Доклады Академии Наук СССР
1950. Том LXX, № 4

*МАТЕМАТИКА*

Б. А. ТРАХТЕНБРОТ

# НЕВОЗМОЖНОСТЬ АЛГОРИФМА ДЛЯ ПРОБЛЕМЫ РАЗРЕШИМОСТИ НА КОНЕЧНЫХ КЛАССАХ

*(Представлено академиком А. Н. Колмогоровым 1 XII 1949)*

1. В этой статье речь будет итти о формулах узкого функционального исчисления, которые мы будем называть просто формулами и обозначать прописными готическими буквами. Иногда в скобках будут указаны функциональные символы, встречающиеся в формуле, например: $\mathfrak{A}(F^i, G^j, H^k, \ldots)$. Здесь верхний индекс указывает число аргументов функции (предиката), а сами функции следует рассматривать как переменные функции.

В 1936 г. Черч ([1]) доказал, что не существует алгорифма для проблемы разрешимости узкого функционального исчисления. Эта проблема заключается в том, что для каждой данной $\mathfrak{A}$ требуется решить вопрос, выводима ли она в исчислении или нет. Мы всюду имеем в виду точное определение понятия „алгорифм", данное в терминах теории общерекурсивных функций. Известно, что формула $\mathfrak{A}(F^i, \ldots, H^k)$ выводима в том и лишь в том случае, когда она истинна, каковы бы ни были функции $F_0^i, \ldots, H_0^k$ и их область определения. Известно также, что существуют формулы, истинные во всякой конечной области, а между тем не выводимые в исчислении. Таким образом, результатом Черча не решается следующая проблема:

(*) Проблема разрешимости на конечных классах. Требуется построить алгорифм, посредством которого можно было бы узнавать для всякой $\mathfrak{A}$, истинна ли она во всякой конечной области или нет.

Для формул частного вида такой алгорифм построил И. И. Жегалкин. В работе ([2]) описывается правило, по которому каждой формуле $\mathfrak{A}$ из класса формул, рассматриваемых автором, приводится в соответствие натуральное число $n(\mathfrak{A})$, обладающее таким свойством: если $\mathfrak{A}$ истинна во всякой области, содержащей не более $n(\mathfrak{A})$ элементов, то она истинна во всякой конечной области. Вопрос же об истинности $\mathfrak{A}$ в области с заранее ограниченным числом элементов решается конечным числом проб.

В настоящей заметке устанавливается, что в общем случае невозможно алгорифмическое решение проблемы (*). Этот результат легко получить, опираясь на теорему 1, представляющую самостоятельный интерес.

2. Можно расширить класс формул узкого функционального исчисления, если допускать в формулах, помимо символов для переменных функций, и символ „=" для специального предиката тождества. Для этого расширенного класса формул проблема (*) сохраняет свой смысл, и легко доказать, что она просто равносильна проблеме

в первоначальной формулировке. Мы не будем налагать никаких ограничений на право пользоваться предикатом тождества.

Моделью формулы $\mathfrak{A}(F^i, \ldots, H^k)$ называется всякое множество $P$ с зафиксированными на нем функциями $F_0^i, \ldots, H_0^k$ такими, что $\mathfrak{A}(F_0^i, \ldots, H_0^k)$ истинна. Нас будут интересовать конечные модели ($P$ конечно).

Пусть дана какая-нибудь конечная модель формулы $\mathfrak{A}(M^1, \ldots)$. Через $\widetilde{M}^1$ будем обозначать число элементов модели, на которых одноместный предикат $M^1(x)$ истинен. $\widetilde{M}^1$ зависит от выбранной модели и при всевозможных конечных моделях пробегает некоторое определенное подмножество (быть может, пустое) натурального ряда, которое мы называем спектром предиката $M^1$. Заметим, что к натуральным числам мы причисляем и 0.

Определение 1. Будем говорить, что функция $f(m)$, определенная для всех натуральных чисел и принимающая натуральные значения, допускает спектральное представление (д. с. п.), если существует формула $\mathfrak{A}(M^1, F^1, \ldots)$, удовлетворяющая следующим требованиям: 1) спектр $M^1$ состоит из всех натуральных чисел; 2) если в некоторой конечной модели $\widetilde{M}^1 = m$, то в ней обязательно $\widetilde{F}^1 = f(m)$.

Пример. Функция $S(x) = x + 1$ допускает такое представление:

$$(Ex)\,[S(x)\,\&\,\overline{X(x)}\,\&\,(y)\,(y \neq a \to (S(y) \sim X(y)))].$$

Примечание 1. Определение 1, как и приведенная ниже теорема 1, формулируется соответствующим образом для функций многих переменных.

