ИЗВЕСТИЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

1998 МАТЕМАТИКА № 8 (435)

УДК 519.716

В.Д. СОЛОВЬЕВ

ПРОБЛЕМА ПОЛНОТЫ В КЛАССЕ МНОГОЧЛЕНОВ РАЗРЕШИМА

Хорошо известна [1] проблема полноты конечных наборов частично рекурсивных функций и предикатов. Первые полные наборы были приведены в [2]. Полным является, например, набор $\{0, x+1, =\}$. В [3] показано, что проблема полноты алгоритмически неразрешима.

В тех случаях, когда для какого-либо класса объектов некоторая проблема оказывается алгоритмически неразрешимой, обычно стремятся выделить содержательные подклассы этого класса объектов, для которых данная проблема окажется уже разрешимой.

В данном сообщении показывается, что в классе многочленов с целыми коэффициентами проблема полноты разрешима. Так как традиционно частично рекурсивные функции определяются на множестве натуральных чисел N, то и значения многочленов ограничим множеством N. Для произвольного многочлена f с целыми коэффициентами функцию $\overline{f}(x_1,\dots,x_n) = \max(f(x_1,\dots,x_n),0)$ назовем многочленом на N.

Определение 1. Схема программ с массивами и равенством — это конечный ориентированный граф, все вершины которого помечены инструкциями.

Инструкции могут иметь следующий вид: а) старт $(x_1,\dots,x_n)$, б) $y := f(x_1,\dots,x_n)$, в) $y := x$, г) $x = y$, д) $p(x_1,\dots,x_n)$, е) $i := i+1$, ж) $i := 0$, з) $i = j$, и) $M[i] := x$, к) $x := M[i]$, л) стоп (x).

Синтаксис и семантика схем программ стандартны [4].

Класс схем программ из определения 1 обозначим $FDA_=$.

Для набора $\mathcal{L} = \langle f_1,\dots,f_n, p_1,\dots,p_m\rangle$, где $f_1,\dots,f_n$ — функции, $p_1,\dots,p_m$ — предикаты, обозначим через $[\mathcal{L}]_{FDA_=}$ замыкание $\mathcal{L}$ относительно класса $FDA_=$, т. е. множество всех частично рекурсивных функций, вычислимых схемами программ из $FDA_=$ при подстановке функций и предикатов из $\mathcal{L}$ вместо переменных f, p в схемы программ.

Определение 2. Набор $\mathcal{L}$ называется полным (относительно $FDA_=$), если $[\mathcal{L}]_{FDA_=}$ есть множество всех частично рекурсивных функций.

В [5] приведен следующий критерий полноты: $\mathcal{L}$ полон тогда и только тогда, когда

1) $\forall x, y\ \exists \tau$ (τ терм сигнатуры $\mathcal{L}$ & $\tau(x) = y$),

2) $\exists a\ \exists \Phi$ (Φ бескванторная формула сигнатуры $\mathcal{L} \cup \{=\}$ & $\Phi(a)$ & $\forall y \neq a \neg\Phi(y)$).

Используем его для получения следующего результата.

Теорема. *Существует алгоритм, который по любому конечному набору многочленов на N определяет, является ли он полным в функциональной системе $\langle \mathcal{F}_0, FDA_=\rangle$.*

Доказательство. Пусть дан набор $\mathcal{L}$ многочленов. Допустим, что $\mathcal{L}$ не содержит ни одного линейного многочлена $ax+b$ с $a > 0$. Легко видеть, что для любого многочлена на N степени 2 и выше и любого многочлена $ax+b$, $a \le 0$, доля чисел отрезка $[0,\dots,n]$, являющихся значениями этих многочленов, стремится к 0 с ростом n. Отсюда следует, что не все натуральные числа являются значениями многочленов из $\mathcal{L}$ и, значит, $\mathcal{L}$ не полон, т. к. не выполняется условие 1) критерия полноты.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, гранты 93-011-16004, 98-01-00900.

