Ю. Т. МЕДВЕДЕВ

ЛОКАЛЬНО-ФИНИТНЫЕ АЛГОРИТМИЧЕСКИЕ ПРОБЛЕМЫ

(Представлено академиком А. Н. Колмогоровым 26 VIII 1971)

В настоящей работе определяется класс локально-финитных проблем (л.ф.п.) и исследуются операции над такими проблемами, ведущие к построениям в духе теории задач А. Н. Колмогорова (1). При этом роль операций $\supset$ и $\perp$ играет вводимая нами трансфинитная иерархия импликаций и отрицаний различного порядка. На этой основе дается истолкование логико-арифметических формул. Интуитионистски выводимые формулы арифметики оказываются «истинными» (теорема 3). Рекурсия до ординалов, меньших ϵ_0 , используемая при получении этого результата, означает выход за рамки финитистских методов, но по существу не в большей степени, чем это требуется для доказательства непротиворечивости арифметики, данного Гёценом (2). Мы приводим также один результат, получаемый более ограниченными средствами (теорема 4).

Определение 1. 1) Пусть $P(n, p, q)$ — примитивно-рекурсивный предикат. Сформулируем следующую проблему: найти общерекурсивную функцию $f(n)$, для которой утверждение $P(n, f(n), f(n+1))$ истинно при всех натуральных n . Эту проблему мы называем локально-финитной проблемой (л.ф.п.) без свободных переменных, соответствующей предикату P , и обозначаем символом $\mathfrak{F}$. Каждая общерекурсивная $f(n)$, удовлетворяющая нашему условию, называется решением проблемы $\mathfrak{F}$. 2) Пусть $P(n, p, q, x_1, \dots, x_k)$ — примитивно-рекурсивный предикат. Семейство тех л.ф.п., которые получаются из P при замене $x_1, \dots, x_k$ произвольными натуральными числами, называется л.ф.п. со свободными переменными $x_1, \dots, x_k$ и обозначается через $\mathfrak{F}(x_1, \dots, x_k)$. Решением этой л.ф.п. называется всякая общерекурсивная функция $f(n, x_1, \dots, x_k)$, для которой $\forall n \forall x_1 \dots \forall x_k P(n, f(n, x_1, \dots, x_k), f(n+1, x_1, \dots, x_k), x_1, \dots, x_k)$.

Класс л.ф.п. охватывает многие типы алгоритмических проблем. В частности, проблема разрешимости любого рекурсивно-перечислимого множества может быть представлена в форме некоторой л.ф.п., и то же самое верно в отношении проблем отделимости рекурсивно-перечислимых множеств посредством рекурсивных множеств.

Вспомогательные определения. Если $n_1, \dots, n_m$ — натуральные числа ($m \geq 0$), то в качестве гёделева номера кортежа $\langle n_0, \dots, n_m \rangle$ принимаем число $p_0^{n_0+1} \dots p_m^{n_m+1}$, где p_i — простые числа в порядке возрастания. Введем следующие обозначения. Если x — номер кортежа $\langle n_0, \dots, n_m \rangle$, то $L(x) = m$, $x^{(i)} = n_i$ при $i \leq m$, $x^{(i)} = 0$ при $i > m$; если x не является номером кортежа, то $L(x) = 0$, $x^{(i)} = 0$ при всех i . Условимся обозначать $(x^{(i)})^{(j)}$ через $x^{(i, j)}$. Числовой предикат $F(u)$ (« u — финитная функция») определяем из условия $F(u) \equiv \forall i \forall j (i, j \leq L(u^{(0)}) \& u^{(0, i)} = u^{(0, j)} \Rightarrow u^{(1, i)} = u^{(1, j)})$. Предикат $!u(x)$ (« x принадлежит области определения u ») определяем из условия $!u(x) \equiv \exists i (i \leq L(u^{(0)}) \& x = u^{(0, i)})$; если i удовлетворяет условию в скобках, то число $u^{(1, i)}$ обозначается через $u(x)$. Определим, далее, предикаты

$$\Delta(u, v) \equiv F(u) \& F(v) \& \forall x [!u(x) \Rightarrow (!v(x) \& u(x) = v(x))],$$

$$\nabla(x, y) \equiv L(x) < L(y) \& \forall i (i \leq L(x) \Rightarrow x^{(i)} = y^{(i)}),$$

$$I(x, b, d) \equiv L(x) = d \& \forall i (i \leq d \Rightarrow x^{(i)} \leq b).$$

Мы будем пользоваться гёделевой нумерацией всех порядковых чисел (ординалов), меньших канторова числа ϵ_0 , посредством всех натуральных чисел. Считаем, что наименьший ординал имеет номер 0. Номер ординала α обозначаем через $\bar{\alpha}$. Отношения порядка $\alpha < \beta$ и $\alpha \leq \beta$ между ординалами переносятся на их номера; при этом мы применяем те же символы $<$ и $\leq$. Соответствующие предикаты примитивно-рекурсивны.

