Введение в математическую логику и теорию алгоритмов

Алексей Львович Семенов

Введение

Цель — ответить на **вопросы:**

- Что значит, что математическое утверждение доказано?
- Что значит определить математическое отношение?
- Что значит, что математическая функция вычислима?

Давид Гильберт, 23.01.1862 — 14.02.1943
II Международный математический конгресс, Париж, 1900

23 Проблемы Гильберта

I, II, X проблемы относятся к математической логике и теории алгоритмов

Из семи математических Проблем тысячелетия первая также относится к нашему предмету

Доказательство. **Ответы:**

- Конец XIX в.:
  Готлоб Фреге,
  Давид Гильберт и др.:
  Математическое доказательство (как деятельность) — получение цепочек символов по математически определенным правилам
  Математическое доказательство (как объект) — цепочка формул, построенная по заданным правилам
- **Георг Кантор:**
  Первичная система понятий математики
- Начало XX в.
  Эрнст Цермело...

Эта система правил будет предъявлена.

Вычисление. **Ответы:**

Курт Гедель, Алан Тьюринг, Алонзо Чёрч,
Эмиль Пост и др. в середине 1930-х гг.

Вычислимая функция — функция, аргументами и результатами которой являются цепочки символов (бывают и обобщения), для которой существует ее описание, построенное по некоторым правилам.

Эта система правил будет предъявлена.

Программа Гильберта основания (и обоснования) математики

Курт Гёдель
(28.04.1906 — 14.01.1978)
указание возможности и доказательства невозможности,
начало 1930-х гг.

Базовые определения

- Множество, объединение, пересечение, прямое произведение, проекция, функции и т. п.
- Отношения на множестве — подмножества прямой (декартовой) степени этого множества. Свойство — функция со значениями И и Л (не обязательно всюду определенная) — задает отношение — множество, где значение функции — И.
- Алфавит = конечное множество символов.
- Цепочка = конечная последовательность, в частности, последовательность может быть и пустой — Λ (длина — 0).
- Слово (в данном алфавите) — конечная последовательность символов (частный случай цепочки). Длина слова — число элементов цепочки.
- Слово v входит в w, если $w = uvs$ для некоторых u, s. Вхождение v в w — это слово вида $u * v * s$, где $uvs = w$. Мы будем пользоваться понятием «первое вхождение», и т. д.
- Ансамбль конструктивных объектов — более общее понятие, чем множество всех слов в данном алфавите, например, можно дать определение ансамбля размеченных графов.

- Цепочка слов — тоже слово (в расширенном алфавите — добавляем запятую после каждого элемента):
  - пустая цепочка — это пустое слово,
  - цепочка из одного пустого слова — это слово из одного символа `,`.

• Кодирование

Код цепочки слов в алфавите $\{0, 1\}$:

- Удвоить каждую букву 0 или 1, запятую заменить на 01
- Функция из ансамбля слов в алфавите трех символов $\{0, 1, ,\}$ в ансамбль слов в алфавите $\{0, 1\}$.

- **Задача:** можно ли кодировать покороче?

- Многоместные функции и свойства можно заменять одноместными.

- Логические значения: символы И, Л, или символы 0, 1.
- Логические операции: $\&$ (и, конъюнкция), $A \vee B$ (или, дизъюнкция), $\neg$ (не, отрицание) применяются к символам 1 (И) и 0 (Л):

A	B	$\neg A$	$A \wedge B$	$A \vee B$
0	0	1	0	0
0	1	1	0	1
1	0	0	0	1
1	1	0	1	1

- Характеристическая функция принимает значения И и Л или 0 и 1 и задает отношение (свойство).

Описания. Действия и проверки

- Действие — исходное понятие. Действие:
  - описано на понятном человеку языке, может осуществляться и человеком и каким-то (реальным или абстрактным) устройством,
  - можно применить к любому исходному данному из фиксированного ансамбля исходных данных (у нас это ансамбль слов), при этом ясно, что всегда получается результат применения — элемент (возможно, другого) фиксированного ансамбля (в нашем случае — слов).
- Действие — всюду определенная функция.
- Кодирование — пример действия.
- Проверка — характеристическая функция (свойство), являющаяся действием.