Для набора $\mathcal{L}$ возможны два случая:

а) $\mathcal{L}$ содержит некоторый многочлен вида $ax+k$, $a>1 \vee a=1 \ \&\ k>0$, и не содержит многочленов вида $x-l$, $l>0$,

б) $\mathcal{L}$ содержит некоторый многочлен вида $x-l$, $l>0$.

Рассмотрим а). Пусть $a_1x+b_1,\dots,a_px+b_p$ — все многочлены набора $\mathcal{L}$ указанного вида ($a_1,\dots,a_p>0$). Если $\mathcal{L}$ не содержит ни многочлена 0 и ни одного многочлена, старший коэффициент которого отрицателен, то найдется такое достаточно большое число x_0, что $\forall f \in \mathcal{L}$ $\forall y \geq x_0$ $(f(y) \geq y)$ и, следовательно, условие 1) критерия полноты не выполняется, например, для пары чисел $\langle x_0, 0\rangle$. В этом случае $\mathcal{L}$ не полон.

Пусть $g \in \mathcal{L}$ и старший коэффициент многочлена g отрицателен. Тогда найдется число x_0 такое, что $\forall y \geq x_0$ $(g(y)=0)$ — в соответствии с определением многочленов на N.

Вычислим значения всех многочленов из $\mathcal{L}$ на числе 0. Если все они равны 0, то $\mathcal{L}$ не полон, т. к. не выполняется условие 1) критерия полноты.

Если среди них есть отличные от 0, то пусть x_1 — корень уравнения $a_1x+b_1=x$. Если x_1 — натуральное число, то вычислим значение всех многочленов из $\mathcal{L}$ на числе x_1. Если окажется, что или все они равны x_1 или все они принадлежат множеству $\{0,x_1\}$ и, кроме того, все значения многочленов из $\mathcal{L}$ на 0 также принадлежат множеству $\{0,x_1\}$, то $\mathcal{L}$ не полон, т. к. не выполняется условие 1) критерия полноты.

В противном случае, пусть $h \in \mathcal{L}$ таково, что $h(x_1) \neq x_1$ и $h(x_1) \neq 0$ или (если такого h не существует) пусть $h_1, h_2 \in \mathcal{L}$ и $h_1(x_1)=0 \ \&\ h_2(0) \neq x_1 \ \&\ h_2(0) \neq 0$. Покажем, как может быть вычислена константа 0. Для входа x вычисляем $y=f(x)=a_1x+b_1$. Если окажется, что $y=x$, то это возможно лишь в двух случаях – когда $y=x=x_1$ и когда $y=x=0$ (при $b_1<0$, по определению многочленов на N). В этом случае вычисляем $z=h(x)$ либо $z=h_2h_1(x)$. По выбору функций h, h_1, h_2 имеем $z \neq 0 \ \&\ z \neq x_1$. Если окажется, что $y=a_1x+b_1 \neq x$, то полагаем $z=y$.

Если $b_1 \geq 0$, то $f^{x_0}(z) \geq x_0$. Если $b_1<0$ и $z>x_1$, то $f(z)>z$ и $f^{x_0}(z) \geq x_0$. Если $b_1<0$ и $z<x_1$, то $f(z)<z$ и $f^{\max(x_0,x_1)}(z)=0$, причем $f^{\max(x_0,x_1)}(z)=f^{\max(x_0,x_1)+1}(z)$. Это позволяет вычислить константу 0 следующим образом: вычисляем $f^{\max(x_0,x_1)+1}(z)$. Если окажется, что $f^{\max(x_0,x_1)}(z)=f^{\max(x_0,x_1)+1}(z)$, то $f^{\max(x_0,x_1)}(z)=0$ и подаем это значение на выход. В противном случае $f^{\max(x_0,x_1)+1}(z)>f^{x_0}(z) \geq x_0$ и $g(f^{\max(x_0,x_1)+1}(z))=0$ по выбору многочлена g. Значение $g(f^{\max(x_0,x_1)+1}(z))$ подаем на выход.