Шести операциям над л.ф.л. $\mathfrak{P}$ и $\mathfrak{Q}$ соответствует столько же примитивно-рекурсивных операций над предикатами P и Q (последние две операции содержат α в качестве параметра). В данных ниже определениях мы лишь указываем условия, которым должен удовлетворять предикат R — результат операции; однако нетрудно фиксировать наши операции однозначно. Предполагается, что проблемы $\mathfrak{P}$, $\mathfrak{P}(x)$, $\mathfrak{Q}$ и $\mathfrak{R}$ (и соответствующие предикаты) могут содержать свободные переменные, не указанные явно.

Определение 2. Проблема $\mathfrak{R} = \mathfrak{P} \vee \mathfrak{Q}$ соответствует предикату

$$R(n, p, q) \equiv (p^{(0)} = 0 \& q^{(0)} = 0 \& P(n, p^{(1)}, q^{(1)})) \vee \\ \vee (p^{(0)} = 1 \& q^{(0)} = 1 \& Q(n, p^{(1)}, q^{(1)})).$$

Определение 3. Проблема $\mathfrak{R} = \mathfrak{P} \& \mathfrak{Q}$ соответствует предикату

$$R(n, p, q) \equiv P(n, p^{(0)}, q^{(0)}) \& Q(n, p^{(1)}, q^{(1)}).$$

Определение 4. Проблема $\mathfrak{R} = \exists x \mathfrak{P}(x)$ соответствует предикату

$$R(n, p, q) \equiv (p^{(0)} = q^{(0)}) \& P(n, p^{(1)}, q^{(1)}, p^{(0)}).$$

Определение 5 (вспомогательные предикаты « s является n -м частичным решением $\mathfrak{P}$ » и « s является частичным решением $\mathfrak{P}$ »).

$$\bar{P}(n, s) \equiv (n = 0) \vee [n > 0 \& L(s) = n \& \forall i (i \leq n - 1 \Rightarrow \\ \Rightarrow P(i, s^{(i)}, s^{(i+1)}))], \quad \tilde{P}(s) \equiv \exists n \bar{P}(n, s).$$

Определение 6. Проблема $\mathfrak{R} = \forall x \mathfrak{P}(x)$ соответствует предикату

$$R(n, p, q) \equiv \forall i [i \leq n \Rightarrow (L(p^{(i)}) = n \& \nabla (p^{(i)}, q^{(i)}))] \& \\ \& \forall i (i \leq n + 1 \Rightarrow \bar{P}(n + 1, q^{(i)}, i)).$$

Следующее определение играет важную роль при определении импликаций. Мы строим индуктивно предикат $N(\xi)$ (« ξ — кортежная сеть»), некоторые связанные с ξ числа ($B(\xi)$ — ширина, $D(\xi)$ — глубина, $O(\xi)$ — порядок ξ), а также предикаты $C(s, \xi)$ (« s — компонента ξ ») и $E(\xi, \eta)$ (« η — продолжение ξ »). Смысл введения этих понятий состоит в возможности рассматривать сложно устроенные финитные множества кортежей, номера которых s удовлетворяют условию $C(s, \xi)$, где $N(\xi)$.

Определение 7. 1) $N(\xi) = 1$, если $L(\xi) = 1$. При этом $B(\xi) = \xi^{(1)}$, $O(\xi) = 0$, $C(s, \xi) \equiv I(s, \xi^{(0)}, \xi^{(1)})$,

2) $N(\xi)$, если выполнены условия $L(\xi) = 3$, $F(\xi^{(3)})$, а также условие

$$\forall x [I(x, \xi^{(0)}, \xi^{(0)}) \Rightarrow (!\xi^{(3)}(x) \& N(\xi^{(3)}(x)) \& O(\xi^{(3)}(x)) < \\ < \xi^{(2)} \& B(\xi^{(3)}(x) = \xi^{(0)} \& D(\xi^{(3)}(x)) \geq \xi^{(1)})].$$

При этом $B(\xi) = \xi^{(0)}$, $D(\xi) = \xi^{(1)}$, $O(\xi) = \xi^{(2)}$, $C(s, \xi) \equiv \exists x (I(x, \xi^{(0)}, \xi^{(1)}) \& C(s, \xi^{(3)}(x) \& \nabla (x, s))$;

3) Если $N(\xi)$ и $N(\eta)$ и если $O(\xi) = 0$, то

$$E(\xi, \eta) \equiv B(\xi) < B(\eta) \& D(\xi) = D(\eta) \& O(\eta) = 0;$$

4) Если $N(\xi)$ и $N(\eta)$, и если $O(\xi) \neq 0$, то

$$E(\xi, \eta) \equiv B(\xi) < B(\eta) \& D(\xi) = D(\eta) \& O(\xi) = O(\eta) \& \Delta(\xi^{(3)}, \eta^{(3)}).$$

Все понятия в этом определении примитивно-рекурсивны.