Теорема 1. *Для того чтобы $f(m)$ допускала спектральное представление, необходимо и достаточно, чтобы она была общерекурсивной функцией.*

Необходимость. Пусть $\mathfrak{A}(M^1, F^1, \ldots)$ удовлетворяет требованиям теоремы. Применение методов арифметизации позволяет доказать последовательно следующие утверждения:

I. Функция $\psi(m, k)$, равная 0, если для $\mathfrak{A}$ существует модель из $k$ элементов, в которой $\widetilde{M}^1 = m$, и равная 1 в противном случае, примитивно рекурсивна.

II. Функция $\chi(m, n, k)$, равная 0, если для $\mathfrak{A}$ существует модель из $k$ элементов, в которой $\widetilde{M}^1 = m$, $\widetilde{F}^1 = n$, и равная 1 в противном случае, примитивно рекурсивна.

Пусть $\gamma(m) = \mu k[\psi(m, k) = 0]$, т. е. наименьшее число $k$ такое, что $\psi(m, k) = 0$; тогда зависимость $\widetilde{F}^1$ от $\widetilde{M}^1$ описывается общерекурсивной функцией $f(m) = \mu n[\chi(m, n, \gamma(m)) = 0]$.

Достаточность вытекает из утверждений a) — f):

a) $S(x) = x + 1$ д. с. п.;

b) функция $E(x)$, равная избытку над наибольшим квадратом, не превосходящим $x$, д. с. п.;

c) если $f(x)$ и $g(x)$ д. с. п., то $h(x) = f(x) + g(x)$ также д. с. п. (если $f(x)$ и $g(x)$ д. с. п., то $h(x) = f[g(x)]$ также д. с. п.);

e) если $f(x)$ д. с. п., то д. с. п. и функция $g(x)$, определенная следующей рекурентной формулой: $g(0) = 0$, $g(x + 1) = f[g(x)]$.

Примечание 2. Как доказал Робинсон ([3]), класс примитивно рекурсивных функций одного переменного совпадает с наименьшим классом, содержащим функции $S(x)$ и $E(x)$ и замкнутым по отношению к операциям, описанным в c) — e). Таким образом, из a) — e) следует, что все примитивно рекурсивные функции одного переменного д. с. п.; из спектрального же представления функций одного

переменного легко получить представления функций многих переменных.

f) Пусть $\mathfrak{B}(M^1, N^1, F^1, \ldots)$ дает д. с. п. функции $f(m, n)$ такой, что для всякого $m$ существует единственное $n$, для которого $f(m, n) = 0$. Тогда функция $n(m) = \mu n[f(m, n) = 0]$ также д. с. п., а именно формулой $\mathfrak{B}(M^1, N^1, F^1, \ldots) \,\&\, (x)\,\overline{F(x)}$.

Докажем, например, утверждение е). Пусть $f(m)$ д. с. п.: $\mathfrak{A}(M^1, F^1, \ldots)$. Произведем в формуле следующие подстановки: $M^1(x)$ заменяем предикатом $M^2(\xi, x)$ и $N^1(x)$ предикатом $M^2(\eta, y)$ ($\xi$, $\eta$ играют роль параметров, причем предполагается, что эти символы не встречаются в $\mathfrak{A}$). Далее подставляем вместо всякого другого предиката $H^k(x_1, \ldots, x_k)$ из $\mathfrak{A}$ предикат $H^{k+2}(\xi, \eta, x_1 \ldots, x_k)$. Полученную формулу обозначим через $\mathfrak{A}_{\xi\eta}$.

Построим еще формулу $\mathfrak{B}(M^1, R^2, S^2, \ldots)$ ($R^2$, $S^2$ символы, не встречающиеся в $\mathfrak{A}$), обладающую следующим свойством: какова бы ни была модель формулы $\mathfrak{B}$, двуместный предикат $R^2$ упорядочивает множество элементов модели, из которых $M^1(x)$ истинен, причем так, что в этом порядке $S^2$ является предикатом непосредственного следования. Тогда функции $g(m)$ соответствует такая формула:

$$\mathfrak{B} \,\&\, (\xi)[(y)\,\overline{S(y, \xi)} \to (x)\,\overline{M(\xi, x)}] \,\&\, (\xi)(\eta)[S(\xi, \eta) \to \mathfrak{A}_{\xi\eta}]$$

$$\&\, (\eta)[(y)\,\overline{S(\eta, y)} \to (x)(G(x) \sim M(\eta, x))].$$

3. Пусть даны произвольная общерекурсивная функция $f(m)$ и соответствующая ей по теореме 1 формула $\mathfrak{A}(M^1, F^1, \ldots)$. Уравнение $f(m) = 0$ имеет целочисленный неотрицательный корень в том и лишь в том случае, когда формула $\mathfrak{A}(M^1, F^1, \ldots) \,\&\, (x)\,\overline{F(x)}$ имеет конечную модель, или, что то же самое, когда отрицание этой формулы не тождественно истинно в любой конечной области.

Таким образом, если бы существовал алгорифм, требуемый в ( * ), то из него можно было бы извлечь алгорифм для следующей проблемы:

( ** ) Требуется решить вопрос о том, имеет ли уравнение вида $f(m) = 0$ ($f(m)$ — какая-нибудь произвольная общерекурсивная функция) целочисленное неотрицательное решение или нет.

