мости следует аналогичный результат для Int. Вначале покажем, что справедлива

Лемма 20. *Пусть* $\mathfrak{A}$ *— псевдобулева алгебра и* $\mathfrak{A} \in Q(\mathcal{F}_\omega(\mathrm{Int}))$, *тогда обертывающая* $\mathfrak{A}$ *топобулева алгебра* $S(\mathfrak{A})$ *входит в* $Q(\mathcal{F}_\omega(\mathrm{Grz}))$.

Доказательство. Пусть $S(\mathfrak{A}) \notin Q(\mathcal{F}_\omega(\mathrm{Grz}))$. Тогда найдется квазитождество $q = (f(x_i) = 1 \Rightarrow g(x_i) = 1)$ такое, что $\neg(S(\mathfrak{A}) \vDash q)$ и $\mathcal{F}_\omega(\mathrm{Grz}) \vDash q$. Из строения $S(\mathfrak{A})$ следует, что

$$\neg(S(\mathfrak{A}) \vDash \Box f(\varphi_i(\Box y_i)) = 1 \Rightarrow \Box g(\varphi_i(\Box y_j)) = 1),$$

где φ_i — некоторые термы. Но формулы $\Box f(\varphi_i(\Box y_j))$ и $\Box g(\varphi_i(\Box y_j))$ эквивалентны в Grz некоторым формулам $T(A)$ и $T(B)$. Следовательно, $\neg(S(\mathfrak{A}) \vDash T(A) = 1 \Rightarrow T(B) = 1)$, где $\mathcal{F}_\omega(\mathrm{Grz}) \vDash T(A) = 1 \Rightarrow T(B) = 1$. Тогда $\neg(\mathfrak{A} \vDash A = 1 \Rightarrow B = 1)$ и $\mathcal{F}_\omega(\mathrm{Int}) \vDash A = 1 \Rightarrow B = 1$. Следовательно, $\mathfrak{A} \notin Q(\mathcal{F}_\omega(\mathrm{Int}))$. Лемма доказана.

Пусть $\mathfrak{A}$ — конечная псевдобулева алгебра и $\mathfrak{A} \in Q(\mathcal{F}_\omega(\mathrm{Int}))$, тогда $S(\mathfrak{A}) \in Q(\mathcal{F}_\omega(\mathrm{Grz}))$ и по аналогу для Grz теоремы 19 $S(\mathfrak{A}) \vDash \varphi_2$, т. е. ширина $S(\mathfrak{A})^+$ не выше 2. Тогда и представляющее множество псевдобулевой алгебры $\mathfrak{A}$ имеет ширину не выше 2, и на $\mathfrak{A}$ истинна формула A_2, выражающая это свойство. Но $A_2 \notin \mathrm{Int}$ и правило $p \supset p/A_2$ недопустимо в Int, а является истинным на $\mathfrak{A}$. Следовательно, Int неаппроксимируема финитно по допустимости.

СПИСОК ЛИТЕРАТУРЫ

1. **Segerberg K.** An essay in classical modal logic. Vol. 1—3.— Uppsala, 1971.
2. **Solovay R. M.** Provability interpretation of modal logic // Isr. J. math.— 1976.— Vol. 25.— P. 287—304.
3. **Friedman H.** One hundred and two problems in mathematical logic // J. symb. log.— 1975.— Vol. 40, N 3.— P. 113—130.
4. **Артемов С. Н.** Приложения модальной логики в теории доказательств // Вопросы кибернетики. Неклассические логики и их применение.— М., 1982.— С. 3—22.
5. **Boolos G.** Fridman's 35-th problem has an affirmative solution // Not. Amer. Math. Soc.— 1975.— Vol. 22.— P. 646.
6. **Циткин А. И.** О допустимых правилах интуиционистской логики высказываний // Мат. сб.— 1977.— Т. 102, № 2.— С. 314—323.
7. **Рыбаков В. В.** Критерий допустимости правил вывода в модальной логике S4 и интуиционистской логике // Алгебра и логика— 1984.— Т. 23, № 5.— С. 546—572.
8. **Рыбаков В. В.** Базисы допустимых правил модальной системы и интуиционистской логики // Мат. сб.— 1985.— Т. 170, № 11.— С. 321—339.
9. **Рыбаков В. В.** Базисы допустимых правил логик S4 и Crz // Алгебра и логика.— 1985.— Т. 24, № 1.— С. 87—107.
10. **Рыбаков В. В.** Допустимые правила предтабличных модельных логик // Там же.— 1981.— Т. 20, № 4.— С. 440—464.
11. **Рыбаков В. В.** Разрешимость проблемы допустимости в конечно-слойных модельных логиках // Там же.— 1984.— Т. 23, № 1.— С. 100—116.
12. **Рыбаков В. В.** Допустимые правила для логик, включающих S4.3 // Сиб. мат. журн.— 1984.— Т. 25, № 5.— С. 141—145.
13. **Port J.** The deducibilities S5 // J. phil. log.— 1981.— Vol. 10.— P. 409—422.
14. **Кузнецов А. В., Муравицкий А. Ю.** Доказуемость как модальность // Актуальные проблемы логики и методологии науки.— Киев: Наук. думка, 1980.— С. 193—229.
15. **Мальцев А. И.** Алгебраические системы.— М.: Наука, 1970.

В. Ю. САЗОНОВ

ЭКВИВАЛЕНТНОСТЬ ПОЛИНОМИАЛЬНОЙ КОНСТРУКТИВНОСТИ ПРИНЦИПА МАРКОВА РАВЕНСТВУ P = NP

Настоящая статья является полным и подробным вариантом [1] и развитием [2, 3]. Ее название и основной результат можно было бы сформулировать даже в виде следующего на первый взгляд сомнительного, но при соответствующем необходимом уточнении верного утверждения: *конструктивность принципа Маркова равносильна равенству* P = NP.

Напомним, что «P = NP?» — это известная проблема теории сложности вычислений [4] о совпадении классов P и NP предикатов, вычислимых на детерминированных и соответственно недетерминированных машинах Тьюринга за полиномиальное время *).

Поскольку принцип Маркова

$$M\colon\ \neg\neg\exists x\alpha \supset \exists x\alpha,$$

где α — разрешимая формула, известен как законный принцип так называемого «русского конструктивизма», из приведенного утверждения, казалось бы, следует решение проблемы «P = NP?», причем, против ожидания, в виде именно равенства. Однако, как мы увидим этот результат, скорее, обосновывает неконструктивность принципа Маркова в случае отказа от общепринятой в конструктивной, а также и в классической математике абстракции потенциальной осуществимости. Что касается гипотезы $P \neq NP$, то здесь устанавливается всего лишь *недоказуемость в некоторой слабой* (по сравнению с классической и конструктивной арифметикой) *теории близкого к ней утверждения об экспоненциальной сложности* NP-*полных задач* (ср. [2, 3]). Это второй основной результат статьи.

Читатель, предпочитающий последовательное формальное изложение, может перейти сразу к § 2.

Автор благодарен Н. В. Белякину и Д. Е. Пальчунову за ряд полезных замечаний по тексту статьи.

§ 1. ПРЕДВАРИТЕЛЬНЫЕ РАССМОТРЕНИЯ, МОТИВИРОВКИ И ФОРМУЛИРОВКИ РЕЗУЛЬТАТОВ

Мы будем рассматривать понятие конструктивности того или иного принципа только по отношению к какой-то формальной теории, в рамках которой этот принцип формулируется. В качестве такой теории обычно выступает, как минимум, гейтингова арифметика HA, содержащая (как и классическая арифметика PA) схему полной математической индукции. Нас же будут интересовать теории с гораздо более слабой формой индукции так, что в них даже не доказуема осуществимость экспоненты, т. е. нельзя вывести, что стандартная машина Тьюринга, вычисляющая экспоненту 2^n, останавливается за конечное число шагов на любом входе n. Поэтому здесь можно без противоречия добавить аксиому: для некоторого натурального n эта машина Тьюринга никогда не остановится (что с учетом вычислительной практики и общепринятого негативного отношения к экспоненциальной сложности вполне справедливо). Во всем остальном эти *безэкспоненциальные* теории не очень уступают традиционным формальным системам вроде PA или HA и пригодны для рассмотрения вопросов дискретной математики. Например, в них можно успешно развивать теорию машин Тьюринга и частично рекурсивных функций (ЧРФ), доказать теорему об универсальной ЧРФ, рассматривать теорию реализуемости по Клини и т. п. Одна из целей статьи заключается в демонстрации этой возможности.

Интерес к слабым теориям, фрагментам арифметики Пеано и т. п. в последнее время сильно возрос (см., например, книги [5, 6]). В нашу задачу не входит давать здесь сколько-нибудь полный обзор или список работ на эту тему. Поясним лишь, что предлагаемый в [1—3, 7—9] и в данной работе подход связан с осознанием особой роли понятия и теории полиномиальной вычислимости (ПВ) с точки зрения оснований математики.

---

*) При этом считается, что недетерминированная (и в частности, детерминированная) машина Тьюринга вычисляет предикат $Q(x)$ за полиномиальное время $p(n)$, если для любого входа x длины n истинность $Q(x)$ равносильна существованию пути вычисления длины $p(n)$, на котором будет получен результат «да».

Отправной точкой здесь служит следующий вариант $PA_{\square}$ обычной арифметики Пеано PA. Во-первых, изменим аксиомы PA, касающиеся операции прибавления единицы так, чтобы для некоторого натурального числа $\square$ было $\square + 1 = \square$ и чтобы это число было последним в натуральном ряду 0, 1, 2, ..., $\square - 1$, $\square$, описываемом этой формальной теорией. Никакой информации о конкретной величине числа $\square$ в аксиомах не содержится. Поэтому моделью для такой теории может служить любой конечный отрезок обычного «стандартного» натурального ряда (или даже нестандартно-конечный отрезок). В частности, здесь нельзя доказать, например, что $3 \neq 5$. Во-вторых, постулируем всевозможные рекурсивные (в том числе и все примитивно-рекурсивные) описания общерекурсивных функций в конечном натуральном ряду 0, 1, ..., $\square$ в виде равенств $\bar{f} = \overline{T}(\bar{f})$, где $\bar{f}$ — описываемые функции, а $\overline{T}$ — произвольные термы, составленные из $\bar{f}$ и заданных операций 0, $x + 1$, $=$, ЕСЛИ-ТО-ИНАЧЕ. В-третьих, примем, как и в PA, схему индукции, в которой, конечно, могут участвовать введенные рекурсивные функции. Заметим, что в отличие от обычной арифметики PA бесконечного натурального ряда здесь рекурсивные функции приходится добавлять явным образом. (Можно также ввести в язык $PA_{\square}$, в рекурсивные описания и в схему индукции функциональные или предикатные параметры, перейдя к более общему понятию относительно-рекурсивных функций или, точнее, рекурсивных функционалов и операторов в конечном натуральном ряду.)

Полученную теорию $PA_{\square}$ можно считать *теорией полиномиальной вычислимости*, поскольку, как показано в [7, 10], (относительно) рекурсивные функции в конечном ряду 0, 1, ..., $\square$ с переменной верхней границей $\square$ — это в точности все функции в таком натуральном ряду, вычислимые на машине Тьюринга (относительно функциональных параметров) за время полиномиальное от величины $\square$ *).

Главное в такой характеризации полиномиальной вычислимости это то, что соответствующая ей теория $PA_{\square}$, благодаря конечности описываемого ею натурального ряда, не использует абстракцию потенциальной осуществимости (т. е. абстракцию от самого существования ресурсных ограничений). Этим, по существу, и обосновывается отношение полиномиальной вычислимости к основаниям математики (см. также [2, 7—9], где в подобных терминах формулируется аналог тезиса Черча для полиномиальной вычислимости).

Можно рассмотреть и аналогичный вариант $\mathrm{PA}^2_{\square}$ арифметики второго порядка с использованием кванторов по функциональным и предикатным переменным. (В [2, с. 573] подобная арифметика была описана под именем UBA.) Благодаря известному результату [15] о Σ^1_1-представлении в конечных линейно упорядоченных моделях класса $NP \supseteq P$ здесь не обязательно рассматривать все рекурсивные функции в конечном натуральном ряду в качестве исходных.

Заметим, что такая параметрическая конечность натурального ряда не является препятствием для построения на его основе дискретной математики и даже некоторого нестандартного варианта анализа бесконечно малых. Например, последнее довольно убедительно продемонстрировано в [16].

В отличие от обычной арифметики кванторы первого порядка в конечном натуральном ряду не приводят к эффектам вроде арифметической неразрешимости. Поэтому нет особого смысла рассматривать интуиционистский вариант $HA_{\square}$ арифметики $PA_{\square}$. Не совсем так обстоит

*) В [10] показано также, что примитивная рекурсия (в отличие от подразумеваемой выше общей рекурсии) в конечном натуральном ряду соответствует понятию вычислимости с логарифмической памятью. Заметим, что примитивную рекурсию в конечном натуральном ряду, видимо, впервые рассматривал А. Мостовский [11]. Аналогичные результаты были получены в [12—14] в связи с теорией реляционных баз данных.

дело с кванторами второго порядка: они могут вывести за пределы полиномиальной вычислимости (т. е. рекурсивности в конечном натуральном ряду). В силу упомянутого Σ^1_1-представления класса NP, это утверждение равносильно гипотезе $P \neq NP$. Да и просто интуитивно, квантор по одноместным предикатам над 0, 1, ..., $\square$ приводит к перебору чрезвычайно большого, экспоненциального числа $2^{\square+1}$ таких предикатов. Поэтому здесь уже имеет смысл перейти к (тому или иному) конструктивному варианту $HA^2_\square$ теории $PA^2_\square$ так, чтобы в случае выводимости, скажем, формулы вида $\forall P \exists Q \varphi(P, Q)$ предикат Q был бы рекурсивен относительно P и, значит, вычислялся бы по P за полиномиальное, а не экспоненциальное время.

Заметим, что конструктивность соответствующего варианта принципа Маркова $\neg\neg\exists P \varphi(P) \supset \exists P \varphi(P)$, где φ — (полиномиально разрешимая) формула первого порядка в конечном натуральном ряду, сразу вызывает сомнения, так как его обычное конструктивное обоснование или «реализация» превращается здесь в полный экспоненциальный перебор всех предикатов P, пока не найдется нужный. Поэтому не так уж удивительно, что конструктивность такого вида принципа Маркова может оказаться эквивалентной равенству $P = NP$.

Кстати, здесь возникает весьма принципиальный вопрос: в каком порядке перебирать предикаты P для реализации такого принципа Маркова? Только-ли в лексикографическом? Оказывается, среди всех возможных способов перебора существует *полиномиально оптимальный* (см. § 4 и [2]), и он будет играть существенную роль в дальнейших построениях.

Однако такой оптимальный перебор определяется в терминах множества двоичных слов $\{0, 1\}^*$ произвольной длины, а не конечного натурального ряда. То же можно сказать и о понятии реализуемости по Клини [17, 18], которым мы собираемся воспользоваться для изучения конструктивности принципа Маркова и теории полиномиальной вычислимости. Поэтому мы будем рассматривать эти вопросы в более традиционной (по форме иной, но по существу близкой) постановке, на основе (потенциально) бесконечного множества двоичных слов. (В случае же $HA^2_\square$ естественно было бы применить гёделевскую интерпретацию [19] функционалов конечных типов над конечным натуральным рядом или технику ФОРМУЛЫ-КАК-ТИПЫ [20].)

Итак, рассмотрим *бескванторную теорию* T_0 *полиномиальной вычислимости* над множеством $\{0, 1\}^*$ всех конечных двоичных слов. А именно, пусть T_0 — (для простоты все) истинные бескванторные формулы, составленные из полиномиально вычислимых функций (ПВФ) и предикатов на множестве $\{0, 1\}^*$ плюс классическая логика первого порядка. Аналогично пусть T — (все) истинные в $\{0, 1\}^*$ формулы в этом языке с *ограниченными кванторами* $\forall x < t$, $\exists x < t$, где $<$ — (полиномиально вычислимый) лексикографический линейный порядок на $\{0, 1\}^*$.

