J_m$. При этом можно считать, что если формула Φ позитивна, то все τ_i имеют вид $s_m \vee (\bigvee \bigwedge s_j)$, а если формула Φ непозитивна, то при каждом i формула τ_i либо имеет указанный вид, либо является константой $\perp$.*

Таким образом, критические импликации играют особую роль при анализе формул, невыводимых в $\mathfrak{J}$. В то же время для критических импликаций удаётся полностью исследовать сложность составной задачи, получающейся в результате подстановки одноэлементных множеств вместо переменных.

Теорема 2. *Для произвольной критической импликации* $J(s_1,\ldots,s_m)$ *найдётся такая константа* C_0*, что для произвольных двоичных слов* $x_1,\ldots,x_m$ *имеет место неравенство*

$$K(J(\{x_1\},\ldots,\{x_m\})) \geqslant \min_j\{K(x_j|x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_m)\} - C_0\,.$$

Из двух сформулированных утверждений теорема 1 получается следующим образом.

Для невыводимой в $\mathfrak{J}$ формулы Φ возьмём построенные в лемме 1 число m и формулы $\tau_1,\ldots,\tau_k$. 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: существует меньше $2^n/m$ программ с длиной меньше $n-\log_2 m$, поэтому количество наборов из m двоичных слов длины n, не удовлетворяющих указанному условию, меньше $m(2^n/m)2^{n(m-1)} = 2^{nm}$.)

Положим $X_i = \tau_i(\{x_1\},\ldots,\{x_m\})$. Проверим, что множества X_i имеют требуемые свойства. Во-первых, если $\Phi(\bot,\ldots,\bot) \neq \bot$, то формула $\Phi(\bot,\ldots,\bot) \to J_m$ не может быть интуиционистски выводимой, поэтому хотя бы для одного i выполнено $\tau_i \neq \bot$, то есть $X_i \neq \varnothing$. Во-вторых, если X_i непусто, то оно имеет вид $\{x_m\} \vee \ldots$, поэтому

$$K(\bigwedge_{X_i\neq\varnothing} X_i) \leqslant K(x_m) + O(1) \leqslant n + C$$

для некоторой константы C, зависящей только от чисел k и m и выбора функции K. В-третьих, из предложения 2 и интуиционистской выводимости импликации $\Phi(\tau_1,\ldots,\tau_k) \to J_m$ следует, что

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

где константа C' зависит только от формул Φ и J_m и выбора функции K. Отсюда и из полученной в теореме 2 оценки на сложность J_m получаем, что

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

Осталось доказать использованные утверждения.

Доказательство теоремы 2. Пусть J — произвольная критическая импликация от m переменных, а $x_1, \ldots, x_m$ — произвольные двоичные слова.

Для упрощения обозначений отождествим натуральное число j и его двоичную запись. Обозначим через ε пустое слово.

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. *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 $x_1, \ldots, x_m$*

$$K\bigl(\Lambda_m(\{x_1\}, \ldots, \{x_m\}) \to ((\bar{P} \to \bar{Q}) \to \bar{Q})\bigr) \leqslant C_1\,,$$

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 функции K.

Доказательство. Следующий алгоритм находит некоторый элемент из $\bar{Q}$ 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 $P(\{x'_1\}, \ldots, \{x'_m\})$. Если первой завершила работу программа r и результат принадлежит множеству $Q(\{x'_1\}, \ldots, \{x'_m\})$, то выдаём этот результат. Пусть первой завершила работу программа q и результат равен j. Если при этом переменная s_j входит в конъюнкцию P, то выдаём любой элемент из $Q(\{x'_1\}, \ldots, \{x'_m\})$, а иначе выдаём результат работы r (когда он определится).

Легко убедиться в корректности алгоритма, поскольку если значение q на пустом слове определено и переменная s_j (где j есть результат работы q) входит в конъюнкцию P, то $Q(\{x'_1\}, \ldots, \{x'_m\}) = \bar{Q}$, а в противном случае $P(\{x'_1\},\dots,\{x'_m\}) = \bar{P}$ (P и Q не имеют общих переменных).