Здесь существенно то обстоятельство, что для данной общерекурсивной функции можно эффективно построить формулу, существование которой гарантируется теоремой 2.

Но известно ([1]), что проблема ( ** ) не допускает алгорифмического решения. Отсюда следует:

Теорема 2. *Невозможен алгорифм для проблемы разрешимости на конечных классах.*

4. Введем обозначения $K_n$ ($n = 1, 2, \ldots$) для класса формул, тождественно истинных в области из $n$ элементов, и $K_\omega$ — для класса формул, истинных в любой конечной области.

Условимся далее говорить, что $\mathfrak{B}$ следует из $\mathfrak{A}$, если $\mathfrak{B}$ выводима в исчислении, получаемом присоединением к узкому функциональному исчислению формулы $\mathfrak{A}$ в качестве новой аксиомы.

Вайсберг ([4]) доказал такую теорему:

Какова бы ни была $\mathfrak{A}$ такая, что $\mathfrak{A} \in K_n$, $\mathfrak{A} \overline{\in} K_{n+1}$, из $\mathfrak{A}$ следует всякая $\mathfrak{B}$ из класса $K_n$.

Что же касается класса $K_\omega$, из теоремы 2 легко получается такое следствие:

Следствие. *Какова бы ни была $\mathfrak{A}$ из $K_\omega$, существует такая $\mathfrak{B}$ в $K_\omega$, что $\mathfrak{B}$ не следует из $\mathfrak{A}$.*

С другой стороны, из невозможности алгорифма для проблемы

разрешимости узкого исчисления можно заключить, что, какова бы ни была $\mathfrak{A}$ из $K_\omega$, существует такая $\mathfrak{B}$ в $K_\omega$, что $\mathfrak{A}$ не следует из $\mathfrak{B}^*$.

На протяжении этого пункта теория множеств рассматривается в виде логического исчисления $\tau$, получаемого присоединением к узкому функциональному исчислению системы аксиом Геделя — Бернайса, включая аксиому Цермело (5). Однако приведенные ниже рассуждения остаются в силе для широкого класса теоретико-множественных исчислений, в которых соблюдаются некоторые требования весьма общего характера.

Будем обозначать через $\mathfrak{A}^*$, $\mathfrak{B}^*$, ... формулы класса $K_\omega$, которые не выводимы в узком функциональном исчислении. Формуле $\mathfrak{A}^*$ соответствует такое определение конечного множества: множество $q$ конечно, если на нем $\mathfrak{A}^*$ тождественно истинна. В теории множеств это определение записывается в виде некоторой формулы, которую мы обозначим через $\mathfrak{A}^*(q)$.

Говорят, что данное предложение неразрешимо в исчислении $\tau$, если оно записывается в виде некоторой формулы этого исчисления, которая в нем не доказуема и не опровержима (т. е. отрицание этой формулы также недоказуемо).

Теорема неполноты. *В формализованной теории множеств существуют неразрешимые предложения вида*

$$\mathfrak{A}^*(q) \to \mathfrak{B}^*(q).$$

Точнее, для всякого $\mathfrak{A}^*(q)$ существуют такие $\mathfrak{B}^*(q)$ и $\mathfrak{G}^*(q)$, что предложения $\mathfrak{A}^*(q) \to \mathfrak{B}^*(q)$, $\mathfrak{G}^*(q) \to \mathfrak{A}^*(q)$ неразрешимы. В книге (6) Френкель указывает на то, что без аксиомы Цермело не удается доказать эквивалентность известного определения конечного множества, данного Дедекиндом, с некоторыми определениями, предложенными другими авторами, и высказывает предположение, что с этой аксиомой можно доказать уже эквивалентность всяких определений конечности.

Теорема неполноты показывает, что в рамках формализованной теории множеств не для всех определений типа $\mathfrak{A}^*(q)$ можно доказать эквивалентность.

Институт математики
Академии наук УССР

Поступило
1 XII 1949

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] A. Church, Am. Journ. Math., 58, 345 (1936); Journ. Symb. Logic, 1, 40 (1936). [2] И. И. Жегалкин, Уч. зап. МГУ, 100 (1) (1946). [3] R. Robinson, Bull. Am. Math. Soc., 53, 925 (1947). [4] M. Wajsberg, Math. Ann., 109, 200 (1933). [5] К. Гедель, Усп. матем. наук, 3 (23), 96 (1948). [6] A. Fraenkel, Zehn Vorlesungen über die Grundlagen der Mengenlehre, 1927.

* После представления к печати настоящей статьи автору стало известно, что в «Sprawozdanja z posiedzeń towarzystwa naukowiego Warszawskiego», Wydział III, 1938 г., стр. 13, А. Мостовским приводятся без доказательства результаты, аналогичные нашему следствию пункта 4.