

Алгоритмическая неразрешимость задачи о нахождении базиса конечной полной системы полиномов с целыми коэффициентами

Н. Ф. Алексиадис (НИУ «МЭИ», Москва)

В настоящей статье доказано, что не существует алгоритма, с помощью которого из конечной полной системы полиномиальных функций с целыми коэффициентами можно было бы выделить базис.

Ключевые слова: полином, алгоритм, неразрешимость, проблема полноты, базис, операции суперпозиций, функциональная система, 10-я проблема Гильберта.

Сведения из теории функциональных систем, необходимые для дальнейшего изложения приведены в [1]. При изложении материала используется терминология книг [2] и [4].

Для удобства изложения полагаем, что $0^0 = 1$.

Z — множество всех целых чисел.

P_Z — множество всех полиномиальных функций с целыми коэффициентами, аргументы которых определены на множестве Z (естественно, сами функции также принимают значения из Z .) Сюда входят и функции от 0-го числа переменных, то есть просто константы из Z .

Для простоты вместо фразы «функция задаваемая полиномом с целыми коэффициентами» мы будем употреблять просто «цп-полином» или «цп-функция», то есть мы отождествляем формулу и функцию, задаваемую этой формулой.

Поскольку любая суперпозиция функций из P_Z является опять функцией из P_Z , то мы вправе рассмотреть пару (P_Z, O) , где O — множество операций суперпозиции над полиномиальными функциями из P_Z ; эта пара является функциональной системой, которую мы назовем *функциональной системой полиномиальных функций с целыми коэффициентами* и обозначим ее через \mathbf{F}_Z , то есть $\mathbf{F}_Z = (P_Z, O)$.

Следует отметить, что операции суперпозиции мы понимаем в широком смысле, то есть они включают в себя: перестановку переменных, отождествление переменных, переименование переменных (без отождествления), введение фиктивной переменной, удаление фиктивной переменной, подстановку одной функции в другую.

Теорема 1. *В функциональной системе \mathbf{F}_Z система функций $\{1, x - y, xy\}$ является полной системой; более того она является и базисом ф.с. \mathbf{F}_Z . (см. [1]).*

Теорема 2. *Имеет ли решение произвольное диофантово уравнение $f(x_1, x_2, \dots, x_n) = 0$, где $f(x_1, x_2, \dots, x_n)$ — любая полиномиальная функция с целыми коэффициентами, алгоритмически неразрешимо (10-я проблема Гильберта). (см. [3]).*

Основной результат данной работы (теорема 3) доказывается с помощью ряда утверждений (леммы 1–6), и естественно, изложение материала начнем с рассмотрения этих вспомогательных фактов. В связи с ограничением объема статьи доказательства лемм очень «сжаты».

Лемма 1. *Для любой цп-функции $f(x_1, x_2, \dots, x_n)$, отличной от констант из Z , множество*

$$M_f = \{(f^2(x_1, x_2, \dots, x_n) + 1)^2(x - y), x - 1, x + y, -xy\}$$

является полной системой в ф.с. \mathbf{F}_Z .

Доказательство. Введем обозначения:

$$\begin{aligned} g_1(x_1, x_2, \dots, x_n, x, y) &= (f^2(x_1, x_2, \dots, x_n) + 1)^2(x - y), \\ g_2(x) &= x - 1, g_3(x, y) = x + y, g_4(x, y) = -xy. \end{aligned}$$

Имеем: $g_1(x_1, x_2, \dots, x_n, x, x) = 0$; $g_2(0) = -1$; $g_2(-1) = -2$; ...

Далее, возможны два случая.

1. $f(0, 0, \dots, 0) = 0$; тогда $g_4(x, y) \equiv (f^2(0, 0, \dots, 0) + 1)^2(x - y) = x - y$; $g_4(0, y) = -y$; $g_4(0, -1) = 1$; $g_4(x, -y) = xy$. Получили систему цп-функций $1, x - y, xy$, которая является полной (см. теорему 1). Следовательно, M_f — полная система.

2. $f(0, 0, \dots, 0) \neq 0$; тогда целое число $k \equiv (f^2(0, 0, \dots, 0) + 1)^2 \geq 2$; поэтому $-k + 1 < 0$, которая у нас имеется. Далее, $g_3(k, -k + 1) = 1$; $g_4(x, g_4(y, 1)) = xy$; $g_3(x, g_4(1, y)) = x - y$. Получили систему цп-функций $1, x - y, xy$, которая является полной (см. теорему 1). Следовательно, M_f — полная система. Лемма доказана.

Лемма 2. Система цп-функций

$$M_1 = \{x - 1, x + y, -xy\}$$

не является полной в ф.с. \mathbf{F}_Z .

Доказательство. Справедливость этой леммы следует из того факта, что каждая функция данной системы сохраняет множество констант $\{-1, -2, -3, \dots\}$.

Лемма 3. Для любой цп-функции $f(x_1, x_2, \dots, x_n)$, отличной от констант из Z , множество

$$M_2 = \{(f^2(x_1, x_2, \dots, x_n) + 1)^2(x - y), x + y, -xy\}$$

не является полной в ф.с. \mathbf{F}_Z .

Доказательство. Справедливость этой леммы следует из того факта, что каждая функция данной системы сохраняет константу 0.

Лемма 4. Для любой цп-функции $f(x_1, x_2, \dots, x_n)$, отличной от констант из Z , множество

$$M_3 = \{(f^2(x_1, x_2, \dots, x_n) + 1)^2(x - y), x - 1, -xy\}$$

является полной в ф.с. \mathbf{F}_Z тогда и только тогда, когда $f(x_1, x_2, \dots, x_n)$ имеет корень в Z .