Далее выясним, какие числа могут быть получены из числа 0 посредством суперпозиции многочленов из $\mathcal{L}$. Рассмотрим совокупность линейных многочленов, содержащихся в $\mathcal{L}$: $a_1x+b_1,\dots,a_px+b_p$. Пусть $a=$ Н.О.К. $(a_1,\dots,a_p)$. Линейный многочлен a_ix+b_i $(i<p)$ имеет то же множество значений, что и совокупность многочленов: $ax+b_i, ax+(b_i+a_i),\dots,ax+(b_i+a_i\cdot(a/a_i-1))$. Пользуясь этим, заменяем исходную совокупность $a_1x+b_1,\dots,a_px+b_p$ на приведенную совокупность линейных многочленов с одинаковыми коэффициентами при x.

Если свободные члены многочленов приведенной совокупности не образуют полную систему вычетов по модулю a, то по меньшей мере $1/a$ часть N не покрывается значениями многочленов из приведенной совокупности. Аналогично тому, как это было показано в начале доказательства теоремы, не все натуральные числа являются значениями каких-либо многочленов из $\mathcal{L}$, и, значит, $\mathcal{L}$ не полон.

Если же свободные члены образуют полную систему вычетов по модулю a, то найдется такое число n (напр., максимальный элемент из свободных членов приведенной совокупности и числа a), что из чисел интервала $[0,n]$ применением (возможно многократным) многочленов приведенной совокупности могут быть получены все натуральные числа, большие n.

Остается решить вопрос: все ли числа интервала $[0,n]$ могут быть получены из числа 0 применением (многократным) многочленов набора $\mathcal{L}$?

Так как в $\mathcal{L}$ по предположению отсутствуют многочлены вида $x-l$ $(l>0)$, то найдется такое число $n'>n$, что $\forall y \geq n'$ $\forall g \in \mathcal{L}$ $(g(y) \geq y)$. Отсюда следует, что рано или поздно остановится следующий алгоритм: применяем к числу 0 многочлены из $\mathcal{L}$, к тем из получившихся чисел, которые меньше n' и $\neq 0$, вновь применяем многочлены из $\mathcal{L}$ и так далее, пока применением к ранее вычислившимся числам, меньшим n', какого-либо многочлена из $\mathcal{L}$, получаются новые числа, меньшие n'. Если в результате его работы вычислятся все числа интервала $[0, n]$, то выполнено условие 1) критерия полноты и $\mathcal{L}$ полон, в противном случае $\mathcal{L}$ не полон. Случай а) разобран.

б). Пусть многочлен $f(x) = x - l$ $(l > 0)$ принадлежит $\mathcal{L}$. Используя его, легко вычислить константу 0, циклически применяя к входу x многочлен $f(x)$ до тех пор, пока не окажется $f^n(x) = f^{n+1}(x)$. Это равенство возможно лишь в случае, когда $f^n(x) = 0$. Значение $f^n(x)$ подаем на выход — условие 2) критерия полноты выполнено.

Проверим, имеет ли место равенство $N = \{\tau(0) \mid \tau$ — терм сигнатуры $\mathcal{L}\}$, обеспечивающее выполнение первого условия критерия полноты.

Пусть $x - l_1, \ldots, x - l_q$ — все многочлены набора $\mathcal{L}$ вида $x - l$ с $l > 0$ и $r = \text{Н.О.Д.}\,(l_1, \ldots, l_q)$. Из теории чисел известно, что $\exists t\ \forall y \geq t\ \exists b_1, \ldots, b_q \geq 0\ \left(yr = \sum\limits_{i=1}^{q} b_i l_i\right)$. Отсюда следует, что если некоторое множество чисел содержит сколь угодно большие числа, дающие при делении на r остаток d, то из чисел этого множества применением функций $x - l_1, \ldots, x - l_q$ можно получить все числа, дающие при делении на r остаток d.

Вычислим значения по модулю r всех многочленов из $\mathcal{L}$ на числах $0, \ldots, r-1$. Построим граф с r вершинами, помеченными числами $0, \ldots, r-1$; вершины, помеченные числами i и j, соединим стрелкой, ведущей от i к j, если в $\mathcal{L}$ найдется такой многочлен h, что $h(i) = j \pmod r$.