Определение 8 (импликация $\supset_\alpha$ порядка α , где α — ординал $< \epsilon_0$). Проблема $\mathfrak{R} = \mathfrak{P} \supset_\alpha \mathfrak{Q}$ соответствует предикат $R(n, p, q)$, исти-

ность которого для заданных n, p, q означает выполнение 5 условий:

- 1) $\forall i [i \leq n \Rightarrow (N(p^{(0, i)}) \& O(p^{(0, i)}) \leq \bar{\alpha} \& B(p^{(0, i)}) = n \& F(p^{(1, i)}) \& \& A_s(C(s, p^{(0, i)}) \Rightarrow !p^{(1, i)}(s)))]$;
- 2) $\forall i (i \leq n + 1 \Rightarrow (N(q^{(0, i)}) \& O(q^{(0, i)}) \leq \bar{\alpha} \& B(q^{(0, i)}) = n + 1 \& F(q^{(1, i)}) \& V_s(C(s, q^{(0, i)}) \Rightarrow !q^{(1, i)}(s)))]$;
- 3) $\forall i [i \leq n \Rightarrow (E(p^{(0, i)}, q^{(0, i)}) \& \Delta(p^{(1, i)}, q^{(1, i)}))]$;
- 4) $\forall i \forall s (i \leq n + 1 \& C(s, q^{(0, i)}) \& P(s) \Rightarrow \bar{Q}(i, q^{(1, i)}(s)))$;
- 5) $\forall i \forall j \forall s \forall t [i < j \leq n + 1 \& C(s, q^{(0, i)}) \& C(t, q^{(0, j)}) \& \bar{P}(s) \& \bar{P}(t) \& (\nabla(s, t) \vee \nabla(t, s)) \Rightarrow \nabla(q^{(1, i)}(s), q^{(1, j)}(t))]$.

Легко видеть, что для любых л.ф.п. $\mathfrak{F}$ и $\mathfrak{D}$ 1) $\mathfrak{F} \supset_0 \mathfrak{F}$ разрешима; 2) Если $\alpha < \beta < \varepsilon_0$ и если f — решение $\mathfrak{F} \supset_\alpha \mathfrak{D}$, то f будет также решением $\mathfrak{F} \supset_\beta \mathfrak{D}$.

Теорема 1. Пусть $\mathfrak{F}$ и $\mathfrak{D}$ — л.ф.п. и пусть f — решение $\mathfrak{F}$, g — решение $\mathfrak{F} \supset_\alpha \mathfrak{D}$ при некотором $\alpha < \varepsilon_0$.

Тогда из f и g может быть построено решение h для $\mathfrak{D}$ посредством примитивно-рекурсивных операций и одной операции рекурсии до α , представляющей определение некоторой функции φ в следующей форме: $\varphi(0, s) = \psi(s)$, $\varphi(a + 1, s) = \varphi(\theta(a, s), \chi(a, s))$, где ψ, θ и χ — заданные функции, причем

$$\forall a \forall s [(a + 1 \leq \bar{\alpha} \Rightarrow \theta(a, s) < a + 1) \& \theta(a, s) \leq \bar{\alpha}].$$

В доказательстве используется также индукция до α , но в такой форме, что ее обоснование сводится к обоснованию указанной рекурсии (т. е. в конечном счете утверждения о том, что всякая эффективно заданная убывающая последовательность ординалов, начинающаяся с α , обрывается на конечном числе шагов).

Определение 9 (отрицание $\neg_\alpha$ порядка α). Л.ф.п. $\neg_\alpha \mathfrak{F}$ есть $\mathfrak{F} \subset_\alpha \mathfrak{F}^0$, где $\mathfrak{F}^0$ — л.ф.п. без свободных переменных, для которой предикат $P^0(n, p, q)$ тождественно ложен.

