П Р И К Л А Д Н А Я   Л О Г И К А
(Вычислительные системы)
1986 год   Выпуск 116

УДК 510.25

ВЫЧИСЛИМЫЕ ФУНКЦИИ И ПРИНЦИП МАРКОВА

А.А. Воронков

Хорошо известно, что по любому доказательству в интуиционистской арифметике НА замкнутой формулы вида $(\forall\bar{x})(\exists y)\ P(\bar{x},y)$ можно эффективно построить общерекурсивную функцию f такую, что для любого набора $\bar{n}$ натуральных чисел имеет место $P(\bar{n},f(\bar{n}))$. В теоретическом программировании в таких случаях говорят, что "программа" f, удовлетворяющая "спецификации" $P(\bar{x},y)$, извлекается, или синтезируется из доказательства. При этом сразу, естественно, возникает ряд интересных как для математической логики, так и для программирования вопросов: какой класс рекурсивных функций можно извлечь из доказательств в арифметике или ее расширениях? Что нужно добавить в НА, чтобы таким образом получить <u>все</u> рекурсивные функции? и т.д. Изучению таких вопросов и посвящена эта статья.

Введем некоторые обозначения. Через $\mathcal{O}^n$ обозначим множество n-местных общерекурсивных функций, через $\mathfrak{N} = \langle N, 0, ', +, \cdot, = \rangle$ - стандартную модель арифметики. Для записи кортежей $x_0,\ldots,x_n$ часто будем использовать сокращение $\bar{x}$. Соответствующим образом понимаются кванторы $(\forall\bar{x})$ и $(\exists\bar{x})$.

Аксиоматика НА и стандартный алгоритм α извлечения программ из доказательств в НА формул вида $(\forall\bar{x})(\exists y)\ P(\bar{x},y)$ приведены, например, в [1] и [2]. Говоря о разрешимости в НА формулы P, мы будем подразумевать, что $\vdash_{HA} P \vee \neg P$. Таким образом, например, любая бескванторная формула арифметики разрешима в НА.

Докажем

ПРЕДЛОЖЕНИЕ 1. *Пусть П - множество доказательств в НА замкнутых формул вида $(\forall\bar{x})(\exists y)\ P(\bar{x},y)$ и α - стандартный алгоритм сопоставления каждому та-*

кому доказательству общерекурсивной функции f такой, что имеет место $\mathfrak{N} \vDash (\forall \bar{x})\ P(\bar{x}, f(\bar{x}))$. Тогда существует $f \in \mathcal{O}$ такая, что f не принадлежит области значений α.

ДОКАЗАТЕЛЬСТВО. Достаточно заметить, что по гёделевской нумерации доказательств из Π можно построить вычислимую нумерацию множества $\alpha(\Pi)$. В то же время хорошо известно [3], что класс всех общерекурсивных функций не имеет вычислимой нумерации.

Предложение I говорит о том, что, пользуясь только интуиционистской арифметикой, невозможно извлечь из доказательств все рекурсивные функции. Более того, аналогичное утверждение имеет место для любого перечислимо-аксиоматизируемого расширения НА, обладающего свойством извлечения программ из доказательств. Поэтому если мы хотим извлекать из доказательств все вычислимые функции, то в понятие доказательства следует включать некоторые принципы неалгоритмического характера.

Для того чтобы определить, что же требуется добавить к интуиционистской арифметике для получения всех общерекурсивных функций, обратимся к определению рекурсивной функции [4]. Единственный неконструктивный момент в этом определении заключается в использовании μ-оператора

$f(\bar{x}) = \mu y[g(\bar{x}, y) = 0]$ при условии, что для любого набора $\bar{m} \in N$ существует $n \in N$ такой, что $g(\bar{m}, n) = 0$,

так как нет алгоритма, проверяющего это условие.

Оказывается, логический принцип, аналогичный использованию μ-оператора, в конструктивной логике уже известен. Это так называемый принцип Маркова [5]:

$$\frac{\neg\neg(\exists y)\ P(\bar{x}, y) \quad P(\bar{x}, y) \vee \neg P(\bar{x}, y)}{(\exists y)\ P(\bar{x}, y)},$$

интуитивно означающий, что свойство остановки алгоритма можно доказывать от противного. Имеется более сильная форма этого принципа, основанная на смешанных классически-конструктивных исчислениях:

$$\frac{\vdash_{cl} (\exists y) P(\bar{x}, y) \quad \vdash_{con} P(\bar{x}, y) \vee \neg P(\bar{x}, y)}{\vdash_{con} (\exists y) P(\bar{x}, y)},$$

где $\vdash_{cl}$ и $\vdash_{con}$ означают соответственно классическую и конструктивную выводимости.

