

Санкт-Петербургский политехнический университет
Петра Великого
Институт компьютерных наук и технологий

Алгоритмическая неразрешимость. Десятая проблема Гильберта

Выполнили: Захаренко Екатерина, Михайловская Софья

Научный руководитель: Доцент кафедры «Высшая математика»

Филимоненкова Надежда Викторовна

Задачи работы

- ▶ Конкретизировать понятие алгоритмической неразрешимости.
- ▶ Разобрать примеры алгоритмически разрешимых и неразрешимых массовых проблем.
- ▶ Изучить историю возникновения 10-й проблемы Гильберта и развитие доказательства ее неразрешимости.

Понятие алгоритма

До 30-х годов XX в.

Алгоритм - это
интуитивное
понятие...



Л. Эйлер



Г.В. Лейбниц

После 30-х годов XX в.

Алгоритм — это точно
установленное предписание о
выполнении в определённом
порядке некоторой
последовательности
операций, однозначно
ведущих к решению
конкретной задачи.

Алгоритмическая неразрешимость

Массовая проблема - это бесконечное множество однотипных задач:

$$\{a_i\}$$

a_i - некоторая единичная задача.

- ▶ Массовая проблема называется *алгоритмически неразрешимой (далее АНР)*, если не существует универсального алгоритма, позволяющего решить каждую ее задачу, иначе *алгоритмически разрешимой (далее АР)*.

Примеры АР проблем

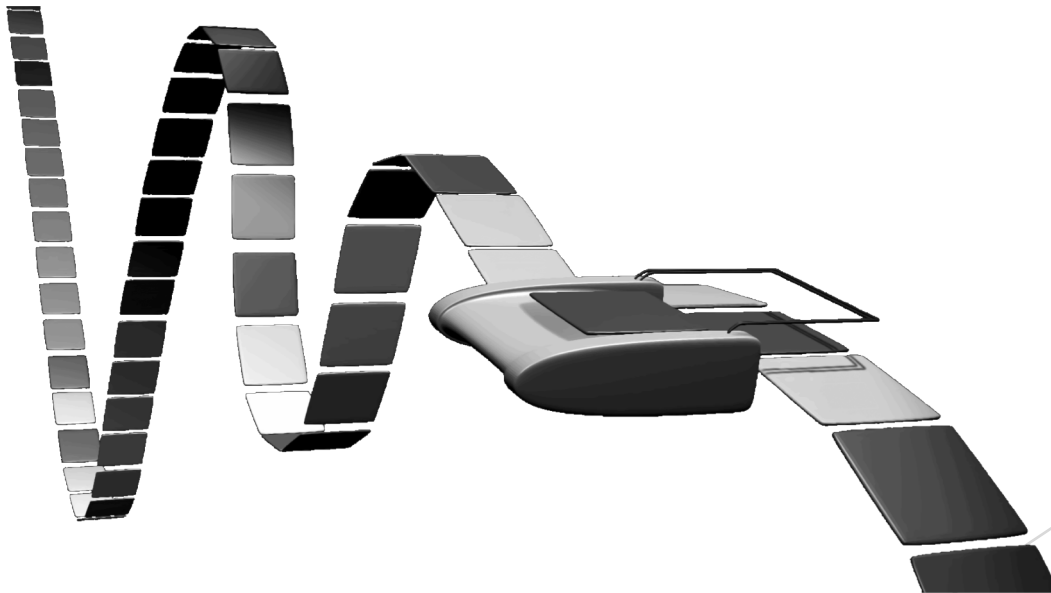
АР проблема	Алгоритм решения
Сложение двух и более целых чисел	Сложение чисел «в столбик» с применением таблицы сложения однозначных чисел
Решение систем m линейных алгебраических уравнений с n неизвестными	Метод Гаусса
Нахождение наибольшего общего делителя n целых чисел	Алгоритм Евклида для двух чисел и теорема о том, что НОД n чисел $a_1, a_2, \dots, a_n$ равен числу d_n , которое находится при последовательном вычислении $\text{НОД}(a_1, a_2)=d_2$, $\text{НОД}(d_2, a_3)=d_3, \dots, \text{НОД}(d_{n-1}, a_n)=d_n$

Примеры АР проблем

АР проблема	Алгоритм решения
Сортировка одномерного массива	«Пузырьковый» метод или метод Quick sort
Решение изобретательских задач	АРИЗ — комплексная программа алгоритмического типа, основанная на законах развития технических систем и предназначенная для анализа и решения изобретательских задач.
Решение задач по генетике	Алгоритм через решетку Пеннета
Разложение функции в степенной ряд	Алгоритм через производные и формулу разложения Тейлора

Машина Тьюринга

- ▶ Машина Тьюринга— абстрактный исполнитель (абстрактная вычислительная машина). Была предложена Аланом Тьюрингом в 1936 году для формализации понятия алгоритма.