Эмиль Борель (1912): *«Я намеренно оставляю в стороне большую или меньшую практическую длительность; суть здесь та, что каждая из этих операций осуществима в конечное время при помощи достоверного и недвусмысленного метода».*

Исчисления. Породимые множества

- Исчисление — это пара из двух проверок:
  $\langle$ правило создания, правило окончания $\rangle$.
- Правило создания применяется к коду цепочки слов, а правило окончания — к слову.
- Множество создаваемых исчислением объектов определяется так:
  Если правило создания выполнено для цепочки объектов $a_0, \ldots, a_n$ и все элементы этой цепочки, кроме последнего, — создаваемы, то и последний элемент создаваем.
- Если правило создания выполнено для цепочки из одного элемента, то его называют начальным объектом.
- Что, если таких у данного исчисления нет?
- Объект порождаем данным исчислением, если он создаваем и для него выполнено правило окончания.
- Множество, порождаемое исчислением. Породимое множество.

Замечания

- Можно считать, что правило создания — это отношение между конечными подмножествами ансамбля (проверка).
- Создаваемость — *замыкание* отношения п.2.
- Если для $a_0, \ldots, a_n$ выполнено (истинно) правило создания, то a_n создается, или выводится, из $a_0, \ldots, a_{n-1}$.
- Вывод объекта a — последовательность объектов, каждый из которых выводится из подмножества предшествующих ему в выводе. Объект создаваем тогда и только тогда, когда у него имеется вывод.

Теоремы замкнутости для исчислений

Т. Объединение, пересечение и проекция породимых множеств породимы.

Д. Пересечение.

А: ⟨ Правило создания А, Правило окончания А ⟩ ,

Б: ⟨ Правило создания Б, Правило окончания Б ⟩ .

- Создаем все по правилу А и все по правилу Б,
- Отбираем то, что породилось и по тому и по другому правилу.
- Проблема — перемешивание правил.
- Метки для объектов, создаваемых по правилу А и по правилу Б.
- Как создавать пары вида ⟨ А,x ⟩ , ⟨ Б, y ⟩ ?
- Припишем ко всем элементам цепочки, входящей в Правило создания, первой компонентой символы А и Б (элементы стали парами).
- Объединим правила.
- Удаляем пометки, то есть добавляем в правило ⟨⟨ А,x ⟩ , ⟨ Б,x ⟩ , x ⟩ .
- Правило окончания?
- Конъюнкция Правил окончания А и Б.

Породимость дополнения?

- В самом определении говорится, как создавать новые объекты, и никак не видно, как можно установить не-создаваемость (и не-породимость).
- Математик, пытаясь понять, что что-то нельзя доказать, часто формулирует отрицание утверждения и пытается доказать это отрицание.
- Иногда он берет даже более сильное негативное утверждение, например, конструирует конкретный контрпример.
- Всегда ли можно доказать или утверждение или его отрицание?
- Вот один из вопросов, на которые математическая логика пытается дать ответ.
- Бывает, что сама постановка вопроса об отрицании бессмысленна.

Ячейки

- Действие работает с объектом целиком.
- Бываете удобно разделить объект на части, каждая из которых лежит в своей ячейке, ячейка имеет отдельное имя, и действие меняет иногда содержимое одной ячейки, иногда — другой.
- Если наши объекты слова, то это можно делать, используя цепочки слов и кодируя их словами.
- Значение имени (содержимое ячейки) можно изменить, в частности, с помощью действия присваивания $\leftarrow$.
- Метки из подходящего конечного алфавита — в ячейках.

Операции над функциями, свойствами и их описаниями

- Действия и проверки задаются своими описаниями.
- Описывать можно и функции, получаемые из имеющихся с помощью операций.

График

- Пусть Γ — описание функции. Тогда $\underline{\Gamma}$ — описание функции, которая перерабатывает объект x в пару $\langle x, \Gamma(x)\rangle$ (график Γ).
- Ячейки с именами: «аргумент Γ» и «значение Γ». $\underline{\Gamma}$ может сначала сделать из x пару $\langle x, x\rangle$ (скопировать x), а потом применить Γ ко второму элементу пары.

Композиция (последовательное выполнение)

Пусть Г, Д — описания функций, тогда

- Г
- Д

описание функции:
сначала применяем функцию, описанную Г,
потом к результату — функцию, описанную Д.

Если Г, Д описывают действия, мы получаем описание действия.

Ветвление (условный оператор)

Пусть П — описание свойства, Г — описание функции, тогда

- Если П
  - Г

описание функции:

Если значение свойства П для объекта — это И,
то применяем Г;
Если значение свойства — Л,
то результат применения функции совпадает с исходным данным;
Если свойство для объекта не определено,
то и описанная функция на этом объекте не определена.

Если П — проверка, а Г — действие, то мы получаем описание действия.

Более детально: перейти от проверки П к действию $\underline{\text{П}}$, ...