Понятно, что такие ограниченные кванторы играют роль кванторов второго порядка в конечном натуральном ряду, поскольку здесь по существу идет речь об ограничении на длину двоичного слова, воспринимаемого как конечный предикат. Если же в этих кванторах дополнительно потребовать, чтобы переменная x пробегала только унарные слова из $\{1\}^*$, то они будут соответствовать кванторам первого порядка арифметики $PA_\square$. Нетрудно понять, что такие унарные ограниченные кванторы, в отличие от ограниченных кванторов $\forall x < t$ и $\exists x < t$ по двоичным словам, выразимы в T_0 бескванторными формулами, так как они сохраняют полиномиальную вычислимость.

Наконец, обозначим через HT_0 интуиционистский вариант теории T_0 (т. е. HT_0 = нелогические аксиомы T_0 + интуиционистская логика). Заметим, что только нелогические аксиомы теорий T_0 и HT_0 являются бескванторными формулами. В доказательствах же и в формулировках теорем можно использовать и неограниченные кванторы по всему бесконечному универсуму двоичных слов.

Как мы увидим, в этих теориях можно определить обычное понятие частично рекурсивной функции (ЧРФ) и ввести обозначение Клини $\{e\}(x)$ для результата применения алгоритма e к двоичному слову x. Заметим, что экспонента здесь является ЧРФ, причем ее всюдуопределенность недоказуема в Т. Более того, в HT_0, T_0 и Т *доказуемо-рекурсивные функции* (т. е. ЧРФ, для которых удается доказать их всюдуопределенность) — *это в точности все функции, вычислимые за полиномиальное время.*

Далее, *тезис Клини — Черча* ECT (ECT_U) — это, как обычно, схема аксиом

$$\forall x(\psi(x) \supset \exists y \varphi(x, y)) \supset \exists e \forall x(\psi(x) \supset ! \{e\}(x) \wedge \varphi(x, \{e\}(x))),$$

где во избежание противоречия в ψ связки $\vee$ и $\exists$ применяются только к бескванторным подформулам (и в случае ECT_U кванторы $\exists$ в ψ, кроме того, имеют вид $\exists v \in \{1\}^*$).

Определим также *два варианта принципа Маркова*

$$\text{M: } \neg\neg\exists x \alpha(x) \supset \exists x \alpha(x),$$

$$\text{M}_U\text{: } \neg\neg\exists x \in \{1\}^* \alpha(x) \supset \exists x \in \{1\}^* \alpha(x),$$

где α — произвольная бескванторная формула.

Формальную теорию назовем *конструктивной*, если из выводимости в ней произвольного предложения вида

$$\forall \bar{x}(\chi(\bar{x}) \supset \exists y \varphi(\bar{x}, y))$$

с U-харроповой (см. начало § 3) посылкой χ следует выводимость предложения вида

$$\forall \bar{x}(\chi(\bar{x}) \supset ! t(\bar{x}) \wedge \varphi(\bar{x}, t(\bar{x})))$$

для некоторого частично рекурсивного терма $t(\bar{x})$. Теорию назовем $\exists$-*конструктивной*, если предыдущее имеет место в отсутствии посылки χ, или когда $\chi \rightleftharpoons$ ИСТИНА. Если при этом $t(\bar{x})$ — ПВФ, то теория называется *полиномиально* $\exists$-*конструктивной.*

Мы можем теперь сформулировать точно основные результаты статьи.

1. *Теории* HT_0, $HT_0 + M_U$, $HT_0 + ECT_U$ *и* $HT_0 + ECT_U + M_U$ *конструктивны и даже полиномиально* $\exists$-*конструктивны* (см. 7.4 (б) и 6.5 (б)).

2. *Теория* $HT_0 + ECT_U + M (= HT_0 + ECT + M_U = HT_0 + ECT + M)$ (*полиномиально* $\exists$-) *конструктивна тогда и только тогда, когда* $P = NP$. *То же верно и для теории* $HT_0 + ECT$ (см. 6.10).

3. *Теория* $HT_0 + ECT + M$ *консервативно расширяет* T_0 *и* HT_0 *относительно* Π_2-*предложений. В частности, ее доказуемо-рекурсивные функции — это в точности все* ПВФ, *и в ней невыводима осуществимость экспоненты* (см. 6.7).

4. $HT_0 + ECT \vdash \exists e\, SA(e)$, *где* $SA(e) \rightleftharpoons$ «*e есть детерминированный алгоритм поиска выполняющего кортежа для выполнимых пропозициональных формул*» (см. 2.1 (а)).

5. *В частности, из утверждений* 3 *и* 4 *следует, что в теории* $HT_U + ECT + M$ (как и в T_0 [2]) *невыводима никакая монотонная сверхполиномиальная нижняя оценка времени работы таких алгоритмов поиска* (см. 6.8).

6. *Следующие теории являются конструктивными*: $HT_0 + SA(e)$, $HT_0 + SA(e) + M = HT_0 + SA(e) + M_U$, $HT_0 + SA(e) + ECT = HT_0 + SA(e) + ECT_U$ *и* $HT_0 + SA(e) + ECT + M$, *где e — новая константа, обозначающая некоторый (неизвестный) алгоритм поиска* (см. 7.4 (а) и 6.5 (а)). *Однако если в этих теориях заменить* $SA(e)$ *на* $\exists e SA(e)$, *то конструктивность каждой из них будет равносильна равенству* $P = NP$ (см. (3.2).

7. *Теория* $HT_0 + M$ *полиномиально* $\exists$-*конструктивна* (см. 7.6).

8. *Конструктивность* (без «∃»!) *теории* $HT_0 + M$ *равносильна равенству* $P = NP$ (см. 7.5).

Итак, мы видим, что только «унарные» варианты ECT_U и M_U тезиса Черча и принципа Маркова могут быть признаны в нашей постановке конструктивными (и даже полиномиально ∃-конструктивными) без каких-то оговорок. Для обоснования же конструктивности ECT и M надо привлечь либо утверждение $P = NP$, которое даже оказывается эквивалентным конструктивности ECT и M, либо гипотетический алгоритм поиска (ср. с замечаниями в конце § 3), либо аксиому об осуществимости экспоненты, которая, очевидно, гарантирует существование такого алгоритма поиска.

Субъективно, ECT_U отличается от ECT, скорее техническим, хотя и важным уточнением, с которым трудно сразу соотнести какой-то содержательный смысл. Роль такого уточнения выясняется в ходе доказательств. Разница же между M_U и M представляется весьма принципиальной и интуитивно оправданной: в первом случае подразумевается перебор унарных слов, а во втором — перебор двоичных слов (в каком-то, явно не оговоренном в формулировке принципа Маркова, порядке).

В доказательстве большинства приведенных результатов существенно используется обычное понятие реализуемости по Клини, приспособленное к безэкспоненциальным теориям. Чтобы вскрыть все пружины, нам приходится довольно детально излагать эту хорошо известную теорию (следуя в основном [17, 18]). Слишком много мест, где требуются те или иные уточнения, чтобы можно было ограничиться общей ссылкой. Это связано с рядом тонких различий, которые смазываются при традиционном взгляде на экспоненту, как на осуществимую арифметическую операцию. Например, здесь можно вполне математически строго говорить о таких, казалось, неформализуемых понятиях, как *длинные* и *короткие*, *конструктивные* и *неконструктивные* конечные двоичные слова. (См. § 4 и добавление 1 о связи с понятием колмогоровской сложности.)

Заметим, что далеко не для каждой безэкспоненциальной теории (основанной на HT_0 или T_0) получается, как в утверждении 5, результат о невыводимости в ней нижней экспоненциальной оценки времени работы алгоритмов поиска (ср. [21]), хотя безэкспоненциальность играет здесь существенную роль (см. также обсуждение в [2] результатов о независимости для проблемы «$P = NP$?».) Примером могут служить теории T (см. в [3, с. 490] исправления к [2]), $T_0 + \Delta$-Coll (см. 2.3, 2.4 и 4.7, а также [2]), $HT_0 + ECT + M +$ ограниченная индукция (см. добавление 3). Наконец, ни для одной из рассмотренных теорий не удается доказать более сильный результат о невыводимости нижней экспоненциальной оценки для детерминированных алгоритмов распознающих какое-нибудь NP-полное множество.

Таким образом, при переходе к слабым, безэкспоненциальным теориям задача установления независимости проблем, близких к «$P = NP$?», несколько облегчается, но весьма незначительно, т. е. содержательный смысл таких проблем остается в контексте рассматриваемых теорий практически тем же. Может, однако, показаться, что если эти проблемы все же разрешимы (в ZF?), то такое ослабление математики до безэкспоненциальной уводит нас от цели, так как разрешимость при этом может потеряться. Но, рассуждая таким образом против ослабления традиционных аксиом математики, можно дойти до того, что для решения подобных проблем теории сложности на всякий случай постулировать как можно более сильные принципы: о существовании больших кардиналов, континуум-гипотезу (а может, ее отрицание?), аксиому детерминированности и т. п. Скорее всего, в рассматриваемом случае эти аксиомы, как и аксиома об осуществимости экспоненты, не имеют отношения к делу. Поэтому мы предпочитаем без особой необходимости их не вводить. Заметим также, что ослабление теории приводит к обогащению класса ее интерпретаций и осмысленных в ней понятий.

Мы видим, что предлагаемый безэкспоненциальный подход основан на (аксиоматическом) пересмотре таких исходных математических понятий, как натуральные числа и конечные двоичные слова. Его можно охарактеризовать также как взгляд на теорию сложности сквозь призму оснований математики. В связи с этим кажется полезной следующая аналогия между проблемой «P = NP?» и проблемой континуума: в первом случае рассматриваются конечные двоичные слова (и ограниченные кванторы по ним), а во втором — бесконечные, при этом, оказывается, в обоих случаях важную роль играет понятие конструктивного двоичного слова. Как и для континуума бесконечных двоичных слов, мы можем поставить, например, следующие весьма неформальные вопросы. В какой степени определенным является практически бесконечное множество «всех» двоичных слов длины, скажем, тысяча? Можно ли, например, мыслить произвольный элемент этого множества как результат случайного подбрасывания монетки? Как оформить все это математически? Напомним, что решение континуум-проблемы, данное К. Гёделем и П. Коэном, состояло прежде всего в поиске разумного ответа на такие вопросы в бесконечном случае. Не исключено, что подобное осознание сложности структуры конечных объектов в терминах оснований математики (а не только теории алгоритмов) может привести нас к некоторому решению и самой проблемы «P = NP?» и других трудных проблем теории сложности.

§ 2. ТЕОРИЯ ПОЛИНОМИАЛЬНОЙ ВЫЧИСЛИМОСТИ И ЧАСТИЧНО РЕКУРСИВНЫЕ ФУНКЦИИ

Обозначим через $\{0, 1\}^*$ множество конечных двоичных слов. Унарные слова $\{1\}^* \subseteq \{0, 1\}^*$ будем отождествлять с натуральными числами. Пусть $p_1, p_2, \ldots$ — все функции и предикаты на $\{0, 1\}^*$, вычислимые (на детерминированной машине Тьюринга) за время, полиномиальное от длины входа. Перечислим некоторые из них:

$x = y$ — равенство двоичных слов,

$\varnothing$ — пустое слово (нульместная функция),

$\sigma_0(x)$, $\sigma_1(x)$ — операции приписывания к слову нуля и единицы,

$\mathrm{Un}(x)$ — «x унарное слово»,

$|x|$, $|x|^2$ — длина и квадрат длины слова x (таким образом имеет место $\mathrm{Un}(|x|)$ и $\mathrm{Un}(|x|^2)$),

xy (или $x + y$) — конкатенация, т. е. результат приписывания друг к другу слов x и y,

$x^{|y|}$ — слово x, повторенное $|y|$ раз,

x', $x \leqslant y$ — лексикографические следование и порядок ($\varnothing < 0 < 1 < 00 < 01 < 10 < 11 < \ldots$),

$B(i) = B_i$ — i-е двоичное слово в лексикографическом упорядочении,

$\widehat{x}$ — результат замены каждого вхождения символа $\delta \in \{0, 1\}$ в слове x на $\delta\delta$,

$\langle x, y\rangle \rightleftharpoons \widehat{x}01y$ и $\langle\langle i, j\rangle\rangle \rightleftharpoons B^{-1}(\langle B_i, B_j\rangle)$ — двоичная и унарная кодировки пар двоичных и унарных слов соответственно (имеющие полиномиально вычислимые проекции),

$\exp(x, y)$ — предикат $2^{|x|} < |y|$,

$x[y]$ — утверждение об истинности «пропозициональной формулы» (закодированной словом) x на «входе» y,

$H(e, n)$ — «алгоритм, точнее, *инициальная машина Тьюринга* e завершает работу за $\leqslant |n|$ шагов». (Здесь e рассматривается как пара $e = \langle u, v\rangle$, где u — двоичный код обычной машины Тьюринга, а v — записанное на ее входной ленте двоичное слово),

$M(e, n)$ — результат работы алгоритма e (т. е. содержимое выходной ленты) на $|n|$-м шаге (считается, что на выходной ленте машины Тьюринга всегда содержится некоторое слово в алфавите $\{0, 1\}$),

$e * x$ — алгоритм e вместе с добавочной входной информацией x (формально для $e = \langle u, v\rangle$ полагаем $\langle u, v\rangle * x \rightleftharpoons \langle u, \langle v, x\rangle\rangle$).

Заметим, что любая ПВФ $f(x)$ термально выразима только через операции $\varnothing$, σ_0, σ_1 $|\cdot|^2$, M и $*$, а именно, в виде $f(x) = M(e * x, |x|^k + c)$, где термы e и c построены из $\varnothing$, σ_0 и σ_1, а k-я степень $|x|^k$ — из x и $|\cdot|^2$ (для k вида 2^m).

Пусть $\mathscr{P}$ — модель $\langle\{0, 1\}^*; p_1, p_2, \ldots\rangle$ сигнатуры $p_1, p_2, \ldots$, а T_0 — множество всех истинных в $\mathscr{P}$ бескванторных формул этой сигнатуры. Аналогично T — множество всех истинных в $\mathscr{P}$ формул (возможно, содержащих свободные переменные) с ограниченными кванторами $\forall x < t$, $\exists x < t$, где (сигнатурный) терм t не содержит переменную x.

Конечно, вместо (классических) теорий T_0 и T более естественно было бы рассмотреть некоторые их подтеории, заданные конечным числом схем аксиом с участием конечного числа символов для полиномиально вычислимых функций и предикатов p_k. Но для изложения дальнейшего материала это не имеет большого значения. Через HT_0 обозначим интуиционистский вариант теории T_0, т. е. указанные выше нелогические аксиомы T_0 + интуиционистская логика (с равенством). В отличие от интуиционистской арифметики HA, теория HT_0 не содержит (явно) аксиому (лексикографической) индукции

$$\varphi(\varnothing) \wedge \forall x < y\,(\varphi(x) \supset \varphi(x')) \supset \varphi(y).$$

Нас здесь интересуют лишь довольно слабые версии аксиомы индукции, а именно, *бескванторная индукция*, когда φ не содержит кванторов, и *ограниченная индукция*, когда φ содержит только ограниченные кванторы $\forall x < t$, $\exists x < t$, где x не входит в терм t. Очевидно, ограниченная индукция, как схема аксиом, просто содержится в теории T. Аналогично для HT_0 имеет место

Предложение 2.1 (ср. [2; 3, с. 490]). (а) *В теории* HT_0 *выводима бескванторная лексикографическая индукция.*

(б) *Аксиомы бескванторной и ограниченной лексикографической индукции эквивалентны в подходящем конечном фрагменте теории* HT_0 *соответственно бескванторной и ограниченной аксиомам линейной индукции*:

$$\varphi(\varnothing) \wedge \forall x\,(\varphi(|x|) \supset \varphi(|\sigma_1(x)|)) \supset \forall x\,\varphi(|x|),$$

где φ *— соответственно бескванторная или ограниченная формула.*

Доказательство. (а) Используя полиномиальную вычислимость предиката $\varphi(x)$, можно вычислить методом дихотомии за полиномиальное время значение $x = f(y) < y$ такое, что в модели $\mathscr{P}$ истинна формула

$$[\varphi(\varnothing) \wedge \neg\varphi(y) \supset \varphi(f(y)) \wedge \neg\varphi((f(y))')] \wedge [f(y) < y].$$

Из этой бескванторной формулы и из бескванторной формулы $\neg\neg\varphi(y) \supset \supset \varphi(y)$, являющихся аксиомами теории HT_0, следует аксиома индукции по формуле φ.