Тем не менее, как видно из доказательства предложения I, ни одного из этих принципов недостаточно для получения всех общерекурсивных функций из доказательств как в НА, так и в любом ее перечислимом расширении. В случае арифметики, как показано в [6], эти правила даже консервативно расширяют НА.

В [7] предложена другая, более сильная формулировка принципа Маркова:

$$\frac{\mathfrak{N} \models (\forall \bar{x})(\exists y)P(\bar{x},y) \quad P(\bar{x},y) \vee \neg P(\bar{x},y)}{(\exists y)P(\bar{x},y)} .$$

Назовем это правило вывода семантическим принципом Маркова. Обозначим систему, полученную из НА добавлением семантического принципа Маркова, через НАМР. В [7] доказана конструктивность этого принципа (даже в более общей формулировке, годной не только для арифметики), которая основана на следующем алгоритме получения по любым $\bar{m}$ такого n, что $P(\bar{m},n)$: пользуясь $P(\bar{m},y) \vee \vee \neg P(\bar{m},y)$, проверяем по очереди $P(\bar{m},0), P(\bar{m},1), \ldots,$ пока не встретится n такой, что $P(\bar{m},n)$ (то, что такой n всегда найдется, гарантируется условием $\mathfrak{N} \models (\forall \bar{x})(\exists y)\, P(\bar{x},y)$). Сам вид приведенного алгоритма показывает, что применение семантического принципа Маркова в точности соответствует получению общерекурсивной функции с помощью μ-оператора.

Теперь перейдем к формальному доказательству того, что из доказательств в НАМР могут быть извлечены в точности все общерекурсивные функции.

Вначале сформулируем теорему об извлечении программ из доказательств в НАМР.

Пусть $\nu\colon \mathbb{N} \to S$ – гёделевская нумерация [3] множества конечных последовательностей формул арифметики. Не ограничивая общности, можно считать, что все доказательства в НАМР являются такими последовательностями (при этом мы считаем, что принцип Маркова записывается в виде

$$\frac{P(\bar{x},y) \vee \neg P(\bar{x},y)}{(\exists y)P(\bar{x},y)}$$

при условии, что $\mathfrak{N} \models (\forall \bar{x})(\exists y)P(\bar{x},y)$). Пусть $\mathbb{K} = (Ч, \varkappa)$ – нумерованное множество всех (не только одноместных) частично рекурсивных функций.

ТЕОРЕМА I. Существует общерекурсивная функция $g: N \to N$ такая, что как только νn является доказательством в НАМР замкнутой формулы вида $(\forall \bar{x})(\exists y) P(\bar{x},y)$, то функция $\varkappa g(n)$ общерекурсивна и для любого набора натуральных чисел $\bar{m}$ имеет место $P(\bar{m},(\varkappa g(n))(\bar{m}))$.

Доказательство см. в [7].

Теорему I можно сформулировать иначе: существует морфизм нумерованных множеств (S,ν) и $\mathbb{K}$, строящий по любому доказательству П формулы указанного вида программу f, удовлетворяющую условию $P(\bar{x},f(\bar{x}))$.

Докажем ряд вспомогательных утверждений. Введем обозначение $x \le y \rightleftharpoons (\exists z)(x+z=y)$.

ЛЕММА I. Следующие формулы выводимы в НА:

а) $x \le y \vee y \le x$;

б) $x \le y \,\&\, y \le z \to x \le z$;

в) $x \le y \,\&\, y \le x \to x = y$;

г) $x \le y \to x + z \le y + z$;

д) $x \le y \to x \cdot z \le y \cdot z$.

Доказательство очевидно.

Определим предикат $C(x,y,z)$ следующим образом:

$$C(x,y,z) \rightleftharpoons (x+y)\cdot(x+y) + 3\cdot x + y = 2\cdot z.$$

Этот предикат представляет стандартную нумерацию пар натуральных чисел [4].

ЛЕММА 2. Следующие формулы выводимы в НА:

а) $(\forall x)(\forall y)(\exists z)\, C(x,y,z)$;

б) $C(x,y,z) \,\&\, C(x,y,u) \to z = u$;

в) $(\forall z)(\exists x)(\exists y) C(x,y,z)$;

г) $C(x,y,z) \,\&\, C(u,v,z) \to x = u \,\&\, y = v$.