Тезис Тьюринга

Для любой алгоритмически
вычислимой задачи существует
вычисляющая её
значения машина Тьюринга

Проблема распознавания самоприменимых машин Тьюринга

- ▶ Самоприменимость - свойство алгоритма успешно завершаться на данных, представляющих собой формальную запись этого же алгоритма
- ▶ Проблема: создать алгоритм, который по любой машине Тьюринга устанавливал бы, самоприменима она или нет.
- ▶ Теорема: Проблема распознавания самоприменимых машин Тьюринга алгоритмически не разрешима.

Проблема распознавания самоприменимых машин Тьюринга

- ▶ Пусть, в случае самоприменимости конечное состояние машины будет x , несамоприменимости - y
Доказательство проводится от противного.
- ▶ Пусть самоприменимая машина A существует. Тогда можно построить машину B , которая
 - 1) перерабатывает несамоприменимые коды в y
 - 2) к самоприменимым кодам уже не применима.
- ▶ Машина $B = \text{машина } A + \text{после появления символа } x \text{ вместо остановки машина должна неограниченно его повторять.}$

Проблема распознавания самоприменимых машин Тьюринга

- ▶ Машина В либо самоприменима, либо несамоприменима.
 - ▶ Если она самоприменима, т.е. применима к коду своего номера, то она применима и к коду самоприменимой машины, но тогда не выполняется требование 2
 - ▶ Если машина В несамоприменима, т.е. она не применима к коду своего номера, то она не применима и к коду несамоприменимой машины, но тогда не выполняется требование 1.
- ▶ В итоге, мы пришли к противоречию, основанное на допущении о том, что существует машина А, решающая проблему самоприменимости. Следовательно, такой машины не существует.

Проблема остановки

- ▶ Дано: описание процедуры и её начальные входные данные.
- ▶ Определить: завершится ли когда-либо выполнение процедуры с этими данными или же она работает всё время без остановки.
- ▶ Доказательство неразрешимости : А. Тьюринг (1936 год)

Применяется для доказательства других АНР проблем.

Проблема ЭКВИВАЛЕНТНОСТИ СЛОВ

- ▶ Дано:
 - ▶ Некоторый алфавит $A = \{a, b, c, \dots\}$ и множество слов в этом алфавите.
 - ▶ Конечная система допустимых подстановок (замен одних комбинаций символов другими).
- ▶ Совокупность всех слов + допустимые подстановки = ассоциативное исчисление
- ▶ Слова A и B называются эквивалентными, если существует конечная последовательность допустимых подстановок, преобразующая A в B .
- ▶ Проблема эквивалентности слов: существует ли единый алгоритм для проверки эквивалентности любых двух слов в любом ассоциативном исчислении?

Проблема эквивалентности слов



А. А. Марков



Э. Пост

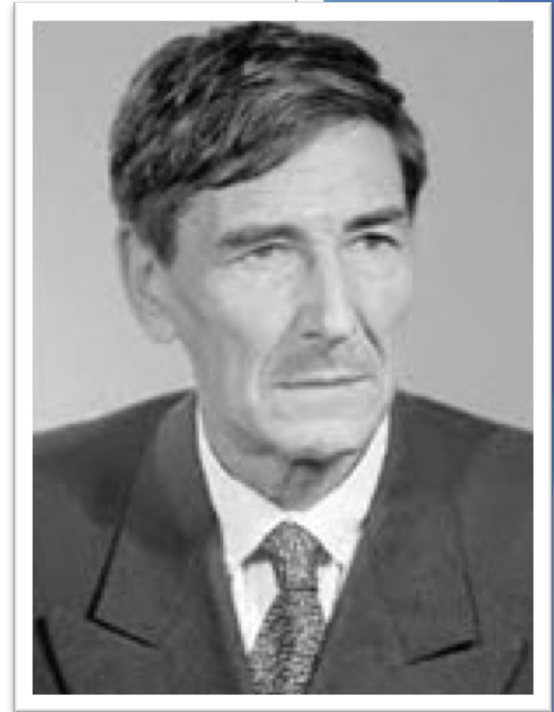
А.А. Марков и Э. Пост построили конкретные примеры ассоциативных исчислений, для каждого из которых проблема эквивалентности слов является АНР проблемой, и, следовательно, не существует алгоритма для распознавания эквивалентности слов в любом исчислении.