Доказательство (б) см. в § 8, п. 2. □

Укажем также другой (эквивалентный) вариант линейной индукции:

$$\varphi(\varnothing) \wedge \forall x\,(\varphi(x) \supset \varphi(x0) \wedge \varphi(x1)) \supset \forall x\,\varphi(x).$$

Открытые вопросы. 1. *Выводима ли в* T_0 *ограниченная индукция*? Заметим, что из отрицательного ответа на этот вопрос (который кажется более правдоподобным) следовало бы, что $P \neq NP$.

2. *Выводим ли в* T_0 *принцип лексикографически наименьшего слова для бескванторных* φ:

$$\varphi(x) \supset \exists y \leqslant x\,(\varphi(y) \wedge \forall z < y\ \neg\varphi(z))?$$

Ответ на этот вопрос, по-видимому, также отрицательный.

Наконец, заметим, что класс бескванторных формул φ замкнут относительно навешивания ограниченных унарных кванторов в том смысле, что, например, формула вида $\exists x \leqslant t\,(\mathrm{Un}(x) \wedge \varphi(x))$, где φ бескванторная

ная, эквивалентна в HT_0 бескванторной формуле $\varphi(\mu x \leqslant t(\mathrm{Un}(x) \wedge \wedge \varphi(x)))$, где $\mu x \leqslant t(\mathrm{Un}(x) \wedge \varphi(x))$ обозначает ПВФ, задающую наименьшее унарное слово x, удовлетворяющее условию $x \leqslant t \wedge \varphi(x)$, если такое x существует, и наибольшее унарное $x \leqslant t$ в противном случае.

Следующие два предложения демонстрируют адекватность теорий T_0 и T по отношению к полиномиальной вычислимости.

Предложение 2.2. *Если* $T_0 \vdash \exists y \varphi(\bar{x}, y)$ *для бескванторной формулы* φ, *то* $HT_0 \vdash \varphi(\bar{x}, t(\bar{x}))$ *для некоторого сигнатурного (и значит полиномиально вычислимого) терма* t. *В частности, в теориях* T_0 *и* HT_0 *выводимы одни и те же* Σ_1*-формулы* (Π_2*-предложения*), *и доказуемо-тотальные* ЧРФ *суть* ПВФ.

Доказательство. По теореме Эрбрана имеем $T_0 \vdash \bigvee_{i=1}^{k} \varphi(\bar{x}, t_i(\bar{x}))$, а значит, и $T_0 \vdash \varphi(\bar{x}, t(\bar{x}))$ для некоторых термов $t_1, \ldots, t_k, t$. В силу выводимости в T_0 закона исключенного третьего для бескванторных формул, последний вывод можно преобразовать в интуиционистский. (Еще проще: выводимая в T_0 бескванторная формула $\varphi(\bar{x}, t(\bar{x}))$ истинна в $\mathscr{P}$ и, значит, является даже аксиомой HT_0.) □

Предложение 2.3 [2, с. 573]. *Если формула* $\exists y \varphi(\bar{x}, y)$ *выводима в теории* T, *возможно, с использованием принципа*

$$\Delta\text{-Coll: } \forall x < a \exists y \psi \supset \exists b \forall x < a \exists y < b \psi,$$

где φ *и* ψ *содержат только ограниченные кванторы, то в теории* T (*без* Δ-Coll) *выводимо* $\exists y < t(\bar{x}) \varphi(\bar{x}, y)$ *для некоторого сигнатурного терма* t.

Доказательство для более общего случая приведено в [22]. □

Аналогичный результат, но без Δ-Coll был получен в [23].

Обозначим через EXP предложение $\forall x \exists y \exp(x, y)$, выражающее осуществимость экспоненты. Заметим, что EXP эквивалентно в HT_0 утверждению об осуществимости стандартного кодирования всех двоичных слов унарными: $\forall x \exists i \in \mathrm{Un}(x = B_i)$. В силу приведенного ниже следствия 2.4 предложения 2.3 и то и другое оказывается в наших теориях неосуществимым (ср. с предложением 4.7).

Следствие 2.4. *В теории* $T + \Delta$-Coll *не выводимы утверждения* EXP *и* $\forall x \exists i (x = B_i)$. □

Это следствие ни в коей мере не свидетельствует об ущербности теорий T_0 и T, хотя к такому выводу можно было бы прийти, если считать, что в них доказуемы не все «истины» вроде EXP. Во-первых, далеко не ясно, что собственно такое есть математические «истины». А во-вторых, предложение EXP представляется нам здесь, скорее, «ложным». Однако мы не будем здесь постулировать $\neg$EXP в качестве новой аксиомы.

В силу следствия 2.4 двоичные слова x вида B_i, т. е. такие x, что $\exists y \exp(x, y)$, естественно называть *короткими* (в рамках теории T_0 или HT_0, T и т. п., но не в модели $\mathscr{P}$, где истинно EXP и, значит, $\forall x \exists i (x = B_i)$). Причем непротиворечиво считать, что это не все возможные слова. Очевидно, если слова x и y короткие, то их конкатенация xy — также короткое слово, но $|x|^2$ уже может быть и не коротким.

Натуральные числа, имеющие короткое унарное представление, естественно называть также *малыми* или *достижимыми*. (Первая математически строгая, достаточно удовлетворительная формализация понятия достижимого натурального числа была предложена в [23].) В теории HT_0 доказуемо, что значением сигнатурного терма без переменных является короткое слово. Для T_0 в этом можно убедиться, например, рассмотрев произвольную, вообще говоря, «нестандартную» модель теории T_0, поскольку в ней «стандартные» слова и числа, являющиеся значениями таких термов, заведомо будут короткими. Теорема о полноте логики предикатов дает тогда требуемый результат.

Говоря о стандартных и нестандартных натуральных числах, мы употребили кавычки потому, что эти понятия имеют точный смысл только по отношению к некоторому воображаемому универсуму множеств, из которого берутся модели для арифметики Пеано и других формальных теорий. Теорема Гёделя о принципиальной неполноте аксиом арифметики, другие известные результаты в основаниях математики и теории множеств, а также рассмотрение безэкспоненциального или даже конечного натурального ряда приводят к более последовательной точке зрения, что всякий натуральный ряд нестандартен.

К сожалению, так же как и в [23], наше формальное определение коротких двоичных слов не вполне отражает интуитивное содержание этого понятия. Например, постоянный сигнатурный числовой терм $(\ldots(2^2)^2\ldots)^2$, полученный, скажем, десятикратным повторением возведения в квадрат, задает практически недостижимое число $2^{2^{10}}$, которое тем не менее здесь приходится признать достижимым в смысле нашего формального определения.

Строго говоря, мы должны были бы также строить доказательства в рассматриваемых теориях только практически достижимой длины. Разумеется, это потребовало бы пересмотра нашего изложения. Во всяком случае, доказательство путем ссылки на теорему о полноте логики предикатов, как это было сделано выше, оказывается при этом неприемлемым.

Все эти неформальные соображения приведены здесь, поскольку они соответствуют существу данной работы. Однако для простоты и по техническим причинам в основном тексте мы полностью придерживаемся традиций во взглядах на синтаксис и семантику.

Заметим, что, несмотря на безэкспоненциальность, рассматриваемый натуральный ряд (состоящий из унарных слов) все же содержит экспоненту как вычислимую частичную функцию, которая определена (или $\neq\infty$) только для достижимых (малых) числовых значений аргумента, а сама при этом принимает, вообще говоря, недостижимые (большие) значения. Собственно в математике и в приложениях важна не всюдуопределенность экспоненты, а уравнения, которым она удовлетворяет, и математический аппарат, в котором она тем или иным образом участвует. В этой статье мы увидим, в какой мере неосуществимость экспоненты влияет на начала теории рекурсивных функций и теории реализуемости по Клини.

Введем следующие сокращения:

$$(\{e\} = y) \rightleftharpoons \exists n\,(M(e, n) = y \wedge H(e, n)),$$

$$!\{e\} \rightleftharpoons \exists n H(e, n) \quad (\leftrightarrow \exists y\,(\{e\} = y)),$$

$$\{e\}(x) \rightleftharpoons \{e * x\},\ \{e\}(\bar{x}) \rightleftharpoons \{e * \bar{x}\},\ \text{где}$$

$$e^*(x_1, \ldots, x_k) \rightleftharpoons (\ldots((e * x_1) * x_2) * \ldots * x_k),\ k \geqslant 1.$$

Очевидно, $\langle u, v\rangle * (x_1, \ldots, x_k) = \langle u, \langle v, x_1, \ldots, x_k\rangle\rangle$, где

$$\langle x_1, \ldots, x_k\rangle \rightleftharpoons \langle\langle x_1, \ldots, x_{k-1}\rangle, x_k\rangle,\ k = 3, 4, \ldots.$$

Дадим обычное индуктивное определение понятия частично рекурсивного терма (ЧРТ),

1) переменные являются ЧРТ,

2) если f — сигнатурная k-местная, $k \geqslant 0$, функция и $t, s_1, \ldots, s_k$ — ЧРТ, то $f(s_1, \ldots, s_k)$ и $\{t\}(s_1, \ldots, s_k)$ ЧРТ.

Для каждого ЧРТ r, как обычно, индуктивно определяется формула $(r = z)$, где z — не входящая в r переменная:

$$(\{t\}(\bar{s}) = z) \rightleftharpoons \exists u\bar{v}\,(t = u \wedge \bar{s} = \bar{v} \wedge \{u\}(\bar{v}) = z),$$

$$(f(\bar{s}) = z) \rightleftharpoons \exists \bar{v}\,(\bar{s} = \bar{v} \wedge f(\bar{v}) = z).$$

Далее, положим

$$!t \rightleftharpoons \exists z(t = z),$$
$$(t = s) \rightleftharpoons \exists z(t = z \wedge s = z),$$
$$p(\bar{s}) \rightleftharpoons \exists \bar{v}(\bar{s} = \bar{v} \wedge p(\bar{v})),$$
$$(t \simeq s) \rightleftharpoons \forall z(t = z \leftrightarrow s = z).$$

Очевидно, первые три из этих формул эквивалентны в HT_0 Σ_1-формулам.

Предложение 2.5. *По любому* ЧРТ t *и* (*возможно пустому*) *списку переменных* $\bar{x}$ *можно построить сигнатурный терм* $\Lambda\bar{x}.t$, *который не содержит* (*свободно*) *переменных* $\bar{x}$ *и такой, что* $\mathrm{HT}_0 \vdash \{\Lambda\bar{x}.t\}(\bar{x}) \simeq t$.

Обращаем внимание, что терм $\Lambda\bar{x}.t$ является сигнатурным термом, т. е. ПВФ от своих свободных переменных, а не только примитивно-рекурсивной, как это утверждается обычно (ср., например, с предложением 5.3 в [17]).

Предложение 2.5 основано на существовании (конкретного для каждого $k = 0, 1, 2, \ldots$) универсального алгоритма u_k, для которого имеет место

Предложение 2.6. $\mathrm{HT}_0 \vdash \{u_k\}(e, \bar{x}) \simeq \{e\}(\bar{x})$, $\bar{x} = x_1, \ldots, x_k$.

В качестве u_k можно взять (с точностью до небольших деталей) обычную универсальную машину Тьюринга. При этом надо убедиться в существовании полиномиальной оценки s_k на время моделирования, т. е. убедиться в истинности в $\mathscr{P}$ следующих предложений.

Предложение 2.7. $H(e * \bar{x}, n) \supset (H(u_k * (e, \bar{x}), s_k(e, \bar{x}, n)) \wedge M(e * \bar{x}, n) = M(u_k * (e, \bar{x}), s_k(e, \bar{x}, n)))$. □

Предложение 2.8. $H(u_k * (e, \bar{x}), n) \supset H(e * \bar{x}, n)$. □

В общем случае предложение 2.5 доказывается индукцией по построению терма t. Например, алгоритм $\Lambda\bar{x}.\{t_1\}(t_2)$ строится из алгоритмов $\Lambda\bar{x}.t_1$, $\Lambda\bar{x}.t_2$ и универсального алгоритма u_1. □

Мы можем (пере)определить алгоритм $\Lambda\bar{x}.t$ так, чтобы он, удовлетворяя предложению 2.5, был еще и *коротким относительно свободных двоичных аргументов терма* $\Lambda\bar{x}.t$. Это означает, что если $\bar{i}$, $\bar{y}$ — список всех переменных терма t, отличных от переменных $\bar{x}$, то для некоторой ПВФ $r(\bar{i})$ дополнительно выполняется (в $\mathscr{P}$)

Условие 2.9. $\mathrm{Un}(\bar{i}) \supset \Lambda\bar{x} \cdot t = B_{r(\bar{i})} * \bar{y}$.

Действительно, $\{\Lambda\bar{x}.t\}(\bar{x}) \simeq \{\Lambda\bar{y}\bar{x}.t\}(\bar{y}, \bar{x}) \simeq \{(\Lambda\bar{y}\bar{x}.t) * \bar{y}\}(\bar{x})$ и, поскольку $\Lambda\bar{y}\bar{x}.t$ — ПВФ, зависящая только от унарных аргументов $\bar{i}$, можно воспользоваться следующим предложением (при $p(\bar{i}) \rightleftharpoons \Lambda\bar{y}\bar{x}.t$ и $\bar{z} = \bar{y}\bar{x}$).

Предложение 2.10. *Для любых* ПВФ $p(i)$ *от унарного аргумента* i *и для* $k = 0, 1, 2, \ldots$ *существуют* ПВФ $r_k(i)$ *и* $s_k(i, \bar{z}, n)$, *где* $\bar{z} = z_1, \ldots, z_k$ *такие, что*

(а) $\mathrm{HT}_0 \vdash \{p(i)\}(\bar{z}) \simeq \{B_{r(i)}\}(\bar{z})\ (\simeq \{B_{r(i)} * \bar{y}\}(\bar{x}))$,

(б) $\mathscr{P} \vDash H(p(i) * \bar{z}, n) \supset H(B_{r(i)} * \bar{z}, s(i, \bar{z}, n))$,

(в) $\mathscr{P} \vDash M(p(i) * \bar{z}, n) = M(B_{r(i)} * \bar{z}, s(i, \bar{z}, n))$.

Доказательство. Пусть π_k — программа обычной неинициальной машины Тьюринга, которая вход $\langle v, z_1, \ldots, z_k\rangle$ сначала перерабатывает в $\langle p(B^{-1}(v)), z_1, \ldots, z_k\rangle$, а затем применяет к результату, если он определен, универсальную программу u_k. В силу 2.6 получаем, что (при $v = B_i$) результатом работы алгоритма $\langle \pi_k, B_i\rangle$ на входе $\bar{z}$ будет $\{p(i)\}(\bar{z})$. Поэтому положим $r_k(i) \rightleftharpoons B^{-1}\langle \pi_k, B_i\rangle$. Полиномиальная вычислимость такой функции $r_k(i)$ следует из предложения 2.2, так как $\langle \pi_k, B_i\rangle$ является коротким словом и, значит, в HT_0 доказывается всюдуопределенность функции $r_k(i)$. Наконец, требуемая оценка s_k получается также по предложению 2.2. □

Заметим, что в доказательстве существенно использована инициальность машин Тьюринга. Действительно, здесь важна линейность длины инициальной программы $\langle \pi_k, B_i\rangle = \pi_k 01 B_i$ относительно $|B_i|$, благодаря которой $\langle \pi_k, B_i\rangle$ является коротким словом при любом i. В случае обыч-

ных машин Тьюринга нам пришлось бы рассматривать вместо программы $\langle \pi_k, B_i\rangle$ неинициальную программу $\widetilde{\pi}_k(B_i)$, получающуюся из π_k путем введения в нее добавочных команд, выписывающих на рабочую ленту слово B_i. Но такие команды заняли бы нелинейную (а именно, квадратичную) относительно $|B_i|$ часть программы $\widetilde{\pi}_k(B_i)$, и поэтому мы не могли бы гарантировать полиномиальную вычислимость и даже всюдуопределенность требуемой функции $r_k(i)$ такой, что $\widetilde{\pi}_k(B_i) = B_{r_k(i)}$.