Повторение (итерация, цикл)

Пусть П — описание свойства, Г — описание функции, тогда

- Пока П
  - Г

описание функции:

Если на исходном данном свойство П — Л,
то результат применения функции совпадает с исходным данным.
Если значение П — И,
то нужно применить Г, снова проверить П, если П даст значение Л,
то остановиться, и т. д.
Если в какой-то момент П или Г не дает значения,
то и описываемая функция — не определена.
Если П никогда не дает значения Л,
то описываемая функция тоже не определена.

Если П — описание проверки, а Г — описание действия, то ...

Логические операции

- Если П и С — описания свойств, то П и С, П или С, не П — описания свойств.
- Если П и С — проверки, то получается проверка, значение задается приведенной таблицей.
- Какое значение имеет комбинация двух свойств, когда одно из них — не определено?
- Естественная договоренность:
  - Если имеющихся значений элементов комбинации достаточно, чтобы указать значение комбинации, то мы его и берем.
  - Если имеющихся значений недостаточно, то значение комбинации не определено.
  - Отрицание истины — ложь, лжи — истина, неопределенности — неопределенность.
  - Если в конъюнкции один из членов ложен, то конъюнкция ложна, если оба истинны, то конъюнкция истинна, в остальных случаях — не опр., и т. д.

Алгоритмы

- Понятие алгоритма, является исходным и неопределяемым.
  Свойства: Алгоритм — описание вида
  - А
  - Пока Б
    - В
  - Г

  где А, В, Г — описания действий, Б — описание проверки
- А — начало
- Б — продолжение
- В — переработка
- Г — извлечение результата

Интуитивные соображения ...

Алгоритмы. Вычислимые функции

- Исходные данные и результаты — обычно, слова в алфавите $\{0, 1\}$. Промежуточные результаты — также слова в некотором — третьем, алфавите.
- Алгоритм задает функцию из слов в алфавите исходных данных в слова в алфавите результатов.
- Алгоритм вычисляет эту функцию.
- Вычислимая функция — это функция, вычисляемая некоторым алгоритмом.
- Вычислимое свойство — аналогично.
- Множество, отношение называется разрешимым, если его характеристическая функция вычислима.
  (Характеристические функции — всюду определены.)

Теоремы замкнутости для вычислимых функций

- **Теорема.** Операции композиции, итерации, ветвления в применении к вычислимым функциям и вычислимым свойствам дают вычислимые. Операции логики в применении к вычислимым свойствам дают вычислимые, к разрешимым свойствам дают разрешимые.

Композиция

Описание (алгоритм для f)

Начало

- Начало f

Продолжение

- Пока Продолжение f

Переработка

- Переработка f

Извлечение результата

- Извлечение результата f

Композиция

Описание (алгоритм для g)

Начало

- Начало g

Продолжение

- Пока Продолжение g

Переработка

- Переработка g

Извлечение результата

- Извлечение результата g

Композиция

Как построить описание для g(f( ))?

Интуитивно очевидно. Более формально:

Ячейки: Этап, Продолжение

Начало

- Начало f
- Этап $\leftarrow$ f

Композиция

Продолжение

- Если Этап = f
  - Продолжение ← Продолжение f
  - Если не Продолжение
    - Извлечение результата f
    - Начало g
    - Этап ← g
- Если Этап = g
  - Продолжение ← Продолжение g

Переработка

- Если Этап = g
  - Переработка g
- Если Этап = f
  - Переработка f

Извлечение результата

- Извлечение результата g

Перечислимые множества

О. Перечислимое множество — это множество значений вычислимой функции.

Т. Следующие свойства множества эквивалентны:

1. Оно — перечислимо.
2. Оно — область определения вычислимой функции.
3. Оно — породимо.

Можно указать общие способы (алгоритмы) построения по любому из описаний 1 — 3 любого другого.

При доказательстве нам может пригодиться тот факт, что ансамбль всех слов перечислим в следующем смысле: есть действие S, для которого множество Λ, $S(\Lambda)$, $S(S(\Lambda))$, ... содержит все элементы ансамбля.

Замечания

Перечислимое множество пусто или является множеством значений всюду определенной вычислимой функции.

Однако, имея описание 1 — 3 такое описание не построить! (увидим далее).

Связь вычислимости и породимости особенно замечательна.

Перечислимые множества

Т. Функция вычислима $\Longleftrightarrow$ ее график перечислим.

Вычислимость можно определить через породимость.

Перечислимость и разрешимость

Т. Множество разрешимо $\Longleftrightarrow$ оно и его дополнение перечислимы.

Содержание лекции

- Проблематика и история
- Функции и свойства
- Описания, действия, проверки
- Исчисления, замкнутость
- Операции над функциями, проверками, их описаниями
- Алгоритмы, вычислимые функции, разрешимые множества. Замкнутость.
- Перечислимые множества. Эквивалентность понятий.

alsemenov@umail.ru