Очевидно, что для задания алгоритма достаточно знать только формулы P и Q. □

Лемма 3. *Если* $p \in \Lambda_m(\{x_1\},\dots,\{x_m\}) \to (\{x_1\} \vee \{x_2\} \vee \dots \vee \{x_m\})$, *то* $K(p) \geqslant \min_j\{K(x_j|x_1,\dots,x_{j-1},x_{j+1},\dots,x_m)\} - C_2$, *где константа* C_2 *зависит только от числа* m *и выбора функции* K.

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

Рассмотрим значения вычислимой функции p на $\langle x_1,\dots,x_m,q_u\rangle \in \Lambda_m(\{x_1\},\dots,\{x_m\})$ при всевозможных u. Можно считать, что эти значения имеют вид $\langle j, x_j\rangle$, где $j \in \{1,\dots,m\}$. Очевидно, что это j является всюду определённой вычислимой функцией u. Поэтому найдётся такое слово u_0 (а именно, программа 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 $x_1,\dots,x_{j_0-1},x_{j_0+1},\dots,x_m$ эффективно построить x_{j_0}. Параллельно для всех пар $\langle u,v\rangle$ будем проверять следующее свойство:

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

$$\text{и}$$

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

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

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

Пусть p' — элемент множества $J(\{x_1\},\dots,\{x_m\})$. Используя лемму 2, нетрудно по программе p' эффективно построить программу p, принадлежащую множеству $\Lambda_m(\{x_1\},\dots,\{x_m\}) \to (\{x_1\} \vee \dots \vee \{x_m\})$ (программа p, получив на вход элемент множества $\Lambda_m(\{x_1\},\dots,\{x_m\})$, строит элементы каждой из посылок $(P_i \to Q_i) \to Q_i$ критической импликации J, а затем применяет к составленному из них кортежу программу p'). Поскольку $K(p) \leqslant K(p') + O(1)$, из леммы 3 следует утверждение теоремы. □

Замечание. Доказательство теоремы 2 обобщает рассуждение из примера 6 в статье [5]. Чтобы сделать изложение более ясным, здесь введена операция Λ_m, а само доказательство разбито на две леммы.

Доказательство леммы 1. Пусть формула $\Phi(t_1, \ldots, t_k)$ невыводима в $\mathfrak{J}$. Для таких формул Янков в [6, § 3] доказал следующее. Если формула Φ позитивна, то она невыводима и интуиционистски. В противном случае найдётся такая позитивная невыводимая интуиционистски формула $\Psi(t_1, \ldots, t_l)$, что выводима импликация $\Phi^* \to \Psi$, где Φ^* получается из Φ подстановкой константы $\perp$ вместо некоторых из переменных $t_1, \ldots, t_k$ (формула Ψ может содержать и переменные, не встречающиеся в Φ).

Как отмечено Медведевым в статье [7], если позитивная формула Ψ невыводима интуиционистски, то из неё выводится некоторая критическая импликация J. Из следующего усиленного варианта этого утверждения непосредственно вытекает лемма 1.

Лемма 4. *Если позитивная формула $\Psi(t_1, \ldots, t_l)$ интуиционистски невыводима, то найдутся такое $m > 0$ и такие формулы τ_i' вида $s_m \vee (\bigvee \bigwedge s_j)$, что импликация $\Psi(\tau_1, \ldots, \tau_l) \to J_m$ интуиционистски выводима.*

Доказательство этой леммы в основном повторяет доказательство теоремы Медведева, приведённое в параграфе 2 статьи [2], поэтому здесь после напоминания необходимых фактов будет изложена только подходящим образом модифицированная завершающая часть рассуждения.

Для каждого $m > 0$ рассматривается шкала Крипке σ_m — семейство всех собственных подмножеств множества $\{1, \ldots, m\}$, упорядоченное по включению, гейтингова алгебра открытых подмножеств шкалы σ_m обозначается $H(\sigma_m)$. Лемма 2 из [2] утверждает, что если позитивная формула $\Psi(t_1, \ldots, t_l)$ невыводима в интуиционизме, то для некоторого m формула Ψ опровергается на шкале σ_m, то есть существуют такие $a_1, \ldots, a_l \in H(\sigma_m)$, что $\Psi(a_1, \ldots, a_l) \neq \mathbf{1}$ в $H(\sigma_m)$. Из доказанных там же лемм 3 и 4 следует, что в этом случае выводима формула

$$\Psi(\tau_1'(s_1, \ldots, s_m), \ldots, \tau_l'(s_1, \ldots, s_m)) \to J_m(s_1, \ldots, s_m)\,,$$