Предложение 2.11 (об унарном μ-операторе). *По любой бесквантор-ной формуле* $\varphi(x)$ *можно построить* ЧРТ s, *содержащий те же переменные, что и* φ, *кроме* x, *такой, что*

$$\mathrm{HT}_0 \vdash s = x \leftrightarrow \mathrm{Un}(x) \wedge \varphi(x) \wedge \forall y \in \mathrm{Un}(y < x \supset \neg\, \varphi(y)). \quad \square$$

Такой терм s будем обозначать $\mu x \in \mathrm{Un}.\varphi(x)$.

Предложение 1.11 можно распространить и на случай частично рекурсивных предикатов в роли φ, если добавить к HT_0 унарный принцип коллекции для бесквантор-ных α:

$$\forall i < n \exists j \alpha \supset \exists m \forall i < n \exists j < m \alpha,$$

где i, j, n, m пробегают унарные слова. Действительно, в этом случае мы можем гарантировать существование верхней границы m, а значит, и требуемую конечность суммарного времени $\leqslant n \cdot m$ вычисления значений $\varphi(\varnothing)$, $\varphi(1)$, $\varphi(11)$, ... вплоть до любого значения n унарного аргумента, до которого все предшествующие значения определены.

Заметим, что мы не можем гарантировать в HT_0 частичную рекурсивность общего (не «унарного») μ-оператора $\mu x.\varphi(x)$, так как его (прямое) определение, очевидно, связано с экспоненциальным перебором двоичных слов. Точнее, ввиду неосуществимости экспоненты прямое определение $\mu x.\varphi(x)$ через перебор $B_\varnothing$, B_1, B_{11}, ... оказывается некорректным. Так, естественное утверждение $y = \mu x(x = y)$ при этом оказалось бы эквивалентным утверждению $\exists i(B_i = y)$, равносильному осуществимости экспоненты.

Докажем предложение о представлении доказуемо-тотальных Σ_1-функций, усиливающее 2.2.

Предложение 2.12. *Предположим, что для новой константы* e, *некоторых бесквантор-ных формул* $\alpha(e, x, y)$, $\beta(e, x, y)$, *и* ЧРТ $f(e, x) = f_e(x)$, *зависящих только от указанных переменных, в теории* $\mathrm{T}_0 + \mathrm{Ax}(e)$, где $\mathrm{Ax}(e)$ — *некоторые бесквантор-ные аксиомы относительно* e, (*классически*) *выводимы формулы*

$$\exists y \alpha(e, x, y) \supset !f_e(x),\ f_e(x) = y \supset \alpha(e, x, y),\ \forall x !f_e(x) \supset \forall x \exists y \beta(e, x, y).$$

Тогда для некоторой суперпозиции $t_e(x)$ *сигнатурных функций,* ЧРФ f_e *и константы* e *существует* (*интуиционистский*) *вывод*

$$\mathrm{HT}_0 + \mathrm{Ax}(e) + \forall x !f_e(x) \vdash \forall x \beta(e, x, t_e(x)).$$

Доказательство (набросок). В рамках рассматриваемой интуиционистской теории $\mathrm{HT}_0 + \mathrm{Ax}(e) + \forall x !f_e(x)$ мы можем использовать f_e, как если бы это был новый сигнатурный функциональный символ, который (по условию предложения и благодаря тому, что $f_e(x) = y$ есть Σ_1-формула) интуиционистски удовлетворяет предложению $\forall x \alpha(e, x, f_e(x))$. По условию в теории $\mathrm{T}_0 + \mathrm{Ax}(e) + \forall x \alpha(e, x, f_e(x))$ (где f_e — функциональный символ) выводимо $\forall x !f_e x$ (здесь f_e уже не функциональный символ) и, значит, классически выводимо $\forall x \exists y \beta(e, x, y)$. Как и в предложении 2.2, используя теорему Эрбрана, получаем интуиционистский вывод в теории $\mathrm{HT}_0 + \mathrm{Ax}(e) + \forall x \alpha(e, x, f_e(x))$, а значит, и в теории $\mathrm{HT}_0 + \mathrm{Ax}(e) + \forall x !f_e(x)$ предложения $\forall x \beta(e, x, t_e(x))$ для некоторой суперпозиции $t_e(x)$ требуемого вида. $\square$

§ 3. ФОРМАЛЬНЫЙ ТЕЗИС КЛИНИ — ЧЕРЧА И ПРИНЦИП МАРКОВА В РАМКАХ ТЕОРИИ ПОЛИНОМИАЛЬНОЙ ВЫЧИСЛИМОСТИ

Как и к интуиционистской арифметике HA, к рассматриваемой теории HT_0 можно добавить следующие варианты формального тезиса Клини — Черча (см. [17, 18]):

$$CT(\varphi):\ \forall x \exists y \varphi(x, y) \supset \exists e \forall x \exists y (\{e\}(x) = y \wedge \varphi(x, y)),$$

$$CT(\chi, \varphi):\ \forall x (\chi(x) \supset \exists y \varphi(x, y)) \supset \exists e \forall x (\chi(x) \supset \exists y (\{e\}(x) = y \wedge \varphi(x, y))),$$

где во избежание противоречия с HT_0 (так же как и в случае HA [17, с. 51]) мы наложим некоторые ограничения на χ.

Формула χ называется *негативной* (соответственно *харроповой*), если она не содержит кванторов существования (соответственно если все ее кванторы существования находятся внутри посылок импликаций)*). Формула χ называется *почти негативной* (соответственно *U-негативной*), если она содержит кванторы существования только вида $\exists \bar{x} \alpha(\bar{x})$ (соответственно вида $\exists \bar{x} \in \mathrm{Un}\, \alpha(\bar{x})$), где α — бескванторная подформула. Если в формуле χ все кванторы существования не такого вида находятся внутри посылок импликаций, то χ называется *почти харроповой* (соответственно *U-харроповой*). Положим

$ECT(\overline{ECT})$ — все примеры $CT(\chi, \varphi)$ с почти негативной (соответственно почти харроповой) формулой χ,

$ECT_U(\overline{ECT_U})$ — все примеры $ECT(\overline{ECT})$ с U-негативной (соответственно U-харроповой) формулой χ.

Позже в следствии 6.9 будет показано, что схема ECT (ECT_U) равносильна формально более общей схеме $\overline{ECT}$ ($\overline{ECT_U}$).

Сформулируем также два варианта принципа Маркова:

$$M:\ \neg\neg \exists x \alpha(x, \bar{z}) \supset \exists x \alpha(x, \bar{z}),$$

$$M_U:\ \neg\neg \exists x \in \mathrm{Un}\, \alpha(x, \bar{z}) \supset \exists x \in \mathrm{Un}\, \alpha(x, \bar{z}),$$

где α — бескванторная формула.

Позже мы установим конструктивность (см. § 1 и следствия 6.5 (б), 7.4 (б)) принципов ECT_U и M_U относительно теории HT_0. Что касается традиционных их вариантов ECT и M, то мы убедимся в их тесной связи с проблемой «P = NP?». Так, эти принципы влекут существование алгоритма для нахождения по произвольной выполнимой пропозициональной формуле выполняющих ее значений переменных (см. 3.1, 3.2, 6.10, 7.5, 7.6).

Двоичное слово e назовем *алгоритмом поиска*, если для него выполняется следующая формула:

$$SA(e) \rightleftharpoons \forall x (\exists y.x[y] \supset \exists y (\{e\}(x) = y \wedge x[y]))$$

или эквивалентная $\forall\exists$-формула

$$\forall x y \exists n \in \mathrm{Un}\, (x[y] \supset H(e * x, n) \wedge x[M(e * x, n)]).$$

Напомним, что $x[y]$ обозначает значение истинности булевой формулы x на кортеже y. Следующие две формулы утверждают существование алгоритма поиска и соответственно короткого алгоритма поиска:

$$SA \rightleftharpoons \exists e.SA(e),$$

$$DSA \rightleftharpoons \exists i \in \mathrm{Un}.SA(B_i).$$

Предложение 3.1. (а) $HT_0 + ECT \vdash SA$,

(б) $HT_0 + ECT_U + M \vdash ECT \wedge SA$.

---

*) В этом определении мы считаем, что предварительно в χ отрицание выражено через импликацию, а дизъюнкция — через квантор существования.

В следствии 5.3 (в) будет установлено также, что $HT_0 + ECT + M_U \vdash M$.

Доказательство. (а) Существование требуемого алгоритма поиска вытекает из следующего примера ECT:

$$\forall x(\exists y.x[y] \supset \exists y.x[y]) \supset \exists e \forall x(\exists y.x[y] \supset x[\{e\}(x)]),$$

поскольку его посылка является логической аксиомой $\varphi \supset \varphi$.

(б) $ECT = CT(\chi, \varphi)$ сводится к ECT_U заменой, в силу M, кванторов $\exists$ в χ на $\neg\neg\exists$, а затем на $\neg\forall\neg$. Остается применить (а). □

Следствие 3.2. *Пусть теория S в языке T_0 имеет те же Π_2-теоремы, что и T_0. Тогда, если S конструктивна и имеет вид $HT_0 + M + \ldots$ или же S $\exists$-конструктивна и имеет вид $HT_0 + SA + \ldots$ или $HT_0 + ECT + \ldots$, то $P = NP$.*

Как мы увидим ниже (см. 6.7), теория S имеет те же Π_2-теоремы, что и T_0, если $HT_0 \subseteq S \subseteq HT_0 + ECT + M$.

Доказательство. Достаточно для некоторого конкретного двоичного слова e_0 установить выводимость Π_2-предложения $SA(e_0)$ в исчислении S, а значит, и в T_0, поскольку в силу 2.2 отсюда следует существование (в $\mathscr{P}$) полиномиального алгоритма поиска e_0 или, эквивалентно, равенство $P = NP$.

В случае $S = HT_0 + M + \ldots$ по принципу Маркова выводится $\neg\forall y\neg x[y] \subset \exists y.x[y]$, откуда по конструктивности S вытекает выводимость $\neg\forall y\neg x[y] \supset x[\{e_0\}(x)]$ для некоторого конкретного e_0 и, следовательно, выводимость $SA(e_0)$.

В случае $S = HT_0 + SA + \ldots$ или $= HT_0 + ECT + \ldots$ выводимость $SA(e_0)$ следует из предложения 3.1 (а) и $\exists$-конструктивности S. □

Предложение 3.3. *Из $P = NP$ следует эквивалентность в HT_0 принципов M и M_U, а также принципов ECT и ECT_U.*

Доказательство. Если α бескванторная формула, то

$$\exists x\alpha(x, \bar{z}) \leftrightarrow \exists n \in \mathrm{Un}\, \exists x < n\ \alpha(x, \bar{z}) \leftrightarrow \exists n \in \mathrm{Un}\, \alpha_0(n, \bar{z})$$

для некоторого полиномиально вычислимого предиката α_0, существующего в силу $P = NP$. Тем самым M и ECT сводятся к своих частным случаям M_U и ECT_U. □

В следствиях 7.4 (б) и 6.5 (б) будет установлена конструктивность теорий HT_0, $HT_0 + M_U$, $HT_0 + ECT_U$ и $HT_0 + ECT_U + M_U$. Поэтому из 3.2, 3.3 вытекает, что каждая из теорий $HT_0 + M$, $HT_0 + ECT$, $HT_0 + ECT + M_U$ и $(=)HT_0 + ECT_U + M = HT_0 + ECT + M$ является конструктивной тогда и только тогда, когда $P = NP$. Более того, равенство $P = NP$ равносильно доказуемости в любой из этих теорий Π_2-предложения $SA(e_0)$ для какого-нибудь конкретного алгоритма поиска e_0 (см. начало доказательства следствия 3.2). Заметим, что этот результат находится в кажущемся противоречии с тем фактом, что ниже (после теоремы 5.2) построен вполне определенный «алгоритм поиска» ε, являющийся в $\mathscr{P}$ даже оптимальным среди всех алгоритмов поиска. Дело в том, что его оптимальность и само предложение $SA(\varepsilon)$ удается доказать лишь в теории $HT_0 + EXP$ или $HT_0 + DET$ (аксиома DET определена в § 4).

В § 5 мы увидим, что алгоритмы поиска имеют более широкое значение, чем это следует непосредственно из определения, и что им можно придать канонический вид. Этим мы воспользуемся для установления основных результатов. Но сначала надо рассмотреть вопрос о кодировании двоичных слов унарными.

§ 4. ПОЛИНОМИАЛЬНО ОПТИМАЛЬНОЕ КОДИРОВАНИЕ КОНЕЧНЫХ ДВОИЧНЫХ СЛОЕВ УНАРНЫМИ

Как уже отмечалось, в теориях, в которых не доказуема осуществимость экспоненты, двоичные слова не могут быть занумерованы посредством обычного кодирования $x = B(i)$ ввиду экспоненциальной сложно-

сти и даже частичности обратной функции $i = B^{-1}(x)$ (если она всюду определена). Слова вида B_i являются в таких теориях очень короткими, и поэтому не могут претендовать даже на приближение ко множеству всех подразумеваемых в теории двоичных слов. Тем не менее возможно кодирование унарными словами довольно богатого запаса (как мы увидим, непротиворечиво даже считать, что всех) двоичных слов, которое является в определенном смысле безэкспоненциальным.

Так, вместо кодирования B_i можно взять кодирование $\{B_i\}$ (= результат работы алгоритма B_i, если он определен). Двоичные слова x вида $x = \{B_i\}$ назовем *конструктивными* или *простыми*. Неконструктивные слова (если такие есть) естественно называть также *случайными* или *сложными* (см. также добавление 1). Нетрудно показать в HT_0, что, например, унарные слова являются конструктивными.

В дальнейшем нас будут интересовать следующие

Аксиомы 4.1. $DET \rightleftharpoons \forall x \exists i (x = \{B_i\})$,

$DET^e \rightleftharpoons \forall x \exists i (x = \{B_i\}(e))$,

$RDET \rightleftharpoons \exists e\, DET^e$.

Эти аксиомы утверждают, что все конечные двоичные слова являются конструктивными или соответственно конструктивными *относительно* некоторого одного двоичного слова e. Аксиомы SA и DSA являются более слабыми формами аксиомы DET о конструктивности двоичных слов (см. § 5).

Недостатком кодирования $\{B_i\}$ является его частичность: алгоритм B_i может «зациклиться». Поэтому перейдем к соответствующему полиномиально вычислимому кодированию ξ_j того же класса конструктивных слов, определяемому с помощью унарной кодировки унарных пар $j = \langle\!\langle i, n \rangle\!\rangle$ (см. § 2).

Определение 4.2. $\xi_{\langle\!\langle i,n \rangle\!\rangle} \rightleftharpoons M(B_i, n)$.

Более общо, определим $\xi_j^{\bar{y}}$, где $\bar{y}$ — кортеж двоичных слов.

Определение 4.3. $\xi^{\bar{y}}_{\langle\!\langle i,n \rangle\!\rangle} \rightleftharpoons M(B_i * \bar{y}, n)$.

В терминах этого кодирования в HT_0 легко переформулировать аксиомы DET и DET^e, используя 2.9 (с пустым списком $\bar{x}$):

$$\xi_j^{\bar{y}} = \{B_{r(j)} * \bar{y}\} = \{B_{r(j)}\}(\bar{y}),$$

$$DET \leftrightarrow \forall x \exists j (x = \xi_j),$$

$$DET_e \leftrightarrow \forall x \exists j (x = \xi_j^e).$$

В [2] подобные эквивалентности были приняты по определению. Из следующей теоремы следует, в частности, конструктивность унарных и коротких двоичных слов. Класс конструктивных слов замкнут относительно ПВФ. Слова, конструктивные относительно конструктивного слова, также являются конструктивными и $DET \leftrightarrow DET^{\varnothing}$. Тем самым (относительно) конструктивные слова образуют определимую в T_0 интерпретацию бесквантворной теории T_0, чего, к сожалению, не удается доказать для теории T или T_0 + ограниченная индукция (см. в связи с этим [2] и особенно исправление к [2] в [3, с. 490]). В этой же интерпретации, очевидно, выполняется и аксиома DET (соответственно RDET).