Если в получившемся графе не все вершины достижимы из вершины с меткой 0, то набор $\mathcal{L}$ не полон. В противном случае продолжим анализ. Пусть x_0 — такое число, что для любого многочлена g из $\mathcal{L}$, за исключением многочленов $x - l_1, \ldots, x - l_q$ $\forall y \geq x_0\ (g(y) = 0 \vee g(y) > y)$ (в зависимости от знака коэффициента при старшем члене).

Рассмотрим последовательность множеств $M_0, M_1, \ldots$ $M_0 = \{0\}$, $M_1 = \{y \mid \exists x, d\ \exists f \in \mathcal{L}\ (f(0) = xr + d\ \&\ y \leq xr + d\ \&\ y \equiv d \pmod r)\}$, $M_2 = \{y \mid \exists z \in M_1\ \exists x, d\ \exists f \in \mathcal{L}\ (f(z) = xr + d\ \&\ y \leq xr + d\ \&\ y \equiv d \pmod r)\} \ldots$

Существует такое число n, что $M_{n+1} \cap [0, \ldots, x_0] = M_n \cap [0, \ldots, x_0]$ и $\forall y \geq x_0\ (y \in M_{n+1} \to \exists y' \geq x_0\ (y' \in M_n\ \&\ y' \equiv y \pmod r)))$. Это следует из конечности отрезка $[0, \ldots, x_0]$ и числа классов вычетов по модулю r. Те же свойства будут выполняться и для любого n', большего n.

Эффективно порождая последовательность $M_0, M_1, \ldots$, найдем такое число n и множество M_n. Если $M_n \cap [0, \ldots, x_0] \neq [0, \ldots, x_0]$ или среди чисел M_n, бо̀льших x_0, присутствуют представители не всех классов вычетов по модулю r, то набор $\mathcal{L}$ не полон, т. к. не выполняется условие 1) критерия полноты.

Итак, остается разобрать случай, когда для каждого класса вычетов по модулю r в множестве M_n найдется число из этого класса вычетов, большее x_0. Рассмотрим ранее построенный граф. В нем есть цикл (ориентированный), ведущий из вершины с пометкой 0 в нее же — это следует из того, что M_n содержит число, большее x_0 и делящееся на r.

Пусть x' — число из множества M_n, большее x_0 и делящееся на r. Применяя к x' функции из $\mathcal{L}$ в соответствии с ребрами ранее указанного цикла, получим число, также делящееся на r и строго большее x' (по определению x_0). Эту операцию можно применять сколько угодно раз и, таким образом, множество $S = \{\tau(0) \mid \tau$ — терм сигнатуры $\mathcal{L}\}$ будет содержать сколь угодно большие числа, делящиеся на r.

Но по ранее сделанному предположению из вершины с пометкой 0 достижимы все остальные вершины. Применяя к числам из S, бо̀льшим x_0 и делящимся на r, функции из $\mathcal{L}$ в соответствии с ребрами, ведущими из вершины с пометкой 0 в остальные вершины, получим и сколь угодно большие числа в множестве S, принадлежащие каждому из классов вычетов по модулю r. По выше доказанному отсюда следует, что $S = N$ и набор $\mathcal{L}$ полон, т. к. выполнены и первое, и второе условия критерия полноты.

Это завершает эффективную проверку условий критерия полноты для набора $\mathcal{L}$. $\square$

Литература

1. Ершов А.П., Ляпунов А.А. *О формализации понятия программы* // Кибернетика. – 1967. – № 5. – С. 40–57.
2. Ершов А.П. *Операторные алгоритмы.* I // Проблемы кибернетики. – М.: Физматгиз, 1962. – № 3. – С. 5–48.
3. Заславский И.Д. *Граф-схемы с памятью* // Тр. Матем. ин-та АН СССР. – 1964. – Т. 74. – С. 99–192.
4. Котов В.Е., Сабельфельд В.К. *Теория схем программ.* – М.: Наука, 1991. – 247 с.
5. Соловьев В.Д. *Алгебраические аспекты абстрактной теории вычислимости* // Матем. вопр. кибернетики. – М.: Наука, 1991. – Вып. 3. – С. 233–256.

Казанский государственный университет

Поступила 29.12.1995