где $\tau_i'(s_1, \ldots, s_m) = \bigvee_{E \in a_i} \bigwedge_{j \in E} s_j$, если $a_i \neq \varnothing$ и $a_i \neq \mathbf{1}$, $\tau_i'(s_1, \ldots, s_m) = \bigwedge_{j=1}^n s_j$ для $a_i = \varnothing$ и $\tau_i'(s_1, \ldots, s_m) = \perp \to \perp$ для $a_i = \mathbf{1}$. Таким образом, достаточно показать, что можно выбрать m и $a_1, \ldots, a_l$ так, чтобы при каждом i выполнялись условия $\{m\} \in a_i$ и $a_i \neq \mathbf{1}$.

Пусть m и $a'_1, \ldots, a'_l \in H(\sigma_{m-2})$ таковы, что $\Psi(a'_1, \ldots, a'_l) \neq \mathbf{1}$ в $H(\sigma_{m-2})$. В шкале σ_m возьмём открытые множества

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

(неформально говоря, множество a_i получается так: в σ_m из конуса над $(m-1)$ выбрасываются максимальные точки; в оставшейся части конуса, изоморфной шкале σ_{m-2}, берётся образ множества a'_i, который уже не будет открытым в σ_m; к нему добавляются все максимальные точки, а также конус над точкой m). Заметим, что по построению $\{m\} \in a_i$ и $\varnothing \notin a_i$, то есть $a_i \neq \mathbf{1}$.

Для любой позитивной формулы Θ индукцией по построению нетрудно показать, что если $E \subset \{1, \ldots, m-2\}$, то $E \in \Theta(a'_1, \ldots, a'_l)$ в $H(\sigma_{m-2})$ тогда и только тогда, когда $E \cup \{m-1\} \in \Theta(a_1, \ldots, a_l)$ в $H(\sigma_m)$. Элементы $a'_1, \ldots, a'_l$ выбирались так, что $\varnothing \notin \Psi(a'_1, \ldots, a'_l)$ 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 $H(\sigma_m)$.

Доказательство леммы 1, а с ней и теоремы 1, полностью завершено. $\square$

Замечанию после теоремы 1 можно придать точный смысл. Для каждой пропозициональной формулы $\Phi(t_1, \ldots, t_k)$ рассмотрим функцию

$$f_\Phi(n) = \max\Big\{K(\Phi(X_1, \ldots, X_k)) \;\Big|\; (\exists i\, X_i \neq \varnothing) \;\Rightarrow\; K\Big(\bigwedge_{X_i \neq \varnothing} X_i\Big) \leqslant n\Big\}.$$

Теорема 1 вместе с неравенством, приведённом в замечании, а также предложениями 1 и 3 даёт полное описание асимптотического поведения этой функции для всех возможных формул Φ. А именно:

- если формула Φ выводится в $\mathfrak{J}$, то $f_\Phi(n) = O(1)$;
- если формула Φ не выводится в классической логике, то $f_\Phi(n) = \infty$ при достаточно больших n;
- если формула Φ не выводится в $\mathfrak{J}$, но выводится в классической логике, то $f_\Phi(n) = n + O(1)$.

В последнем случае значение $n + O(1)$ может быть достигнуто на множествах, мощности которых конечны и не превышают 2^m, то есть зависят только от формулы Φ, но не от аргумента функции n; из анализа доказательств теорем Янкова и Медведева видно, что $m \leqslant 2+2^{N(\Phi)}$, где $N(\Phi)$ — количество всех подформул формулы Φ. Интересно было бы для каждой формулы Φ найти оптимальную оценку мощности таких множеств, то есть наименьшую константу $S = S(\Phi)$, для которой функция

$$f_{\Phi,S}(n) = \max\Big\{K(\Phi(X_1,\ldots,X_k)) \,\Big|\, K\Big(\bigwedge_{X_i\neq\varnothing} X_i\Big) \leqslant n \;\&\; \forall i\; |X_i| \leqslant S\Big\}$$

асимптотически равна $n+O(1)$ (а может быть, и набор таких констант $S_1,\ldots,S_k$, отдельно для каждого $X_1,\ldots,X_k$). Например, для закона исключённого третьего $S = 1$, поскольку $K(\{x\}\vee\neg\{x\}) = K(x)+O(1)$ для любого двоичного слова x. Однако в общем случае неочевидно даже, может ли $S(\Phi)$ принимать сколь угодно большие значения.