Теорема 4.4. *Последовательность* $\xi_j^{\bar{x}}$, $j = \varnothing, 1, 11, 111, \ldots$ *является полиномиально оптимальной в том смысле, что в* HT_0 *выводимы (для унарных* $\bar{i}$*) соотношения*:

(а) $p(\bar{i}) = \xi_{r(\bar{i})}$,

(б) $p(\bar{i}, \bar{x}) = \xi^{\bar{x}}_{r(\bar{i},\bar{x})}$,

(в) $\{e\}(\bar{i}, \bar{x}) \simeq \xi^{e,\bar{x}}_{q(e,\bar{i},\bar{x},t(e,\bar{i},\bar{x}))}$,

где $t(e, \bar{i}, \bar{x}) \rightleftharpoons \mu z \in \mathrm{Un}\, H(e * (\bar{i}, \bar{x}), \bar{z})$, *а* p, q, r — *полиномиально вычислимые функции, причем* p — *произвольная,* r — *зависящая от* p, *а* q — *подходящая фиксированная.*

Таким образом, полиномиально оптимальная последовательность $\xi_j^{\bar{x}}$ задает «быстрейший», с точностью до полиномов, перебор двоичных слов. Она «догоняет» любую другую вычислимую (частичную) последовательность $\{e\}(i, \bar{x})$, $i = \varnothing$, 1, 11, 111, ..., если учитывается соответствующее время вычисления $t(e, i, \bar{x})$.

Доказательство. Из пункта (б), очевидно, следует его частный случай (а), а также (в):

$$\{e\}(\bar{i}, \bar{x}) \simeq M(e * (\bar{i}, \bar{x}), t(e, \bar{i}, \bar{x})) \overset{(б)}{\simeq} \xi^{e,\bar{x}}_{r(\bar{i}, t(e,\bar{i},\bar{x}), e, \bar{x})}.$$

Таким образом, надо доказать (б). Сначала установим (б) для последовательности $\tilde{\xi}_j^{\bar{x}}$, задаваемой, наподобие $\xi_j^{\bar{x}}$, равенством $\tilde{\xi}^{\bar{x}}_{\langle\langle n,i,t\rangle\rangle} \rightleftharpoons M(B_n * (i, \bar{x}), t)$. Пусть B_{n_0} — конкретная программа *) для вычисления $p(i, \bar{x})$ и $t_0(i, \bar{x})$ — (полиномиальное) время работы этой программы на входе i, $\bar{x}$. Тогда

$$p(i, \bar{x}) = M\left(B_{n_0} * (i, \bar{x}), t_0(i, \bar{x})\right) = \tilde{\xi}^{\bar{x}}_{\langle\langle n_0, i, t_0(i,\bar{x})\rangle\rangle} = \tilde{\xi}^{\bar{x}}_{r(i,\bar{x})}.$$

Тем самым последовательность $\tilde{\xi}_j^{\bar{x}}$ полиномиально оптимальна. Такова же и наша последовательность $\xi_j^{\bar{x}}$, поскольку (на основании 2.10 (в)) к ней полиномиально сводится последовательность $\tilde{\xi}_j^{\bar{x}}$:

$$\tilde{\xi}^{\bar{x}}_{\langle\langle n,i,t\rangle\rangle} = M((B_n * i) * \bar{x}), t) \overset{2.10(в)}{=} M(B_{v(n,i)} * \bar{x}, s(n, i, \bar{x}, t)) =$$

$$= \xi^{\bar{x}}_{\langle\langle v(n,i), s(n,i,\bar{x},t)\rangle\rangle}. \quad \square$$

Легко построить также разнозначную (от унарного аргумента n) полиномиально оптимальную последовательность $\zeta_n^{\bar{x}} \rightleftharpoons$ ЕСЛИ $\xi_n^{\bar{x}} \notin \{\zeta_m^{\bar{x}} \mid m < n\}$ ТО $\xi_n^{\bar{x}}$ ИНАЧЕ первое $B_j \notin \{\zeta_m^{\bar{x}} \mid m < n\}$. Очевидно, здесь $j \leqslant n$, и значит, для некоторой ПВФ $s(n, \bar{x}) \leqslant n$ в $\mathscr{P}$ имеет место равенство $\xi_n^{\bar{x}} = \zeta^{\bar{x}}_{s(n,\bar{x})}$, из которого следует полиномиальная оптимальность разнозначной последовательности $\zeta_n^{\bar{x}}$.

Предложение 4.5. $\mathrm{HT}_0 + \mathrm{EXP} \vdash \mathrm{DET}$, $\mathscr{P} \vdash \mathrm{DET}$ (т. е. осуществимость экспоненты влечет возможность оптимального кодирования всех двоичных слов посредством унарных).

Доказательство следует из эквивалентности $\mathrm{EXP} \leftrightarrow \forall x \exists i\ (x = B_i)$ и оптимальности ξ_i: $B_i = \xi_{r(i)}$. $\square$

Однако обратное утверждение неверно:

Теорема 4.6 [2]. *В теории* $\mathrm{T}_0 + \mathrm{DET}$ *недоказуемо EXP. В* $\mathrm{T}_0 + \mathrm{DET}$ *доказуемо-рекурсивные функции от унарного аргумента суть* ПВФ.

Доказательство. Обозначим через $\nu(x)$ ЧРФ $\mu i \in \mathrm{Un}(x = \xi_i)$, принимающую унарные значения и обратную к функции ξ_i. Таким образом, $x \simeq \xi_{\nu(x)}$ и $\nu(\xi_i) \leqslant i$. Заметим, что функция $\alpha(i) \rightleftharpoons \nu(\xi_i)$, очевидно, полиномиально вычислима. Благодаря DET функция ν всюду определена.

---

*) К сожалению, унарный номер n_0 слова B_{n_0} может оказаться, в отличие от самого B_{n_0}, практически недостижимым. Тем не менее с точки зрения традиционно принятого подхода к конечному, число n_0 является «стандартным» и в этом смысле также конкретным.

Из мощностных соображений легко следует, что она для некоторых аргументов растет экспоненциально, и потому невычислима за полиномиальное время. Тем не менее любая суперпозиция $t(n)$ сигнатурных функций и функции ν, зависящая только от одной унарной переменной n, задает ПВФ. Действительно, функцию ν можно элиминировать из $t(n)$ на основании полиномиальной оптимальности ξ: $\nu(p(n)) = \nu(\xi_{r(n)}) = \alpha(r(n))$, где $p(n)$ — произвольная ПВФ. Отсюда, как и в предложении 2.2 и следствии 2.4, используя теорему Эрбрана, получаем требуемый результат. □

В отличие от теоремы 4.6 и следствия 2.4 имеет место

Предложение 4.7 [2, с. 574]. $T_0 + \Delta\text{-Coll} + \text{RDET} \vdash \text{EXP}$.

Доказательство. $\Delta = \text{Coll}$ и DET^e дают

$$\forall n \exists m \forall x \leqslant n \exists j < m\,(x = \xi^e_j).$$

Но это приводит к EXP, поскольку в T_0 выводима (очевидно, истинная) импликация $\forall x \leqslant n \exists j < m\,(x = \xi^e_j) \supset m \geqslant 2^{n+1} - 1$. Действительно, ее контрапозиция следует из истинной в $\mathscr{P}$ бесквантворной формулы $m < 2^{n+1} - 1 \supset \forall j < m\,(X^e(m) \neq \xi^e_j) \wedge X^e(m) \leqslant n$, где $X^e(m) \rightleftharpoons B(\mu i \leqslant \leqslant m \forall j < m\,(B_j \neq \xi^e_j))$ — ПВФ от m и e. □

Открытый вопрос. *Верно ли, что* $T_0 +$ *ограниченная индукция* $+ \text{DET} \vdash \text{EXP}$? (См. в связи с этим исправление к [2] в [3, с. 490].)

Для более слабых, чем DET, аксиом RDET и DET^e (e — новая константа) можно усилить теорему 4.6 следующим образом.

Теорема 4.8. *Теории* $T_0 + \text{RDET}$ *и* $T_0 + \text{DET}^e$ *консервативно расширяют теорию* T_0 *относительно* Π_2*-формул, не содержащих константу* e.

Доказательство. Сначала заметим, что слова вида ξ^e_i, где i пробегает унарные слова (a e фиксировано), образуют интерпретацию в теории T_0 теории $T_0 + \text{DET}^e$ (ср. замечание перед теоремой 4.4). Поэтому если $T_0 + \text{DET}^e \vdash \forall x \exists y \alpha(e, x, y)$ для бесквантворной α, то $T_0 \vdash \forall i \exists j \alpha(e, \xi^e_i, \xi^e_j)$, где константа e уже выступает в роли переменной. Отсюда и из того, что любое слово x, очевидно, представимо в виде $x = \xi^x_i$ для некоторого i, получаем $T_0 \vdash \forall x \exists y \alpha(x, x, y)$. Тем самым, в частности, доказана требуемая консервативность относительно Π_2-формул $\forall x \exists y \alpha(x, y)$, не содержащих константы e. □

§ 5. ОБЩИЕ КАНОНИЧЕСКИЕ АЛГОРИТМЫ ПОИСКА

Вернемся к рассмотрению алгоритмов поиска. На основе полиномиально оптимального перебора $\xi^{(e)}_i$ двоичных слов, очевидно, можно построить (относительно) короткий алгоритм поиска, если выполняется соответствующая аксиома об (относительной) конструктивности всех двоичных слов. Таким образом, в HT_0 имеем импликации

$$\text{EXP} \to \text{DET} \nearrow \text{DSA} \searrow \text{SA}. \quad \text{DET} \searrow \text{RDET} \nearrow \text{SA}.$$

В частности, из импликации $\text{RDET} \to \text{SA}$ и теоремы 4.8 следует

Теорема 5.1. *Теория* $T_0 + \text{SA}(e)$ *консервативно расширяет теорию* T_0 *относительно* Π_2*-формул (без* e*).* □

Отсюда или же из теоремы 4.6 и импликации $\text{DET} \to \text{SA}$ следует невыводимость в T_0 нижней экспоненциальной оценки времени работы алгоритмов поиска (см. [2], а также точную формулировку о нижней оценке в следствии 6.8).

Кроме формулы $x[y]$, участвующей в определении алгоритма поиска, нас будут интересовать произвольные бесквантворные формулы $\alpha(x, y)$, выступающие в той же роли.

Теорема 5.2 (о канонических алгоритмах поиска). *Для любой бескванторной формулы* $\alpha(x, y)$ *в* HT_0 *выводимы следующие формулы*:

а) $\exists j\,\mathrm{SA}(\xi_j^e) \wedge \exists y\alpha(x, y) \supset \exists i\alpha(x, \xi_i^{e,x})$,

б) $\mathrm{DSA} \wedge \exists y\alpha(x, y) \supset \exists i\alpha(x, \xi_i^x)$,

в) $\mathrm{DET} \wedge \exists y\alpha(x, y) \supset \exists i\alpha(x, \xi_i)$.

Заметим, что согласно предложению 2.10 (а) $\mathrm{DSA} \leftrightarrow \exists j\,\mathrm{SA}(\xi_j)$.

Пункт (а) теоремы 5.2 означает, что по любому двоичному слову e, в котором содержится информация о некотором алгоритме поиска $e' = \xi_j^e$ для пропозициональных формул, можно легко построить (по существу единый) алгоритм поиска для всех бескванторных формул $\alpha(x, y)$, основанный на переборе $\xi_i^{e,x}$, $i = \varnothing$, 1, 11, 111, ..., а именно, алгоритм

$$\varepsilon_\alpha(e) \rightleftharpoons \Lambda x.\xi^{e,x}(\mu i \in \mathrm{Un}.\,\alpha(x, \xi_i^{e,x})).$$

Если эта исходная информация e была короткой, то, согласно (а) или (б), аналогичный алгоритм поиска ε (для $\alpha(x, y) \rightleftharpoons x[y]$), основанный на переборе ξ_i^x, вообще не зависит от e. При этом, очевидно, $\mathrm{DSA} \leftrightarrow \leftrightarrow \mathrm{SA}(\varepsilon)$. Более того, алгоритм ε является *полиномиально оптимальным* среди всех коротких алгоритмов поиска и даже среди всех алгоритмов поиска вида ξ_j в том смысле, что для любой выполнимой пропозициональной формулы x время вычисления $\{\varepsilon\}(x)$ может оказаться дольше времени вычисления $\{\xi_j\}(x)$ не более чем в полином раз, причем полином, естественно, зависит также от j. Это утверждение можно получить с помощью теоремы 4.4 (в) и (б) с $e = \xi_j$. Можно также сначала на основе полиномиальной оптимальности ξ и определения алгоритма ε вывести в HT_0 формулу

$$\forall xjn\exists m\,(x\,[M\,(\xi_j * x, n)] \wedge H\,(\xi_j * x, n) \supset x\,[M\,(\varepsilon * x, m)] \wedge H\,(\varepsilon * x, m)),$$

а затем воспользоваться предложением 2.2. Существование полиномиально оптимального алгоритма поиска (в «стандартном» универсуме конечных объектов) утверждалось в [24], однако без предъявления самого алгоритма и доказательства, а также без определения оптимального перебора двоичных слов, на котором основаны наши алгоритмы поиска (введенные в [2]). Понятно, что лексикографический перебор, как алгоритм поиска, крайне неэффективен.

Доказательство теоремы 5.2. Пункт (в) очевиден, (б) следует из (а) и полиномиальной оптимальности ξ. Доказательство (а), очевидно, сводится к случаю, когда квантор $\exists y$ ограничен, т. е. имеет вид $\exists y \leqslant n$, где n новая переменная. В силу хорошо известной полиномиальной сводимости задачи нахождения $y \leqslant n$ такого, что верно $\alpha(x, y)$ к задаче выполнения подходящей пропозициональной формулы (т. е. в силу NP-полноты проблемы выполнимости пропозициональных формул [4]) можно перестроить (за полиномиальное время) заданный алгоритм поиска $e' = \xi_i^e$, удовлетворяющий $\mathrm{SA}(e')$, в алгоритм поиска $s(e')$ для $\alpha(x, y)$:

$$\mathrm{HT}_0 \vdash \exists y \leqslant n\alpha(x, y) \supset \exists y\,(y = \{s(e')\}(x) \wedge y \leqslant n \wedge \alpha(x, y)).$$

Но согласно теореме 4.4 (в), (б) и равенству $e' = \xi_j^e$ имеем

$$y = \{s(e')\}(x) \overset{(\text{в})}{\simeq} \xi_{q(s(e'),x,t(s(e'),x))}^{s(e'),x} \overset{(\text{б})}{\simeq} \xi_{r(j,e,x,t_1(j,e,x))}^{e,x}.$$

Таким образом, y имеет вид $\xi_i^{e,x}$. Теорема доказана. □

Следствие 5.3. (а) $\mathrm{HT}_0 + \mathrm{SA} + \mathrm{ECT}_U \vdash \mathrm{ECT}$,

(б) $\mathrm{HT}_0 + \mathrm{SA} + \mathrm{M}_U \vdash \mathrm{M}$,

(в) $\mathrm{HT}_0 + \mathrm{ECT} + \mathrm{M}_U \vdash \mathrm{M}$.