Теорема 2. Существуют примитивно-рекурсивные функции $U_1(n, a, b, c)$, $U_i(n, a)$ ($2 \leq i \leq 4$), $U_j(n, x, a)$ ($5 \leq j \leq 6$), для которых справедливо следующее. Определим л.ф.п. $\mathfrak{Z}_i$ ($1 \leq i \leq 6$), как указано ниже, где $\mathfrak{F}, \mathfrak{D}, \mathfrak{R}, \mathfrak{S}$ — любые л.ф.п. без свободных переменных, $\mathfrak{F}(x)$ — любая л.ф.п. с единственной свободной переменной x , α, β, γ — ординалы $< \varepsilon_0$:

$$\mathfrak{Z}_1 = (\mathfrak{R} \supset_\alpha \mathfrak{F}) \& (\mathfrak{R} \& \mathfrak{D} \supset_\gamma \mathfrak{S}) \supset_0 (\mathfrak{R} \& (\mathfrak{F} \subset_\beta \mathfrak{D}) \supset_0 \mathfrak{S}),$$

$$\text{где } \delta = ((1 + \alpha + 1)(\beta + 1) + 1)\gamma + (1 + \alpha + 1)(\beta + 1),$$

$$\mathfrak{Z}_2 = (\mathfrak{R} \& \mathfrak{F} \supset_\alpha \mathfrak{D}) \supset_0 (\mathfrak{R} \supset_\alpha (\mathfrak{F} \supset_\alpha \mathfrak{D})),$$

$$\mathfrak{Z}_3 = \forall x (\mathfrak{R} \supset_\alpha \mathfrak{F}(x)) \supset_0 (\mathfrak{R} \supset_\alpha \forall x \mathfrak{F}(x)),$$

$$\mathfrak{Z}_4 = \forall x (\mathfrak{R} \& \mathfrak{F}(x) \supset_\alpha \mathfrak{D}) \supset_0 (\mathfrak{R} \& \exists x \mathfrak{F}(x) \supset_\beta \mathfrak{D}),$$

$$\text{где } \beta = \alpha + 1,$$

$$\mathfrak{Z}_5(x) = (\mathfrak{R} \& \mathfrak{F}(x) \supset_\alpha \mathfrak{D}) \supset_0 (\mathfrak{R} \& \forall x \mathfrak{F}(x) \supset_\alpha \mathfrak{D}),$$

$$\mathfrak{Z}_6(x) = (\mathfrak{R} \supset_\alpha \mathfrak{F}(x)) \supset_0 (\mathfrak{R} \subset_\alpha \exists x \mathfrak{F}(x)).$$

Тогда функция $f_1(n) = U_1(n, \bar{\alpha}, \bar{\beta}, \bar{\gamma})$ является решением $\mathfrak{Z}_1$, функция $f_i(n) = U_i(n, \bar{\alpha})$ является решением $\mathfrak{Z}_i$ при $2 \leq i \leq 4$, а функция $f_j(n, x) = U_j(n, x, \bar{\alpha})$ является решением $\mathfrak{Z}_j(x)$ при $5 \leq j \leq 6$.

Замечание 1. Утверждения, относящиеся к $\mathfrak{Z}_1 - \mathfrak{Z}_6$, соответствуют правилам введения символов $\supset, \forall$ и $\exists$ в исчислении Генцена LJ (см. (3)). Мы опустили формулировку свойств операций над л.ф.п., соответствующих остальным правилам — они либо более элементарны, либо могут быть легко получены из предыдущих.

Рассмотрим класс арифметических формул. Любая такая формула Φ строится посредством логических операций из элементарных формул, т. е. формул вида $t_1 = t_2$, где t_1 и t_2 — термы (4). Поставим в соответствие каждой элементарной подформуле $\Phi_i(x_1, \dots, x_m)$ формулы Φ некоторую л.ф.п. $\mathfrak{F}_i$, определив предикат P_i из условия $P_i(n, p, q, x_1, \dots, x_m) \equiv \Phi_i(x_1, \dots, x_m)$, где Φ_i понимается как (примитивно-рекурсивный) предикат.

Если теперь каждому вхождению $\supset$ или $\neg$ в Φ приписать некоторый ординал $\alpha < \varepsilon_0$ и заменить это вхождение на $\supset_\alpha$ (соответственно $\neg_\alpha$), то полученное выражение можно понимать, в согласии с определением операций над л.ф.п., как некоторую л.ф.п. $\mathfrak{F}$. Обозначим через $\{\Phi\}_\alpha^\beta$ л.ф.п. $\mathfrak{F}$, полученную из Φ заменой каждого отрицательного вхождения $\supset$ или $\neg$ на $\supset_\alpha$ (соответственно $\neg_\alpha$), а каждого положительного — на $\supset_\beta$ (соответственно $\neg_\beta$).