ДОКАЗАТЕЛЬСТВО. Пункты "а" и "б" очевидны. Применяя индукцию по z, сводим "в" к

$$(\exists x)(\exists y)C(x,y,0) \qquad (1)$$

и

$$(\exists x)(\exists y)C(x,y,z) \to (\exists u)(\exists v)C(u,v,z'). \tag{2}$$

Доказательство (I) очевидно; (2) сводится к

$$C(x,y,z) \to (\exists u)(\exists v)C(u,v,z'). \tag{3}$$

Пользуясь разрешимостью в НА равенства, доказываем (3) разбором случаев по $y = 0 \vee y \neq 0$,

$$x \cdot x + 3 \cdot x = 2 \cdot z \to (\exists u)(\exists v)C(u,v,z'), \tag{4}$$

$$y \neq 0 \to (C(x,y,z) \to (\exists u)(\exists v)C(u,v,z')). \tag{5}$$

Формула (4) выводится из

$$x \cdot x + 3 \cdot x = 2 \cdot z \to C(0,x',z'). \tag{6}$$

Чтобы показать (5), находим, используя $y \neq 0$, такой w, что $w' = y$. После этого (5) выводится из

$$w' = y \to (C(x,y,z) \to C(x',w,z')). \tag{7}$$

Формулы (6) и (7) доказываются тривиально.

Перейдем к доказательству п. "г". Достаточно показать, что

$$(x+y) \cdot (x+y) + 3 \cdot x + y = (u+v) \cdot (u+v) + 3 \cdot u + v \to x = u \;\&\; y = v. \tag{8}$$

Будем доказывать (8) разбором случаев по $x+y \leq u+v \vee u+v \leq x+y$ (см. лемму I). В силу симметрии достаточно рассмотреть только первый случай:

$$x+y \leq u+v \to ((x+y) \cdot (x+y) + 3 \cdot x + y = (u+v) \cdot (u+v) + 3 \cdot u + v \to x = u \;\&\; y = v). \tag{9}$$

Это сводится к

$$x+y+z = u+v \to ((x+y) \cdot (x+y) + 3 \cdot x + y = (u+v) \cdot (u+v) + 3 \cdot u + v \to x = u \;\&\; y = v). \tag{10}$$

Формула (I0) доказывается разбором случаев по $z = 0 \vee z \neq 0$. При $z=0$ из посылок (I0) вытекает

$$x + y = u + v. \tag{11}$$

При $z \neq 0$ (I0) сводится к

$$x+y+w' = u+v \to (x+y) \cdot (x+y) + 3 \cdot x + y = (u+v) \cdot (u+v) + 3 \cdot u + v \to x = u \;\&\; y = v. \tag{12}$$

Из посылок (12), применяя лемму 1, доказываем

$$(u+v)\cdot(u+v) + 3\cdot u+v = (x+y)\cdot(x+y) + 3\cdot x+y \le$$
$$\le (x+y)\cdot(x+y) + 3\cdot(x+y) \le (x+y+2)\cdot(x+y) + (x+y) \le$$
$$\le (x+y+1)\cdot(x+y+1) + (x+y) \le (u+v)\cdot(u+v) + (x+y), \tag{13}$$

и, следовательно,

$$(u+v)\cdot(u+v) + 3\cdot u+v \le (u+v)\cdot(u+v) + (x+y) \quad . \tag{14}$$

Из (14) следует $u+v \le x+y$.

Таким образом, в этом случае также получаем $u+v = x+y$. Пользуясь этим равенством, легко доказываем (8).

Определим теперь предикат $C_n(x_0,\dots,x_n)$, $n \ge 2$, представляющий нумерацию n-ок натуральных чисел:

$$C_2(x_0,x_1,x_2) \rightleftharpoons C(x_0,x_1,x_2),$$

$$C_{n+1}(\bar{x},y,z) \rightleftharpoons (\exists u)(C_n(\bar{x},u) \,\&\, C_2(u,y,z)).$$

ЛЕММА 3. Следующие формулы выводимы в НА:

а) $(\forall\bar{x})(\exists y)C_n(\bar{x},y)$;

б) $C_n(\bar{x},y) \,\&\, C_n(\bar{x},z) \to y = z$;

в) $(\forall x)(\exists\bar{y})C_n(\bar{y},x)$;

г) $C_n(\bar{x},z) \,\&\, C_n(\bar{y},z) \to \bar{x} = \bar{y}$.