Доказательство. В силу теоремы 5.2(а) и предложения 3.1(а) из SA и ECT следует эквивалентность любой формулы вида $\exists y\alpha(y, \bar{z})$

формуле $\exists i \in \mathrm{Un}\alpha(\xi_i^{e,z}, \bar{z})$ с унарным $\exists$, где α бескванторна, а e обозначает алгоритм поиска, существование которого утверждает SA. Используя этот прием, сводим ECT и M соответственно к ECT_U и M_U. □

Определим ЧРФ, «обратные» к введенным в теореме 5.2 каноническим алгоритмам поиска:

$\nu(x) \rightleftharpoons \mu i \in \mathrm{Un}(x = \xi_i)$ (см. доказательство теоремы 4.6),

$\nu^2(x, y) \rightleftharpoons \mu i \in \mathrm{Un}(x[y] \supset x[\xi_i^x])$,

$\nu^3(e, x, y) \rightleftharpoons \mu i \in \mathrm{Un}(x[y] \supset x[\xi_i^{e,x}])$.

Введем обозначение

$$\mathrm{SA}^e \rightleftharpoons \forall xy!\nu^3(e, x, y)(\leftrightarrow \forall xy(x[y] \supset \exists i.x[\xi_i^{e,x}])).$$

В силу теоремы 5.2 и полиномиальной оптимальности ξ справедливо

Предложение 5.4. *В* HT_0 *выводимы эквивалентности*

$$\mathrm{SA}^e \leftrightarrow \exists j\, \mathrm{SA}(\xi_j^e),$$

$$\forall xy!\nu^2(x, y) \leftrightarrow \mathrm{DSA},$$

$$\forall x!\nu(x) \leftrightarrow \mathrm{DET}. \ \square$$

Заметим, что если некоторый конкретный алгоритм поиска e_0 работает (в $\mathscr{P}$) полиномиальное время, т. е. если $\mathrm{P} = \mathrm{NP}$, то $\mathrm{T}_0 \vdash \mathrm{SA}(e_0) \wedge$ $\wedge$ DSA и, значит, по 5.4 $\mathrm{T}_0 \vdash \mathrm{SA}^{e_0} \wedge \forall xy!\nu^2(x, y)$ и по предложению 2.2 функции $\nu^3(e_0, x, y)$ и $\nu^2(x, y)$ оказываются полиномиально вычислимыми (в $\mathscr{P}$). Точнее, имеет место

Предложение 5.5. *Существование в* $\mathscr{P}$ *конкретного слова* e_0, *для которого функция* $\nu^3(e_0, x, y)$ *полиномиально вычислима, равносильно полиномиальной вычислимости функции* $\nu^2(x, y)$ *и равносильно равенству* $\mathrm{P} = \mathrm{NP}$. □

Напомним, что функция $\nu(x)$ заведомо невычислима за полиномиальное время.

§ 6. РЕАЛИЗУЕМОСТЬ ПО КЛИНИ И КОНСТРУКТИВНОСТЬ ТЕОРИЙ, СОДЕРЖАЩИХ ECT_U

Определим теперь клиниевскую реализуемость, т. е. каждой формуле φ сопоставим формулу $x\mathbf{r}\varphi$, свободные переменные которой суть в точности свободные переменные формулы φ плюс переменная x. Причем сделаем это так, чтобы формула $x\mathbf{r}\varphi$ оказалась не только почти негативной (как в [17, с. 51]), а U-негативной, т. е. содержала бы кванторы $\exists$ только по унарным словам (это нужно для доказательства предложения 6.1). Положим индуктивно:

$$x\mathbf{r}\varphi \rightleftharpoons \varphi, \text{ если } \varphi \text{ атомарная формула},$$

$$\langle x, y\rangle \mathbf{r}(\alpha \wedge \psi) \rightleftharpoons x\mathbf{r}\varphi \wedge y\mathbf{r}\psi,$$

$$\langle x, y, z\rangle \mathbf{r}(\varphi \vee \psi) \rightleftharpoons (x = 0 \supset y\mathbf{r}\varphi) \wedge (x \neq 0 \supset z\mathbf{r}\psi),$$

$$\langle x, y\rangle \mathbf{r}\exists y\psi(y) \rightleftharpoons x\mathbf{r}\psi(y),$$

$$x\mathbf{r}(\varphi \supset \psi) \rightleftharpoons \forall y(y\mathbf{r}\varphi \supset \exists z \in \mathrm{Un}\, H(x * y, z)) \wedge \forall yz(y\mathbf{r}\varphi \wedge H(x * y, z) \supset$$
$$\supset M(x * y, z)\mathbf{r}\psi),$$

$$x\mathbf{r}\forall y\psi(y) \rightleftharpoons \forall y\exists z \in \mathrm{Un}\, H(x * y, z) \wedge \forall yz(H(x * y, z) \supset M(x * y, z)\mathbf{r}\psi(y)).$$

Определим также $\mathbf{r}\varphi \rightleftharpoons \exists x(x\mathbf{r}\varphi)$.

Предложение 6.1. *В теории* HT_0 *из схемы* ECT_U *выводима схема* $\varphi \leftrightarrow \mathbf{r}\varphi$.

Как следует из теоремы 6.3(в), эти схемы на самом деле эквивалентны.

Доказательство проводится индукцией по построению φ. Пусть, например, $\varphi = \psi \supset \eta$. Используя предположение индукции, получим $(\psi \supset \eta) \leftrightarrow (\exists x(x\mathbf{r}\psi) \supset \exists y(y\mathbf{r}\eta)) \leftrightarrow \forall x(x\mathbf{r}\psi \supset \exists y(y\mathbf{r}\eta))$. Отсюда и из ECT_U (с учетом того, что формула $x\mathbf{r}\psi$ почти негативная с унарными $\exists$) следует $\exists e \forall x(x\,\mathbf{r}\psi \supset \exists y(\{e\}(x) = y \wedge y\mathbf{r}\eta))$, т. е. $\mathbf{r}(\psi \supset \eta)$. Обратно, покажем, что $e\mathbf{r}(\psi \supset \eta)$ влечет $\psi \supset \eta$, т. е. выведем η из $e\mathbf{r}(\psi \supset \eta)$ и ψ. По предположению индукции имеем $x\mathbf{r}\psi$ для некоторого x. Тогда $\{e\}(x)\mathbf{r}\eta$ и снова по предположению индукции получаем η. Заметим, что в случае $\varphi = \forall y\psi$ вместо ECT_U достаточно будет воспользоваться его частным случаем СТ. □

В отсутствии формального тезиса Черча такую связь истинности формул с их реализуемостью, как в предложении 6.1, можно гарантировать только для формул специального вида. Определим для любой почти харроповой формулы χ ее *потенциальную* реализацию — ЧРТ $\tau_e[\chi]$, где параметр e обозначает двоичное слово, содержащее информацию о некотором алгоритме поиска, т. е. предполагается SA^e (см. 5.4). Положим индуктивно:

$$\tau_e[\text{атом}] = \varnothing,$$

$$\tau_e[\varphi \wedge \psi] = \langle \tau_e[\varphi], \tau_e[\psi] \rangle,$$

$$\tau_e[\alpha \vee \beta] = \langle \text{ЕСЛИ } \alpha \text{ ТО } 0 \text{ ИНАЧЕ } 1, \tau_e[\alpha], \tau_e[\beta] \rangle,$$

$$\tau_e[\eta \supset \psi] = \Lambda x.\tau_e[\psi] \quad (x \text{ — новая переменная}),$$

$$\tau_e[\neg\eta] = \Lambda x.\varnothing,$$

$$\tau_e[\forall x\psi(x)] = \Lambda x.\tau_e[\psi(x)],$$

$$\tau_e[\exists x \in \mathrm{Un}\,\alpha(x)] = \langle \varnothing,\ \mu x \in \mathrm{Un}\,\alpha(x) \rangle,$$

$$\tau_e[\exists x \alpha(x, \bar{z})] = \langle \varnothing, \xi^{e,\bar{z}}(\mu i \in \mathrm{Un}\,\alpha(\xi_i^{e,\bar{z}}, \bar{z})) \rangle,$$

где φ, ψ — почти харроповы, α, β — бескванторные, а η — произвольная формулы. Если почти харропова формула χ фактически является харроповой, то $\tau_e[\chi]$ — сигнатурный (всюду определенный полиномиально вычислимый) терм.

Лемма 6.2. *Если $\chi(e)$ — почти харропова и $\theta(e)$ — почти негативная формулы, то в теории $\mathrm{HT}_0 + \mathrm{SA}^e$ выводимы эквивалентности*

$$\mathbf{r}\chi \leftrightarrow !\,\tau_e[\chi] \wedge \tau_e[\chi]\,\mathbf{r}\chi,$$

$$\mathbf{r}\theta \leftrightarrow \theta \leftrightarrow !\tau_e[\theta] \wedge \tau_e[\theta]\,\mathbf{r}\theta.$$

При этом в случае U-негативной θ и U-харроповой χ аксиома SA^e не используется и ξ^e не участвует в $\tau[\theta]$ и $\tau[\chi]$.

Доказательство проводится индукцией по построению формул χ и θ с использованием в случае χ, $\theta = \exists x\alpha$ теоремы 5.2 о канонических алгоритмах поиска. Фактически для θ надо доказать импликации $\mathbf{r}\theta \supset \theta$ и $\theta \supset !\,\tau_e[\theta] \wedge \tau_e[\theta]\,\mathbf{r}\theta$. □

и

Теперь мы можем сформулировать и доказать основной результат об r-реализуемости.

Теорема 6.3. (а) *Для любого логического правила $\varphi_1, \ldots, \varphi_n/\varphi$, $n \geqslant 0$, теории HT_0 и ЧРТ $t_1, \ldots, t_n$ (возможно с новыми константами) можно построить ЧРТ t такой, что*

$$\mathrm{HT}_0 + \widetilde{\forall} \bigwedge_{i=1}^{n} (!t_i \wedge t_i\mathbf{r}\varphi_i) \vdash !\,t \wedge t\mathbf{r}\varphi,$$

где $\widetilde{\forall}$ обозначает универсальное замыкание по всем свободным переменным.

(б) *Для нелогических (бескванторных) аксиом θ теории HT_0 имеем $\mathrm{HT}_0 \vdash \tau[\theta]\,\mathbf{r}\theta$, причем $\tau[\theta]$ — сигнатурный терм.*

(в) *Для каждого примера* $\overline{\mathrm{ECT}}$, $\overline{\mathrm{ECT}_U}$, M *и* M_U *можно построить соответствующие реализующие сигнатурные термы* $t(e)$, t_U, $t_{\mathrm{M}}(e)$ *и* $t_{\mathrm{M}U}$ *такие, что*

$$\mathrm{HT}_0 \vdash t_U \mathbf{r}\overline{\mathrm{ECT}_U},$$

$$\mathrm{HT}_0 + \mathrm{SA}^e \vdash t(e)\mathbf{r}\overline{\mathrm{ECT}},$$

$$\mathrm{HT}_0 + \mathrm{ECT} \vdash \mathbf{r}\overline{\mathrm{ECT}},$$

$$\mathrm{HT}_0 + \mathrm{M}_U \vdash t_{\mathrm{M}U}\mathbf{r}\mathrm{M}_U,$$

$$\mathrm{HT}_0 + \mathrm{SA}^e + \mathrm{M} \vdash t_{\mathrm{M}}(e)\mathbf{r}\mathrm{M},$$

$$\mathrm{HT}_0 + \mathrm{ECT}_U + \mathrm{M} \vdash \mathbf{r}\mathrm{M} \wedge \mathbf{r}\overline{\mathrm{ECT}}.$$

(г) *Существует* ЧРТ $t_S(e)$ *такой, что*

$$\mathrm{HT}_0 + \mathrm{SA}^e \vdash !\, t_S(e) \wedge t_S(e)\,\mathbf{r}\mathrm{SA}^e \wedge \mathbf{r}\mathrm{SA}.$$

Заметим, что из формулировки теоремы не удается вывести существование ЧРТ t такого, что $\mathrm{HT}_0 + \mathrm{SA} \vdash t\mathbf{r}\mathrm{SA}$ или $\mathrm{HT}_0 + \mathrm{ECT} \vdash t\mathbf{r}\mathrm{ECT}$.

Доказательство (а) см., например, [17, с. 54—55], а (б) следует из леммы 6.2: $\mathrm{HT}_0 \vdash \theta \leftrightarrow \tau[\theta]\mathbf{r}\theta$.

(в) В качестве реализации $\overline{\mathrm{ECT}_U}$ и $\overline{\mathrm{ECT}}$,

$$\forall x(\psi(x, \bar{z}) \supset \exists y\psi(x, y, \bar{z})) \supset \exists f \forall x(\psi(x, \bar{z}) \supset \exists n(H(f * x, n) \wedge$$

$$\wedge \varphi(x, M(f * x, n), \bar{z}))),$$

можно взять ЧРТ $t \rightleftharpoons \Lambda v\langle R(v, \bar{z}), F(v, \bar{z})\rangle$, где $F(v, \bar{z}) \rightleftharpoons$ $\rightleftharpoons \Lambda x(\{\{v\}(x)\}(\tau(x, \bar{z})))_2$, $\tau(x, \bar{z}) \rightleftharpoons \tau_e[\psi(x, \bar{z})]$ — потенциальная реализация из леммы 6.2 (без участия ξ и e в случае $\overline{\mathrm{ECT}_U}$) почти харроповой формулы ψ, $R(v, \bar{z}) \rightleftharpoons \Lambda xw.\langle\langle 0, S(v, x, \bar{z})\rangle, N(v, x, \bar{z})\rangle$ (w — новая «фиктивная» переменная), $S(v, x, \bar{z}) \rightleftharpoons (\{\{v\}(x)\}(\tau(x, \bar{z})))_1$ и $N(v, x, \bar{z}) \rightleftharpoons$ $\rightleftharpoons \mu n \in \mathrm{Un}.H(F(v, \bar{z}) * x, n)$.

Действительно, покажем, что из

$$v\mathbf{r}\forall x(\psi(x) \supset \exists y\varphi(x, y)) \tag{1}$$

следует

$$R(v, \bar{z})\,\mathbf{r}\forall x(\psi(x, \bar{z}) \supset \exists n(H(F(v, \bar{z}) * x, n) \wedge \varphi(x, M(F(v, \bar{z}) * x, n), \bar{z})))$$

или, эквивалентно,

$$\forall xw(w\mathbf{r}\psi(x) \supset !\, N(v, x, \bar{z}) \wedge !\, S(v, x, \bar{z})\,\mathbf{r}\varphi(x, M(F(v, \bar{z}) * x, N(v, x, \bar{z})), \bar{z})). \tag{2}$$

В силу леммы 6.2 из $w\mathbf{r}\psi(x, \bar{z})$ и SA^e в случае $\overline{\mathrm{ECT}}$ вытекает $!\tau(x, \bar{z})\mathbf{r}\psi(x, \bar{z})$. Значит, благодаря предположению (1) имеем $!\{\{v\}(x)\}(\tau(x, \bar{z}))\mathbf{r}\exists y\varphi(x, y, \bar{z})$, т. е.

$$!\{F(v, \bar{z})\}(x), \tag{3}$$

$$!S(v, x, \bar{z})\mathbf{r}\varphi(x, \{F(v, \bar{z})\}(x)). \tag{4}$$

Но (3) равносильно $!N(v, x, \bar{z})$, а из (4) и $\{F(v, \bar{z})\}(x) \simeq M(F(v, \bar{z}) * x, N(v, x, \bar{z}))$ следует и второй конъюнктивный член доказываемой импликации (2).

Утверждение $\mathrm{HT}_0 + \mathrm{ECT} \vdash \mathbf{r}\overline{\mathrm{ECT}}$ получается теперь с помощью предложения 3.1 (а).

В качестве реализации принципа Маркова М, $\neg\neg\exists x\alpha(x) \supset \exists x\alpha(x)$, и его частного случая M_U, при $\alpha(x) \rightleftharpoons x \in \mathrm{Un} \wedge \alpha'(x)$, можно взять сигнатурный терм $t_{\mathrm{M}}(e) \rightleftharpoons \Lambda y.\tau_e(\exists x\alpha(x))$. Действительно, в HT_0 из $y\mathbf{r}\neg\neg\exists x\alpha(x)$ следует $\neg\neg\exists x\alpha(x)$ и, значит, опираясь на М или соответственно на M_U, выводим $\exists x\alpha(x)$. Отсюда с помощью леммы 6.2

(и SA^e в случае M) получаем $!\tau_e[\exists x\alpha(x)] \wedge \tau_e[\exists x\alpha(x)]\,\mathbf{r}\exists x\alpha(x)$, что и требовалось.