Проблема эквивалентности слов

Российский математик П. С. Новиков доказал алгоритмическую неразрешимость проблемы тождества групп.

Примеры, построенные А. А. Марковым и П. С. Новиковым, были громоздкими и насчитывали сотни допустимых подстановок.

Петербургскому математику Г. С. Цейтину удалось построить пример алгоритмически неразрешимого исчисления, в котором используется лишь семь допустимых подстановок.



П. С. Новиков

Проблема представимости матриц

- ▶ Дано: система целочисленных матриц $U, U_1, U_2, \dots, U_q$ размера $n \times n$.
- ▶ Определить: представима ли матрица U через произведение остальных матриц системы:

$$U = U_1 * U_2 * \dots * U_r, r \leq q$$

- ▶ Частный случай: фиксируем матрицы $U_1, U_2, \dots, U_q$, матрица U - переменная.
- ▶ Доказательство неразрешимости: А. А. Марков

Десятая проблема Гильберта

На Втором международном конгрессе математиков (1900) Дэвид Гильберт огласил 23 проблемы из различных разделов математики.

Десятая из них посвящена разрешимости диофантовых уравнений.



Д. Гильберт

Десятая проблема Гильберта

«Пусть задано произвольное диофантово уравнение с произвольными неизвестными и целыми рациональными числовыми коэффициентами. Указать способ, при помощи которого возможно после конечного числа операций установить, разрешимо ли это уравнение в целых рациональных числах.»

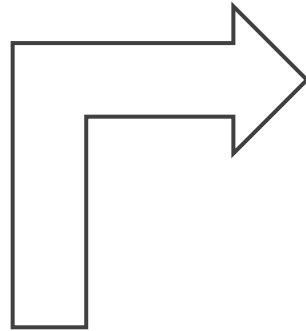


Д. Гильберт

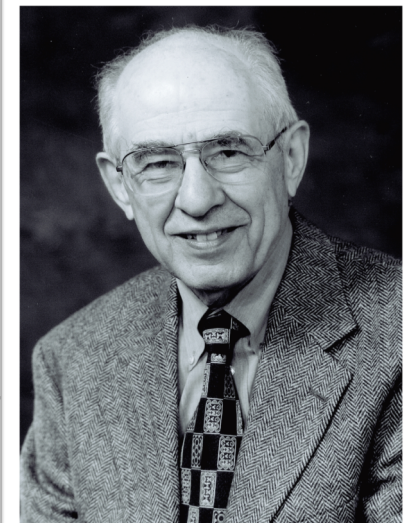
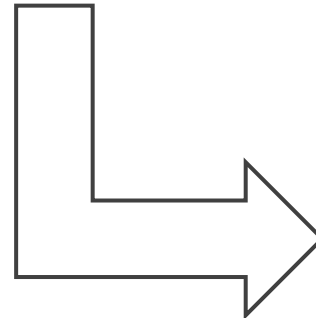
Первые шаги доказательства



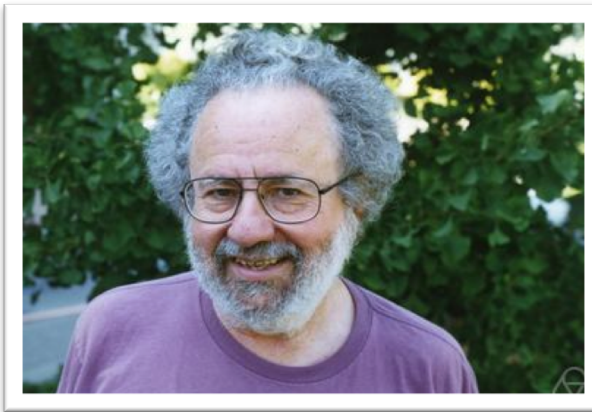
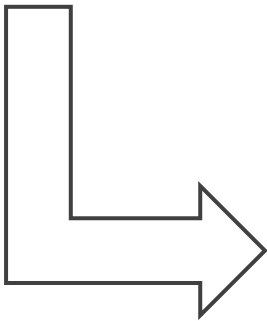
Э. Пост