Доказательство прямо следует из леммы 2.

Перейдем к доказательству основного утверждения.

ТЕОРЕМА 2. Для любой общерекурсивной функции f от k переменных существует формула арифметики $P(\bar{x},y)$ такая, что

$$f(\bar{x}) = y \leftrightarrow \mathfrak{N} \models P(\bar{x},y);$$

$$\vdash_{HAMP} (\forall\bar{x})(\exists y)\, P(\bar{x},y) \quad .$$

ДОКАЗАТЕЛЬСТВО. По основной теореме из [8], существует бескванторная формула арифметики $R(\bar{x},y,\bar{z})$ такая, что для любого набора натуральных чисел $\bar{n},m$ имеет место

$$f(\bar n) = m \Leftrightarrow \mathfrak{N} \models (\exists \bar z)\, R(\bar n, m, \bar z).$$

Пусть l – длина кортежа $\bar z$. Рассмотрим формулу
$Q(\bar x, u) \rightleftharpoons (\exists \bar z)(\exists y)(C_{l+1}(y, \bar z, u) \,\&\, R(\bar x, y, \bar z))$.

Докажем, что в НА выводима формула

$$Q(\bar x, u) \vee \neg Q(\bar x, u) \quad . \tag{15}$$

Для этого достаточно показать выводимость формулы

$$(\exists \bar z)(\exists y)(C_{l+1}(y, \bar z, b) \,\&\, R(\bar a, y, \bar z)) \vee$$

$$\vee \neg (\exists \bar z)(\exists y)(C_{l+1}(y, \bar z, b) \,\&\, R(\bar a, y, \bar z)), \tag{16}$$

где $\bar a, b$ – новые константы.

По лемме 3, в НА выводимо $(\exists \bar z)(\exists y) C_{l+1}(y, \bar z, b)$. Поэтому для доказательства (16) достаточно показать

$$C_{l+1}(c, \bar d, b) \to (\exists \bar z)(\exists y)(C_{l+1}(y, \bar z, b) \,\&\, R(\bar a, y, \bar z)) \vee$$

$$\vee \neg (\exists \bar z)(\exists y)(C_{l+1}(y, \bar z, b) \,\&\, R(\bar a, y, \bar z)). \tag{17}$$

Так как R – бесkванторная формула, то она разрешима в НА и мы можем доказать (17) разбором случаев по $R(\bar a, c, \bar d) \vee \neg R(\bar a, c, \bar d)$. Легко видеть, что для доказательства (17) достаточно вывести в НА

$$C_{l+1}(c, \bar d, b) \,\&\, R(\bar a, c, \bar d) \to (\exists \bar z)(\exists y)(C_{l+1}(y, \bar z, b) \,\&\, R(\bar a, y, \bar z)) \tag{18}$$

и

$$C_{l+1}(c, \bar d, b) \,\&\, \neg R(\bar a, c, \bar d) \to \neg (\exists \bar z)(\exists y)(C_{l+1}(y, \bar z, b) \,\&\, R(\bar a, y, \bar z)). \tag{19}$$

Доказательство формулы (18) очевидно, доказательство (19) сводится к

$$C_{l+1}(c, \bar d, b) \,\&\, (\exists \bar z)(\exists y)(C_{l+1}(y, \bar z, b) \,\&\, R(\bar a, y, \bar z)) \to R(\bar a, c, \bar d). \tag{20}$$

Для доказательства (20) достаточно вывести в НА

$$C_{l+1}(c, \bar d, b) \,\&\, C_{l+1}(r, \bar s, b) \,\&\, R(\bar a, r, \bar s) \to R(\bar a, c, \bar d). \tag{21}$$

По лемме 3, в НА выводимо

$$C_{l+1}(c, \bar d, b) \,\&\, C_{l+1}(r, \bar s, b) \to c = r \,\&\, \bar d = \bar s, \tag{22}$$

и (21) легко следует из (22). Итак, формула (15) доказана.