Определение 10. Пусть $\rho \leq \varepsilon_0$. Арифметическая формула $\Phi(x_1, \dots, x_k)$ обладает ρ -свойством, если существует такая примитивно-рекурсивная функция $A(a)$ и общерекурсивная функция $V(n, x_1, \dots, x_k, a)$, что $\forall \alpha (\alpha < \rho \Rightarrow A(\bar{\alpha}) < \bar{\rho})$ и при каждом $\alpha < \rho$ функция $f_\alpha(n, x_1, \dots, x_k) = V(n, x_1, \dots, x_k, \bar{\alpha})$ является решением л.ф.п. $\{\Phi\}_\alpha^{\beta(\alpha)}$, где $\beta(\alpha)$ — ординал с номером $A(\bar{\alpha})$.

Интуиционистская выводимость арифметической формулы Φ (см. (4)) эквивалентна выводимости секвенции $\rightarrow \Phi$ в исчислении Генцена LJ , расширенного путем присоединения равенства $=$, арифметических термов и аксиом вида $\Gamma_1 \rightarrow \Gamma_2$, где Γ_1 и Γ_2 содержат только элементарные формулы, а также правила индукции: если $\Gamma, \Phi(x) \rightarrow \Phi(x')$ то $\Gamma, \Phi(0) \rightarrow \Phi(t)$ (Γ не содержит свободно x). Обозначим это арифметическое исчисление через Z .

Теорема 3. Пусть $\Phi(x_1, \dots, x_k)$ — интуиционистски выводимая формула арифметики и пусть $\gamma < \varepsilon_0$ — порядок вывода в Z секвенции $\rightarrow \Phi$ (см. (2)).

Тогда Φ обладает ε_0 -свойством, причем в качестве $V(n, x_1, \dots, x_k, a)$ можно взять функцию, примитивно-рекурсивную относительно некоторой функции $\varphi(c, s)$, заданной посредством рекурсии по γ следующего вида: $\varphi(0, s) = \psi(s)$, $\varphi(c+1, s) = \pi(c, s, \varphi(\theta(c, s), \chi(c, s)))$, где ψ, π, θ и χ примитивно-рекурсивны и $\forall c \forall s [(c+1 \leq \bar{\gamma} \Rightarrow \theta(c, s) < c+1) \& \& \theta(c, s) \leq \bar{\gamma}]$.

Эта теорема доказывается методом редукции вывода, открытым Генценом (2), с использованием теоремы 2.

Существует формула Φ (притом не содержащая вхождений $\supset$ или $\neg$) такая, что формула $\Phi \vee \neg \Phi$ не обладает ε_0 -свойством. С другой стороны, можно указать пример такой формулы Φ_1 , что для любого предельного ординала $\rho \leq \varepsilon_0$ Φ_1 обладает ρ -свойством и $\neg \Phi_1$ обладает ρ -свойством. Этот факт означает, в частности, что утверждение «если Φ_1 и $\Phi_1 \supset \Phi_2$ обладают ρ -свойством, то Φ_2 обладает ρ -свойством» не всегда верно. Можно показать однако, что оно верно в том случае, когда Φ_1 не содержит отрицательных вхождений $\supset$ или $\neg$.

Приведем еще один результат, который получается с помощью теорем 1 и 2. Рассмотрим систему арифметики Z^* , отличающуюся от Z тем ограничением на правила сечения и индукции, что в применениях этих правил формула сечения (соответственно формула индукции) не должна содержать отрицательных вхождений $\supset$ или $\neg$. Пусть $\omega_1 = \omega^\omega$, $\omega_2 = \omega^{\omega_1}$, где $\omega_2 = \omega^\omega$.

Теорема 4. Если секвенция $\rightarrow \Phi$ выводима в Z^* , то существует такой ординал $\rho < \omega_1$, что формула Φ обладает ρ -свойством. Соответствующая функция V может быть построена посредством примитивных рекурсий и некоторого числа рекурсий до ρ , имеющих вид, указанный в теореме 1 (с ρ в качестве a).

Математический институт им. В. А. Стеклова
Академии наук СССР
Москва

Поступило
25 VIII 1971

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

- ¹ A. N. Kolmogoroff, Math. Zs., 35, № 1, 58 (1932). ² G. Gentzen, Forschungen zur Logik, Neue Folge, H. 4, 19 (1939). ³ G. Gentzen, Math. Zs., 39, H. 2, 176 (1935). ⁴ S. C. Kleene, Introduction to Metamathematics, N. Y.—Toronto, 1952.