Доказательство. Доказательство объемное, суть которого состоит в следующем.

Пусть $f(x_1, x_2, \dots, x_n)$ имеет корень в Z . Тогда, аналогично доказательству леммы 1, можно показать, что из заданных цп-функций с помощью операций суперпозиции можно получить систему $\{1, x - y, xy\}$, которая является полной (см. теорему 1). Следовательно, M_3 — полная система.

Для доказательства обратного, то есть в том случае, когда $f(x_1, x_2, \dots, x_n)$ не имеет корней в Z , строим по индукции последовательность множеств H_1, H_2, H_3, \dots функций из P_Z .

Базис индукции. Положим $H_1 = M_f$.

Индуктивный переход. Пусть уже построены $H_1, H_2, H_3, \dots, H_k$. Тогда H_{k+1} определяется как множество всевозможных суперпозиций вида $g(h_1, \dots, h_m)$, где g — функция из M_f , а h_1, \dots, h_m — либо переменные, либо функции из H_k .

Далее, с помощью математической индукции по k можно показать, что $H_k (k = 1, 2, 3, \dots)$ не содержит цп-функцию вида $\pm x \pm y \pm c$, где c — произвольная константа из Z .

Следовательно, $\cup_{k=1}^{\infty} H_k$ не содержит цп-функцию вида $\pm x \pm y \pm c$. Значит, из заданной системы цп-функций с помощью операций суперпозиций невозможно получить все цп-функции, то есть эта система не является полной в ф.с. \mathbf{F}_Z . Лемма доказана.

Лемма 5. Для любой цп-функции $f(x_1, x_2, \dots, x_n)$, отличной от констант из Z , множество

$$M_4 = \{(f^2(x_1, x_2, \dots, x_n) + 1)^2(x - y), x - 1, x + y\}$$

не является полной в ф.с. \mathbf{F}_Z .

Доказательство. Вместо множества M_4 рассмотрим множество $M_4^* = \{(f^2(x_1, x_2, \dots, x_n) + 1)^2 t, x - y, x - 1, x + y\}$ и заметим, что замыкание множества M_4 является подмножеством замыкания множества M_4^* .

Далее, относительно M_4^* строим последовательность множеств

$$H_1, H_2, H_3, \dots, H_k, \dots$$

функций из P_Z также, как это сделано в лемме 4 и с помощью математической индукции по k можно показать, что $H_k (k = 1, 2, 3, \dots)$ содержит цп-функции, которые содержат члены вида sxy только с четными коэффициентами, (то есть $c = 2l$, где l — произвольное целое число).

Значит, из заданной системы цп-функций с помощью операций суперпозиции невозможно получить все цп-функции, то есть эта система не является полной в ф.с. \mathbf{F}_Z . Лемма доказана.

Лемма 6. Для любой цп-функции $f(x_1, x_2, \dots, x_n)$, отличной от констант из Z , базисом полной системы

$$M_f = \{(f^2(x_1, x_2, \dots, x_n) + 1)^2(x - y), x - 1, x + y, -xy\}$$

является

- i) множество M_3 , если $f(x_1, x_2, \dots, x_n)$ имеет корень в Z ;
- ii) множество M_f , если $f(x_1, x_2, \dots, x_n)$ не имеет корней в Z .

Доказательство. 1. Если $f(x_1, x_2, \dots, x_n)$ имеет корень в Z , то в силу леммы 4 система M_3 полной. Никакая ее собственная подсистема не является полной в силу вышедоказанных лемм, то есть в данном случае эта система является базисом.

2. Если $f(x_1, x_2, \dots, x_n)$ не имеет корней в Z , то в силу вышедоказанных лемм ни одна собственная подсистема системы M_f не является полной. Значит, M_f — базис. Лемма доказана.

Теорема 3. *Не существует алгоритма, который из любой конечной полной системы в ф.с. \mathbf{F}_Z выделит базис.*

Доказательство. Допустим, что существует такой алгоритм. Тогда этот алгоритм, в частности, выделит базис из вышеприведенной системы M_f . В силу леммы 6 возможны два случая.

1. Базисом системы M_f является множество M_3 ; тогда полином $f(x_1, x_2, \dots, x_n)$ имеет корень в Z (в силу леммы 6).

2. Базисом системы M_f является множество M_f ; тогда полином $f(x_1, x_2, \dots, x_n)$ не имеет корней в Z (в силу леммы 6).

Следовательно, существует алгоритм, распознающий имеет ли произвольный полином с целыми коэффициентами $f(x_1, x_2, \dots, x_n)$ корень в Z , то есть существует алгоритм для решения произвольного диофантова уравнения. Это противоречиво в силу теоремы 2. Теорема доказана.

Автор выражает глубокую благодарность профессору Московского государственного университета им. М.В. Ломоносова В.Б. Кудрявцеву за постоянную поддержку при выполнении данной работы.

Список литературы

- [1] Алексиадис Н. Ф. Алгоритмическая неразрешимость проблемы полноты для полиномов с целыми коэффициентами // Вестник МЭИ. — 2015. № 3. — С. 110–117.
- [2] Кудрявцев В. Б. Функциональные системы. — М.: Изд-во МГУ, 1982.
- [3] Матиясевич Ю. В. Десятая проблема Гильберта. — М.: Наука, 1993.
- [4] Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986.