Д. Робинсон



Х. Патнем



М. Дэвис

Полное доказательство неразрешимости



Юрий Матиясевич

Советский математик
Юрий Матиясевич
обобщил все ранее
известное о Десятой
проблеме Гильберта и
окончательно доказал ее
алгоритмическую
неразрешимость.

Диофантовы уравнения



Древнегреческий
математик Диофант

$P(x_1, x_2, \dots, x_n) = 0$,
где P - многочлен с
целыми
коэффициентами

Примеры диофантовых уравнений

1. $x^2 + y^2 = z^2$

Все натуральные решения этого уравнения имеют следующий вид:

$$x = (m^2 - n^2)l$$

$$y = 2mnl$$

$$z = (m^2 + n^2)l$$

$$l, m, n \in \mathbb{N}$$

2. $x^n + y^n = z^n, n \in \mathbb{N}$

Великая теорема Ферма: данное уравнение при $n > 2$ не имеет решений в целых числах (доказана Эндрю Уайлисом в 1995).

Основное положение доказательства. Гипотеза Дэвиса



М. Дэвис

Теорема Лагранжа:
любое натуральное
число можно
представить в виде
суммы квадратов 4
целых чисел.

Решение в
целых числах



Решение в
натуральных
числах

Гипотеза Дэвиса.

Диофантовы множества

- ▶ Мартин Дэвис рассмотрел семейства диофантовых уравнений вида $P(a_1, a_2, \dots, a_m, x_1, x_2, \dots, x_n) = 0$ $a_1, a_2, \dots, a_m$ целочисленные параметры.
- ▶ Диофантово множество - это множество тех значений параметров, при которых уравнение (*) разрешимо относительно переменных $x_1, \dots, x_n$:

$$\langle a_1, a_2, \dots, a_m \rangle \in M$$

$$\Leftrightarrow \exists x_1, x_2, \dots, x_n \{P(a_1, a_2, \dots, a_m, x_1, x_2, \dots, x_n) = 0\}$$

Примеры: множество всех полных квадратов

$$a - x^2 = 0$$

множество всех составных чисел

$$a - (x_1 + 2)(x_1 + 2) = 0$$

Гипотеза Дэвиса как основа доказательства

Перечислимое множество - это множество, все элементы которого могут быть получены с помощью некоторого алгоритма. Например, множество натуральных чисел.

Гипотеза Дэвиса: Понятия диофантова и перечислимого множества совпадают.
Множество диофантово тогда и только тогда, когда оно перечислимо.

Данная гипотеза была доказана Ю. Матиясевичем, Д. Робертсон и Х.Патнем.

Итог - DPRM-теорема (формулировка совпадает с гипотезой Дэвиса).

Выводы

- ▶ Развитие ЭВМ позволяет доказывать больше AP и АНР массовых проблем;
- ▶ Алгоритмическая неразрешимость массовой проблемы не означает алгоритмической неразрешимости ее единичных задач;
- ▶ Чем шире массовая проблема, тем проще доказательство ее алгоритмической неразрешимости, и наоборот;
- ▶ Универсальный алгоритм - нечто из раздела фантастики (пока).

Список литературы

1. Матиясевич Ю.В. «Десятая проблема Гильберта»
2. Успенский В. А., Семенов А. Л. «Теория алгоритмов: основные открытия и приложения»
3. Успенский В. А., Семёнов А. Л. Решимые и неразрешимые алгоритмические проблемы. // Квант, 1985, № 7, с. 9 – 15
4. Галиев Ш.И. «Математическая логика и теория алгоритмов»
5. https://ru.wikipedia.org/wiki/Алгоритмически_не_разрешимая_задача
6. <https://habr.com/post/145929/>

Спасибо за внимание.