Утверждение $HT_0 + ECT_U + M \vdash \mathbf{r}M \wedge \mathbf{r}\overline{ECT}$ следует теперь из предложения 3.1 (б).

(г) Поскольку формула SA^x является почти негативной с унарным $\exists$, то по лемме 6.2 $HT_0 \vdash SA^x \leftrightarrow !\tau[SA^x]\,\mathrm{r}SA^x$ и, значит, можно положить $t_S(e) \rightleftharpoons \tau[SA^e]$. □

Следствие 6.4. *Если* $HT_0 + SA^e + M + ECT \vdash \varphi(e, \bar{x})$, *где* e — *новая константа, то для некоторого* ЧРТ $t(e, \bar{x})$ *имеем* $HT_0 + SA^e + M \vdash$ $\vdash !t(e, \bar{x}) \wedge t(e, \bar{x})\mathbf{r}\varphi(e, \bar{x})$. *Причем, если первый вывод проведен в теории* $HT_0(+M_U) + ECT_U$, *то второй можно провести в* $HT_0(+M_U)$ *и терм* $t(e, \bar{x}) = t(\bar{x})$ *может быть взят* (в силу предложения 2.2) *сигнатурным.*

Согласно предложению 2.12 и определениям v^3 и SA^e в конце § 5 здесь можно считать, что терм $t(e, \bar{x})$ является суперпозицией сигнатурных функций, функции $v^3(e, x, y)$ от x и y и константы e, а также, что $HT_0 + SA^e \vdash !t(e, \bar{x})$. В этом смысле с учетом следствия 6.5 и определения конструктивности теории, приведенного в § 1, можно утверждать, что степень конструктивности теории $HT_0 + SA^e + ECT + M$ (и ряда ее ослаблений) характеризуется сложностью вычисления функции $v^3(e, x, y)$ от x и y.

Следствие 6.5 (о конструктивности). (а). *Теория* $HT_0 + SA^e(+M) +$ $+ ECT_U$ *конструктивна* *). *Фактически, если в ней выводима импликация* $\chi(e, \bar{x}) \supset \exists y\varphi(e, \bar{x}, y)$ *с почти харроповой посылкой* χ, *то в этой теории с* ECT *вместо* ECT *выводима импликация* $\chi(e, \bar{x}) \supset !t(e, \bar{x}) \wedge \varphi(e, \bar{x}, t(e, \bar{x}))$ *для некоторого* ЧРТ $t(e, \bar{x})$. *Если же посылка* χ *отсутствует, то* $t(e, \bar{x})$ — *суперпозиция сигнатурных функций, функции* $v^3(e, x, y)$ *и константы* e.

(б) *Теория* $HT_0 + ECT_U(+M_U)$ *является конструктивной и даже полиномиально* $\exists$*-конструктивной* (см. § 1).

Доказательство. (а). По следствию 6.4 получаем в $HT_0 +$ $+ SA^e(+M)$ вывод формулы вида $w\mathbf{r}\chi(e, \bar{x}) \supset \mathbf{r}\varphi(e, x, \{\tilde{t}(e, \bar{x})\}(w))$. Далее, лемма 6.2 дает $\mathbf{r}\chi(e, \bar{x}) \supset \mathbf{r}\varphi(e, \bar{x}, \{\tilde{t}(e, \bar{x})\}(\tau_e[\chi(e, \bar{x})]))$. Отсюда, применив предложение 6.1 и положив $t \rightleftharpoons \{\tilde{t}\}(\tau_e[\chi])$, получаем требуемый результат. В отсутствии χ имеем $\vdash !t$ и используем предложение 2.12.

(б) Утверждение следует из доказательства (а) с учетом второй части следствия 6.4, U-харраповости формулы χ, требуемой в определении конструктивности теории, и леммы 6.2, благодаря чему аксиома SA^e не используется (и $\tilde{t}$ — сигнатурный терм). □

Следствие 6.6. *Теория* $HT_0 + SA^e(+M) + ECT$ *консервативно расширяет теорию* $HT_0 + SA^e(+M)$ *относительно почти негативных формул. Аналогично для* $HT_0(+M_U) + ECT_U$ *и* U*-негативных формул.*

Доказательство состоит в применении следствия 6.4 (и теоремы 6.3), леммы 6.2. □

Отсюда и из теоремы 5.1 получаем

Следствие 6.7. *Теория* $HT_0 + ECT + M$ *консервативно расширяет теории* T_0 *и* HT_0 *относительно* Π_2*-формул; и значит, ее доказуемо-рекурсивные функции являются в точности полиномиально вычислимыми функциями.* □

В частности, в этой теории не доказуемо предложение EXP, но доказуемо SA, и поэтому имеет место

Следствие 6.8. *В теории* $HT_0 + ECT + M$ (как и в T_0 [2]) *недоказуемо утверждение о существовании нижней экспоненциальной оценки времени работы алгоритмов поиска, т. е. не доказуема формула* $SA(e) \supset$ $\supset \forall z\exists x > z\exists n(H(e * x, n) \wedge \forall m < n \neg H(e * x, m) \wedge \exp(x, n))$. □

Из теоремы 6.3 (в) и предложения 6.1 получаем также

Следствие 6.9. $HT_0 + ECT \vdash \overline{ECT}$, $HT_0 + ECT_U \vdash \overline{ECT}_U$.

---

*) К сожалению, не удается опустить здесь e или, равносильно, SA^e.

Теорема 6.10. *Конструктивность теории* $\mathrm{HT}_0+\mathrm{ECT}(+\mathrm{M})$ *равносильна ее (полиномиальной)* Э*-конструктивности и равносильна равенству* $\mathrm{P}=\mathrm{NP}$.

Доказательство. Мы покажем, что из Э-конструктивности этой теории следует равенство $\mathrm{P}=\mathrm{NP}$, откуда, в свою очередь, следует ее (полиномиальная Э-)конструктивность. Действительно, из Э-конструктивности рассматриваемой теории и предложения 3.1 (а) следует выводимость в ней формулы $\mathrm{SA}(e_0)$ или эквивалентно формулы

$$\forall x y \exists n \in \mathrm{Un}\,(x[y] \supset H(e_0 * x, n) \wedge x[M(e_0 * x, n)])$$

для некоторого конкретного алгоритма поиска e_0. Но в таком случае по следствию 6.7 и предложению 2.2 алгоритм поиска e_0 работает (в $\mathscr{P}$) полиномиальное время, что, как известно, приводит к равенству $\mathrm{P}=\mathrm{NP}$.

Далее, из $\mathrm{P}=\mathrm{NP}$ вытекает (полиномиальная Э-) конструктивность рассматриваемой теории. Доказательство состоит в применении предложения 3.3 и следствия 6.5 (б). □

§ 7. КОНСТРУКТИВНОСТЬ ТЕОРИЙ БЕЗ ECT_U

В отсутствии схемы ECT_U мы не можем воспользоваться предложением 6.1 о выводимости эквивалентности $\varphi \leftrightarrow \mathbf{r}\varphi$ для доказательства конструктивности рассматриваемой теории (см. следствие 6.5). В связи с этим мы несколько модифицируем понятие реализуемости. А именно, определим формулу $x\mathbf{q}\varphi$ (см. [18, с. 178]) индукцией по построению φ аналогично определению $x\mathbf{r}\varphi$, изменив только три пункта:

$$\langle u, v, w\rangle\, \mathbf{q}(\varphi \vee \psi) \rightleftharpoons [u = 0 \supset (v\mathbf{q}\varphi) \wedge \varphi] \wedge [u \neq 0 \supset (w\mathbf{q}\psi) \wedge \psi],$$

$$\langle x, y\rangle\, \mathbf{q}\exists y \varphi(y) \rightleftharpoons (x\mathbf{q}\varphi(y)) \wedge \varphi(y),$$

$$x\mathbf{q}(\varphi \supset \psi) \rightleftharpoons \forall y\,((y\mathbf{q}\varphi) \wedge \varphi \supset !\{x\}(y) \wedge \{x\}(y)\,\mathbf{q}\psi).$$

Теперь уже формула $x\mathbf{q}\varphi$, вообще говоря, не является почти негативной.

Лемма 7.1. *Утверждения леммы* 6.2 *полностью выполняются и для* $\mathbf{q}$*-реализуемости с добавлением* $\mathrm{HT}_0+\mathrm{SA}^e \vdash \chi \supset !\tau_e[\chi]\mathbf{q}\chi$ *(для почти харроповых* χ *и без* SA^e *для* U*-харроповых* χ*).* □

Теорема 7.2. *Все пункты теоремы* 6.3, *кроме утверждений о реализуемости схем* ECT *и* ECT_U, *выполняются и для* $\mathbf{q}$*-реализуемости с теми же термами.*

В доказательстве этой теоремы используется лемма 7.1 лишь для Σ_1- и Π_2-формул θ при доказательстве $\mathbf{q}$-реализуемости M и SA^e. □

Следствие 7.3. *Если* $\mathrm{HT}_0+\mathrm{SA}^e(+\mathrm{M}) \vdash \varphi(e, \bar{x})$, *где* e *— новая константа, то для некоторой суперпозиции* t *сигнатурных функций,* ЧРФ $\nu^3(e, z, y)$ *и константы* e *в этой же теории выводимо* $!t(e, \bar{x})\mathbf{q}\varphi(e, \bar{x})$. *При этом если первый вывод проведен в* $\mathrm{HT}_0(+\mathrm{M}_U)$, *то таков же и второй вывод, и терм* t *в этом случае можно взять сигнатурным.* □

Следствие 7.4. (о конструктивности). (а). *Если в теории* $\mathrm{HT}_0+\mathrm{SA}^e(+\mathrm{M})$ *выводима импликация* $\chi(e, \bar{x}) \supset \exists y \varphi(e, \bar{x}, y)$ *с почти харроповой посылкой, то в этой же теории выводима импликация* $\chi(e, \bar{x}) \supset \supset !t(e, \bar{x}) \wedge \varphi(e, \bar{x}, t(e, \bar{x}))$ *для некоторого* ЧРТ t *такого же вида, как в следствии* 6.5.

(б) *Теории* HT_0 *и* $\mathrm{HT}_0+\mathrm{M}_U$ *(полиномиально* Э-*) конструктивны.*

Доказательство. (а) На основании следствия 7.3 получаем вывод в $\mathrm{HT}_0+\mathrm{SA}^e(+\mathrm{M})$ формулы вида

$$w\mathbf{q}\chi(e, \bar{x}) \wedge \chi(e, \bar{x}) \supset \mathbf{q}\varphi(e, \bar{x}, \{\tilde{t}(e, \bar{x})\}(w)) \wedge \varphi(e, \bar{x}, \{\tilde{t}(e, \bar{x})\}(w)).$$

Отсюда лемма 7.1 дает $\chi(e, \bar{x}) \supset \varphi(e, \bar{x}, \{\tilde{t}(e, \bar{x})\}(\tau_e[\chi(e, \bar{x})]))$, что и требовалось.

(б) Доказывается аналогично п. (б) следствия 6.5. □

Следующие теоремы 7.5 и 7.6 показывают, что вопрос о (полиномиальной $\exists$-) конструктивности теории $HT_0 + M$ имеет решение, несколько отличающееся от решения, например, для теории $HT_0 + ECT_U + M = HT_0 + ECT + M$, для которой свойства ее конструктивности и $\exists$-конструктивности являются эквивалентными (равенству $P = NP$; см. теорему 6.10).

Теорема 7.5. *Конструктивность теории* $HT_0 + M$ *равносильна равенству* $P = NP$.

Доказательство. Из конструктивности теории $HT_0 + M$, содержащей частный случай принципа Маркова $\neg\forall y\,\neg x[y] \supset \exists y.x[y]$, следует выводимость в этой же теории, а значит, и в теории T_0 формулы вида $x[y] \supset !\,t(x) \wedge x[t(x)]$, где ЧРТ $t(x)$ зависит только от переменной x. По предложению 2.2 время вычисления значения $t(x)$ можно считать полиномиальным. Это, очевидно, приводит к равенству $P = NP$.

Обратно, из равенства $P = NP$ по предложению 3.3 следует, что принцип M сводится к M_U, откуда по следствию 7.4 (б) получаем конструктивность теории $HT_0 + M$. □

Теорема 7.6. *Теория* $HT_0 + M$ *является полиномиально* $\exists$*-конструктивной.*

Сначала сформулируем одно естественное *обобщение теоремы об устранении сечений* [2, 22]*), доказательство которого во многом совпадает с доказательством обычного необобщенного ее варианта (см., например, [25]; вместо LK- или LJ-выводов, содержащих ровно одно сечение, следует рассматривать регулярные [25] выводы, содержащие ровно одно «плохое» сечение, причем к п. 2.1.2 из доказательства в [25] добавляется нетривиальный подпункт, когда J_2 — сечение).

Теорема 7.7. *Из всякого вывода в генценовском исчислении секвенций* LK *или* LJ, *обогащенном некоторым набором начальных секвенций* (кроме обычных, вида $\varphi \to \varphi$), *замкнутым относительно операций подстановки термов вместо переменных, можно устранить все сечения, кроме, быть может, сечений по формулам, встречающимся в новых начальных секвенциях. Полученный вывод можно считать регулярным.* □

Доказательство теоремы 7.6. Согласно обобщенной теореме об устранении сечений любой вывод в теории $HT_0 + M$, основанный на интуиционистском исчислении секвенций LJ [25], где M представляется как секвенция $\neg\neg\exists x\alpha \to \exists x\alpha$, можно перестроить в вывод без «плохих» сечений, т. е. с сечениями лишь по формулам вида α, $\exists x\alpha$ или $\neg\neg\exists x\alpha$ с бескванторными α. Поэтому предположим, что в $HT_0 + M$ выводима без использования плохих сечений секвенция $\Gamma \to \exists y\varphi(y)$, где список Γ состоит из формул вида α, $\exists x\alpha$ или $\neg\neg\exists x\alpha$ с бескванторными α. Индукцией по выводу покажем, что тогда выводима также секвенция вида $\Gamma' \to \varphi(t)$, где t сигнатурный терм и Γ' получается из Γ путем снятия всех кванторов $\exists$ и $\neg\neg\exists$. (Таким образом, список Γ' состоит из бескванторных формул.)

Если $\Gamma \to \exists y\varphi(y)$ является начальной секвенцией, т. е. частным случаем принципа Маркова $\neg\neg\exists y\varphi \to \exists y\varphi$ (с бескванторной φ), то в силу тривиальной выводимости секвенции $\varphi \to \varphi$ мы можем взять в качестве t терм y. В противном случае $\Gamma \to \exists y\varphi$ получается по одному из следующих правил вывода.

$$(\to\exists) \qquad \frac{\Gamma \to \varphi(t)}{\Gamma \to \exists y\varphi(y)}$$

При этом требуемой секвенцией является $\Gamma' \to \varphi(t)$. Она выводится (с помощью сечения) из посылки и из очевидно выводимых секвенций

*) Отметим, что в автореферате [26] на [22] (но не в [2,22]) приведена ошибочная, слишком сильная формулировка обобщенной теоремы об устранении сечений.

вида $\alpha(x) \to \exists x \alpha(x)$, $\alpha(x) \to \neg\neg \exists x \alpha(x)$, заключения которых лежат в Γ.

(ослабление справа) $$\frac{\Gamma \to}{\Gamma \to \exists y \varphi(y)}$$

При этом, как и в случае $(\to \exists)$, выводима секвенция $\Gamma' \to$ и, значит, секвенция $\Gamma' \to \varphi(t)$ для совершенно произвольного t.