Рассмотрим один пример вычисления $S(\Phi)$. Как нетрудно убедиться, из доказательства теоремы 1 вытекает оценка $S(J) \leqslant 2$ для всех критических импликаций J. Оказывается, что $S(J_m) = 2$. Действительно, предположим, что $S(J_m) = 1$. Среди посылок критической импликации J_m для каждого $j \in \{1,\ldots,m\}$ есть формула $((\bigwedge_{i\neq j} s_i) \to s_j) \to s_j$, поэтому

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

Легко проверить, что для любых двоичных слов $x_1,\ldots,x_m$ таких, что $K(\bigwedge\{x_i\}) \leqslant n$, верна оценка $\min_j\{K(x_j|x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_m)\} \leqslant n/m + O(\log n)$, поэтому $f_{J_m,1}(n) \ll n + O(1)$.

Ту же самую верхнюю оценку на сложность J (и тем самым неравенство $S(J) \neq 1$) можно доказать не только для J_m, но и для некоторых других критических импликаций J. Если для всех $j \in \{1,\ldots,m\}$ среди посылок $J(s_1,\ldots,s_m)$ есть формулы $((\bigwedge_{i\neq j} s_i) \to s_j) \to s_j$, то изложенное доказательство остаётся верным. Однако достаточно, если посылка импликации содержит эти формулы для всех $j \neq l$ при каком-нибудь l, и это вытекает из следующих двух утверждений, которые дополняют леммы 2 и 3 и верны для произвольных двоичных слов $x_1,\ldots,x_m$.

Во-первых, для любого $l \in \{1,\ldots,m\}$

$$K\Big(\bigwedge_{j\neq l}\big((\bigwedge_{i\neq j}\{x_i\} \to \{x_j\}) \to \{x_j\}\big) \to \Lambda_m(\{x_1\}\ldots\{x_m\})\Big) = O(1)\,.$$

(Доказательство требует довольно громоздких рассуждений. Основная идея состоит в том, что, используя приём из примера 3 в статье [5], по любому элементу из $\bigwedge_{i\neq j}\{x_i\} \to \{x_j\}$ можно „почти эффективно“ найти либо $\langle x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m\rangle$, либо x_j).

Во-вторых, для любого $j \in \{1, \ldots, m\}$

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

(достаточно применить лемму 2 к $P = \bigwedge_{i\neq j} s_i$ и $Q = s_j$, и учесть, что $K(\bigwedge_{i\neq j}\{x_i\} \to \{x_j\}) = K(x_j|x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m) + O(1)$).

Для критических импликаций J_m функция $f_{J_m,1}(n)$ хотя и не равна $n + O(1)$, всё же растёт линейно по n. Однако бывает и так, что $f_{\Phi,1}(n) = o(n)$, а $f_{\Phi,2}(n) = n + O(1)$. В качестве примера можно рассмотреть закон Пирса $\Phi(t, s) = ((t \to s) \to t) \to t$ (он невыводим в $\mathfrak{J}$). В [5] показано, что для любых двоичных слов x, y сложность множества $((\{x\} \to \{y\}) \to \{x\}) \to \{x\}$ не превышает $O(\log(K(x) + K(y)))$ (то есть $f_{\Phi,1}(n) = O(\log n)$). С другой стороны, интуиционистски выводима импликация $\Phi(t \vee s, s) \to J_2(t, s)$, поэтому для множеств $X = \{x, y\}$ и $Y = \{y\}$, где x и y имеют длину n, а $K(x, y) \geqslant 2n$, верна оценка $K(\Phi(X, Y)) \geqslant n - O(1)$.

Автор благодарен своему научному руководителю Н. К. Верещагину за постановку задачи и постоянную помощь в работе, а также Ан. А. Мучнику и А. Х. Шеню за многочисленные полезные обсуждения.

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. В печати.

[3] Плиско В. Е. О языках с конструктивными логическими связками // Доклады АН СССР. 1987. Т. 296. № 1. С. 35–38.

[4] Плиско В. Е. Абсолютная реализуемость предикатных формул // Известия АН СССР. Сер. матем. 1983. Т. 47. № 2. С. 315–334.

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

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

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