Так как функция f всюду определена, то

$$\mathcal{N} \models (\forall \bar{x})(\exists y)(\exists \bar{z})R(\bar{x},y,\bar{z}).$$

Из этого следует, что

$$\mathcal{N} \models (\forall \bar{x})(\exists u)Q(\bar{x},u). \qquad (23)$$

Применяя к (15) и (23) семантический принцип Маркова, получаем

$$\vdash_{\text{НАМР}} (\exists u)Q(\bar{x},u). \qquad (24)$$

Возьмем в качестве P формулу $P(\bar{x},y) \rightleftharpoons (\exists u)(\exists \bar{z})(Q(\bar{x},u) \,\&\, \&C_{l+1}(y,\bar{z},u))$. Используя лемму 3 и (24), получаем, что

$$\vdash_{\text{НАМР}} (\forall \bar{x})(\exists y)P(\bar{x},y).$$

Докажем теперь, что P удовлетворяет условию I теоремы 2. В самом деле, из определения формул P,Q,R вытекает эквивалентность следующих утверждений:

а) $f(x) = y$;

б) $\mathcal{N} \models (\exists \bar{z})R(\bar{x},y,\bar{z})$;

в) существует u такое, что u - номер кортежа $(y,\bar{z})$ и $R(\bar{x},y,\bar{z})$;

г) существует u такое, что u - номер некоторого кортежа вида $(y,\bar{z})$ и $Q(\bar{x},u)$;

д) $\mathcal{N} \models P(\bar{x},y)$.

Сделаем несколько замечаний по поводу доказательства теоремы 2. Как известно, у любой общерекурсивной функции существует нормальная форма [4]

$$f(\bar{x}) = l(\mu u(g(\bar{x},u) = 0)), \qquad (\bullet)$$

где g - примитивно-рекурсивная функция. Доказательство теоремы 2 следовало такому виду функции f. Предикат $Q(\bar{x},u)$ из доказательства теоремы 2 представляется предикатом $g(\bar{x},u) = 0$. Применение μ-оператора в $(\bullet)$ соответствовало применению принципа Маркова, а взятие функции l в $(\bullet)$ - переходу от доказательства формулы $(\forall \bar{x})(\exists u)Q(\bar{x},u)$ к доказательству формулы $(\forall \bar{x})(\exists y)P(\bar{x},y)$.

Кроме того, можно заметить, что при доказательстве представимости любой общерекурсивной функции мы использовали только ограниченные формулы индукции. А именно, если ввести в язык арифметики ограниченные кванторы, как это сделано в теории допустимых множеств [9] или в теории списков [10] $(\forall x < y)$ и $(\exists x < y)$, и добавить аксиомы для отношения $<$ (например, как в [11]), то для доказательства теоремы 2 достаточно так называемой Δ_0-индукции, или индукции по Δ_0-формулам [10]. Это еще раз демонстрирует, что семантический принцип Маркова является очень сильным принципом, существенно расширяющим возможности конструктивной логики.

Как показано в [7], любая формула, выводимая в НАМР, конструктивно истинна в стандартной модели арифметики. Остается открытым вопрос, верно ли обратное утверждение, т.е. является ли семантический принцип Маркова достаточно сильным, чтобы с его помощью вывести все конструктивно истинные формулы арифметики?

Автор благодарен А.В.Манциводе и А.П.Косенкову за стимулирующие обсуждения.

Литература

1. КЛИНИ С.К. Введение в метаматематику.–М.: МЛ, 1957, –526 с.
2. PRAWITZ D. Ideas and results in proof theory.– In: Proc. 2-nd Scandinavian logic symposium. Amsterdam, North-Holland, 1971, p.235–308.
3. ЕРШОВ Ю.Л. Теория нумераций.–М.: Наука, 1977. – 416 с.
4. МАЛЬЦЕВ А.И. Алгоритмы и рекурсивные функции.–М.: Наука, 1965.
5. МАРКОВ А.А. Попытка построения логики конструктивной математики. –В кн.: Исследования по теории алгорифмов и математической логике. Т. 2., – М., 1976, с.3–31.
6. NOVIKOFF P.S. On the consistency of certain logic calculus. – Мат.сборник, 1943, т.12, № 2, с.231–261.
7. ВОРОНКОВ А.А. Синтез логических программ. – Препринт ИМ СО АН СССР, № 24, 1986, – 42 с.
8. МАТИЯСЕВИЧ Ю.В. Диофантовость перечислимых множеств.–Докл. АН СССР, 1970, т.191, с. 279–288.
9. BARWISE J. Admissable sets and structures.– Berlin: Springer-Verlag, 1975.
10. ГОНЧАРОВ С.С., СВИРИДЕНКО Д.И. Σ-программирование. –В кн.: Логико-математические аспекты проблемы МОЗ (Вычислительные системы, вып.107). Новосибирск, 1985, с.3–29.
11. ШЕНФИЛД Дж. Математическая логика.–М.: Наука, 1975. –528 с.

Поступила в ред.-изд.отд.
20 июня 1986 года