(сечение) $$\frac{\Pi \to (\neg\neg)\, \exists x \alpha(x)\ (\neg\neg)\, \exists x \alpha(x),\ \Delta \to \exists y \varphi(y)}{\Pi, \Delta \to \exists y \varphi(y)}$$

При этом $\Gamma = \Pi, \Delta$ и по предположению индукции можно считать, что выводимо $\alpha(x)$, $\Delta' \to \varphi(r(x))$ для некоторого терма $r(x)$. Поскольку теория $HT_0 + M$ является фрагментом классической теории (а именно, T_0) и в ней классически выводима секвенция $\Pi' \to \exists x \alpha(x)$, где Π', α — бескванторные формулы, то мы можем использовать теорему Эрбрана для обоснования выводимости секвенции $\Pi' \to \alpha(s_1) \vee \ldots \vee \alpha(s_k)$, а значит, и секвенции $\Pi' \to \alpha(s)$ для некоторых термов $s_1, \ldots, s_k, s$. Отсюда с помощью сечения по $\alpha(s)$ и подстановки s вместо x в выводимую секвенцию $\alpha(x)$, $\Delta' \to \varphi(r(x))$ получаем вывод секвенции Π', $\Delta' \to \varphi(r(s))$ и полагаем $t \rightleftharpoons r(s)$.

$(\exists \to)$ $$\frac{\alpha(x), \Gamma \to \exists y \varphi(y)}{\exists x \alpha(x), \Gamma \to \exists y \varphi(y)}$$

В этом случае существующий по предположению индукции вывод секвенции $\alpha(x)$, $\Gamma' \to \varphi(t)$, является требуемым.

$(\supset \to)$ $$\frac{\Gamma_1 \to \alpha_1\ \alpha_2,\ \Gamma_2 \to \exists y \varphi(y)}{\alpha_1 \supset \alpha_2,\ \Gamma_1,\ \Gamma_2 \to \exists y \varphi(y)}$$

Здесь терм t, существующий по предположению индукции для правой посылки, годится и для заключения, причем соответствующий вывод секвенции $\alpha_1 \supset \alpha_2$, $\Gamma_1', \Gamma_2' \to \varphi(t)$ получается из выводов $\Gamma_1' \to \alpha_1$ и α_2, $\Gamma_2' \to \varphi(t)$ применением этого же правила $(\supset \to)$.

$(\wedge \to)$ $$\frac{\alpha_1, \Gamma \to \exists y \varphi(y)}{\alpha_1 \wedge \alpha_2, \Gamma \to \exists y \varphi(y)}$$

Этот случай аналогичен предыдущему.

$(\vee \to)$ $$\frac{\alpha_1, \Gamma \to \exists y \varphi(y)\ \ \alpha_2, \Gamma \to \exists y \varphi(y)}{\alpha_1 \vee \alpha_2, \Gamma \to \exists y \varphi(y)}$$

По предположению индукции в этом случае существуют соответствующие термы t_1 и t_2 для верхних секвенций. Поскольку α_1 и α_2 здесь бескванторные, в роли t, очевидно, можно взять терм ЕСЛИ α_1, ТО t_1 ИНАЧЕ t_2.

Еще проще рассматриваются оставшиеся возможные случаи правил ослабления сокращения и перестановки слева. □

§ 8. ДОБАВЛЕНИЕ

1. Связь с теорией сложности по Колмогорову

Приведенное в этой статье разбиение конечных объектов на конструктивные и неконструктивные или простые и сложные было введено в [2] на основе полиномиально оптимального упарного кодирования ξ_i. Выше было установлено, что к такому же разбиению приводит частично рекурсивное кодирование $\{B_i\}$. Эти определения также следующим образом связаны с понятием сложности конечных объектов по Колмогорову (см. [27]).

Прежде всего заметим, что ЧРФ $\{x\}$ определена нами так, чтобы она была аддитивно оптимальной (по Колмогорову). Это значит, что любое

другое частично рекурсивное кодирование $\{e\}(x)$ сводится к данному кодированию $\{x\}$ с увеличением длины кода x не более, чем на (аддитивную) константу: $\{e\}(x) \simeq \{e * x\}$, где $|e * x| \leqslant |x| + \mathrm{const}_e\ (= |x| + 2|e|)$.

Двоичное слово y назовем *простым по Колмогорову*, если оно имеет существенно более короткое, чем само слово y, описание x посредством аддитивно оптимального алгоритма, т. е. $y = \{x\}$ и, используя неформальное обозначение, $|x| \ll |y|$. Заметим, что в рамках традиционного представления о конечном, это определение является нестрогим, и непонятно, как его можно было бы уточнить, чтобы оно не зависело от небольших вариаций аддитивно оптимального кодирования и т. п. и при этом действительно осуществляло разбиение множества двоичных слов на два класса. Конечно, подход самого А. Н. Колмогорова является несколько иным, математически вполне точным и «машинно-независимым». Но основан он на переходе к бесконечности — в терминах асимптотики.

В случае же безэкспоненциальной математики (например, теорий T_0, T, HT_0 и т. п.) оказывается возможным уточнить само это определение. Например, конструктивные слова вида ξ_i или вида $\{B_i\}$ естественно охарактеризовать как *логарифмически простые по Колмогорову*, поскольку длины кодов B_j этих слов (в аддитивно оптимальном кодировании) являются логарифмами от всех возможных длин в «безэкспоненциальном мире» конечных объектов. Можно также определить слово y простым по Колмогорову в другом смысле, если оно имеет код x, $y = \{x\}$, такой, что целая часть дроби $|y|/|x|$ является длинным унарным словом, т. е. не имеет вида $|B_i|$. Причем заметим, что здесь эти определения имеют точный (и невырожденный) смысл, поскольку в наших теориях слова вида $|B_i|$ это, вообще говоря, не все возможные унарные слова.

2. Доказательство предложения 2.1(б).

Во-первых, линейная индукция выводится из лексикографической, поскольку из $\forall x(\varphi(|x|) \supset \varphi(|x1|))$ следует $\forall x(\varphi(|x|) \supset \varphi(|x'|))$ в силу бесквантороной аксиомы $|x'| = |x| \vee |x'| = |x1|$ и закона исключенного третьего для бесквантороных формул. Обратно, лексикографическая индукция выводится из линейной в бесквантороном случае, следуя доказательству предложения 2.1 (а). В случае ограниченной индукционной формулы представим лексикографическую индукцию в форме

$$\forall x\ (\varphi(x) \supset \varphi\ (x')) \supset \forall m \forall n \leqslant m \forall x,\ y \leqslant 1^m\ (|y| = m - n \wedge |x| = n \wedge \varphi(y0^n) \supset \varphi(yx)),$$

где φ ограниченная формула и переменные m, n пробегают унарные слова *), и выведем заключение этой импликации из посылки с помощью ограниченной индукции по унарному n. Случай $n = \varnothing$ очевиден. Докажем шаг индукции от n к $n+1$. Пусть имеет место $|y| = m - n - 1$, $|x| = n + 1$, $\varphi(y00^n)$. Надо показать, что для любого слова v длины $n+1$ выполняется $\varphi(yv)$. По предположению индукции для любого z длины n имеем $\varphi(y0z)$ и, в частности, $\varphi(y01^n)$. Переходя к лексикографически следующему слову, отсюда получаем $\varphi(y10^n)$. Снова по предположению индукции для любого z длины n имеем $\varphi(y1z)$. Таким образом, мы доказали, что для любого v (=$0z$ или =$1z$) длины $n+1$ имеет место $\varphi(yv)$, что и требовалось.

Непосредственно усматривается, что в этом доказательстве мы опирались лишь на конечное число схем аксиом теории HT_0. При подходящем выборе конечного базиса для п. в. функций и предикатов и конечного числа соответствующих бесквантороных аксиом теории HT_0 (индуктивно определяющих базисные функции и предикаты) эти схемы аксиом следуют из одной схемы линейной ограниченной индукции.

*) Заметим, что неравенство $y \leqslant 1^m$, очевидно, равносильно $|y| \leqslant m$.

3. О реализации ограниченной индукции

К сожалению, не удается усилить основные результаты этой статьи (например, о невыводимости нижней экспоненциальной оценки для алгоритмов поиска), заменив в них теорию HT_0 на HT_0 + ограниченная индукция, например, в виде

$$\varphi(\varnothing) \wedge \forall i(\varphi(i) \supset \varphi(i+1)) \supset \forall i \varphi(i),$$

где φ содержит только ограниченные кванторы и i переменная по унарным словам (натуральным числам). Для этого надо было бы построить реализацию e_φ этой схемы и доказать, что e_φ действительно является реализацией, используя при этом лишь ограниченную индукцию. Единственное, что удается сделать, это взять в качестве e обычную реализацию полной схемы индукции, т. е. с совершенно произвольной индукционной формулой φ. Такая реализация e не зависит от φ и определяется системой уравнений

$$\{\{e\}(\langle x, y\rangle)\}(0) \simeq x,$$

$$\{\{e\}(\langle x, y\rangle)\}(i+1) \simeq \{\{y\}(i)\}(\{\{e\}(\langle x, y\rangle)\}(i)),$$

т. е., по существу, с помощью *примитивной рекурсии*. При этом чтобы e действительно было реализацией, должно быть доказано, что оператор e по реализациям x и y дает всюдуопределенную функцию от i. А это удается сделать лишь в теориях, в которых оператор примитивной рекурсии является законным и тем самым экспонента, итерация экспоненты и т. п. примитивно-рекурсивные функции являются осуществимыми.

СПИСОК ЛИТЕРАТУРЫ

1. **Сазонов В. Ю.** Эквивалентность полиномиальной конструктивности принципа Маркова равенству P = NP // 19-я Всесоюз. алгебраическая конф., Львов, сент. 1987 г.: Тез. сообщ.— Львов, 1987.— Ч. 2.— С. 250—251.
2*). **Sazonov V. Yu.** A logical approach to the problem "P = NP?" // Math. Found. of Computer Sci.: Proc./9th Symp. Rydzyna, Poland, Sept. 1980.— Berlin a. o.: Springer, 1980.— P. 562—575.— (Lecture Notes in Computer Sci.; 88).
3. **Sazonov V. Yu.** On existence of complete predicate calculus in metamathematics without exponentiation // Math. Found. of Computer Sci.: Proc./10th Symp. Strbske Pleso, Czechoslovakia, sept. 1981.— Berlin a. o.: Springer, 1981.— P. 483—490.— (Lecture Notes in Computer Sci.; 118).
4. **Гэри М., Джонсон Д.** Вычислительные машины и труднорешаемые задачи.— М.: Мир, 1982.
5. **Buss S. R.** Bounded arithmetic.— Bibliopolis, 1986.— 221 p.— (Studies in Proof Theory. Lecture Notes).
6. **Nelson E.** Predicative arithmetic.— Princeton, New Jersey: Princeton Univ. Press, 1986.— (Mathematical Notes; 32.)
7. **Sazonov V. Yu.** Polynomial computability and recursivity in finite domains // Electronische Informationsverarbeitung und Kybernetik.— 1980.— Vol. 16, N 7.— P. 319—323.
8. **Сазонов В. Ю.** Ограниченная теория множеств и полиномиальная вычислимость // Всесоюз. конф. по прикладной логике, Новосибирск, окт. 1985: Тез. докл.— Новосибирск.— С. 188—191.
9. **Сазонов В. Ю.** Ограниченная теория множеств, полиномиальная вычислимость и Δ-программирование // Прикладные аспекты математической логики.— Новосибирск, 1987.— Вып. 122: Вычислительные системы.— С. 110—131.
10. **Gurevich Y.** Algebras of feasible functions // Proc. 24th IEEE Conf. on Found. of Computer Sci., Tucson.— 1893.— P. 210—214.
11. **Mostowski A.** Concerning a problem of H. Sholz // Z. math. Log. und Grundl. Math.— 1956.— N 3.— P. 210—214.
12. **Ливчак А. Б.** Язык полиномиальных запросов // Расчет и оптимизация теплотехнических объектов с помощью ЭВМ.— Свердловск, 1982.— С. 41.
13. **Immerman N.** Relational queries computable in polynomial time // 14th ACM Symp. on Theory of Computing, San-Francisco.— 1982.— P. 147—152.
14. **Vardi M.** Complexity of relational query languages // Ibid.— P. 137—146.
15. **Fagin R.** Generalized first order spectra and polynomial time recognizable sets // Complexity of Computations, SIAM — AMS Proc; 7.— 1974.— P. 43—73.

*) Важное исправление к этой статье приведено в [3, с. 490].

16. **Mycielski J.** Analysis without actual infinity // J. Symbol Log.— 1981.— V. 46.— P. 625—633.
17. **Драгалин А. Г.** Математический интуиционизм. Введение в теорию доказательств.— М.: Наука, 1979. (Серия: Математическая логика и основания математики).
18. **Трулстра А. С.** Аспекты конструктивной математики: Пер. с англ. // Справочная книга по математической логике.— М.: Наука, 1983.— Ч. 4.— С. 160—240.
19. **Гёдель К.** Об одном еще не использованном расширении финитной точки зрения: Пер. с англ. // Математическая теория логического вывода.— М.: Наука, 1967.— С. 499—510.
20. **Howard W. A.** The formulae-as-types notion of construction // To H. B. Curry: essays on combinatory logic, lambda calculus and formalizm.— London: Acad. Press, 1980.— P. 479—490.
21. **Berman P.** Review on [2] // Math. Reviews 83j : 68055.
22. **Сазонов В. Ю.** Принцип коллекции и квантор существования // Логико-математические проблемы МОЗ.— Вып. 107: Вычислительные системы.— Новосибирск, 1985.— С. 30—39.
23. **Parikh R.** Existence and feasibility in arithmetic // J. Symbol. Log.— 1971.— Vol. 36.— P. 494—508.
24. **Левин Л. А.** Универсальные задачи перебора // Проблемы передачи информации.— 1973.— Т. 9, вып. 3.— С. 115—116.
25. **Такеути Г.** Теория доказательств: Пер. с англ.— М.: Мир, 1978.
26. **Сазонов В. Ю.** Автореферат на [22] // Zbl. Math. 605, 03022.
27. **Звонкин А. К., Левин Л. А.** Сложность конечных объектов и обоснование понятий информации и случайности с помощью теории алгоритмов // Успехи мат. наук.— 1970.— Т. 25, вып. 6.— С. 85—127.

В. Л. СЕЛИВАНОВ

ТОНКИЕ ИЕРАРХИИ АРИФМЕТИЧЕСКИХ МНОЖЕСТВ И ОПРЕДЕЛИМЫЕ ИНДЕКСНЫЕ МНОЖЕСТВА

Теоретико-рекурсивные иерархии позволяют измерять алгоритмическую сложность множеств ординалами. Этим их роль в теории алгоритмов аналогична роли чисел для измерения геометрических величин. Давно замечено [1], что индексные множества с «естественными» определениями оказываются универсальными в некотором уровне подходящей иерархии. Возникает общая проблема классификации индексных множеств, определимых в естественном языке. Например, если $(A; \Sigma, \alpha)$ — нумерованная система конечной сигнатуры, можно классифицировать индексные множества формульных предикатов. Очевидна связь этой задачи со сложностью элементарной теории $\mathrm{Th}(A; \Sigma)$ и некоторыми вопросами теории моделей. Так, если существует формульный предикат $X \subseteq A^k$ к которому m-сводится любое рекурсивно-перечислимое относительно диаграммы $(A; \Sigma)$ множество, то $\mathrm{Th}(A; \Sigma)$ не является модельно полной. Первые результаты по этой проблеме получены в [2, 3].

Данная работа посвящена классификации индексных множеств предикатов, формульно определимых на решетке рекурсивно-перечислимых множеств $(\mathscr{E}; \cup, \cap)$. Результаты были объявлены в [4, 5]. Неожиданно оказалось, что для классификации даже очень простых индексных множеств недостаточно иерархий, известных до появления работы [6], аналогично тому, что рациональных чисел недостаточно для измерения даже простых геометрических величин. Это послужило одним из стимулов для поиска естественного класса иерархий, дающих в определенном смысле полную иерархическую классификацию арифметических множеств. Такой класс иерархий найден в [6]. В этом же году появилась работа [7], посвященная классификации борелевских множеств. Сопоставление этих работ показывает, что иерархии из [6] имеют много общих черт со степенями Уэджа борелевских множеств. Эта связь подтверждается полученным в § 1 описанием иерархий из [6] с помощью теоретико-множественных операций из [7]. В § 2 и 3 эти результаты