Введение в математическую логику и теорию алгоритмов

Лекция 10

Алексей Львович Семенов

Утверждение, которое вы сейчас видите на экране, – *ложно*.

Формализация

Утверждение в формальном языке, говорящее о собственной истинности (ложности)

Арифметики

Желаемое:

• Арифметика = Настоящие натуральные числа и операции.

• Эта Арифметика полностью описывается Аксиомами, то есть:

Все свойства натуральных чисел могут быть выведены из Аксиом.

Леопольд Кронекер:

Бог создал натуральные числа, всё остальное — создание человека.

Арифметики

Реальность:

- Существует много арифметик, не изоморфных (Настоящим) натуральным числам (с операциями), но со всеми свойствами натуральных чисел
  - обсуждалось раньше.
- Не существует системы аксиом, из которых могут быть выведены все свойства натуральных чисел (и только они)
  - **тема сегодня.**

Аксиоматика Пеано – PA

1. Аксиомы равенства для S, +, x;
2. $\neg S(a) = 0, \quad S(a) = S(b) \rightarrow a = b,$
3. $a + 0 = a, \quad a + S(b) = S(a + b),$
4. $a \times 0 = 0, \quad a \times S(b) = a \times b + a,$
5. (Схема аксиом индукции)

$\Phi[x/0] \wedge \forall u\,(\Phi[x/u] \rightarrow \Phi[x/S(u)]) \rightarrow \forall u \Phi[x/u]$

для любой формулы Φ.

У Пеано – для любого свойства Ф.

Кодирование

- Язык логики отношений при фиксированной сигнатуре.
- Слова в алфавите языка логики отношений кодируются натуральными числами (которые можно считать словами в алфавите {0, 1}). Операция Код.
- При необходимости можно кодировать натуральными числами также последовательности слов.

Модель М (вариант арифметики)

Область (носитель) – натуральные числа, представленные своими двоичными записями (словами в алфавите {0,1}).
Будем использовать функции, а не только отношения.
В сигнатуре есть 0,1, функции +, x, может быть, кроме этого, операция приписывания слов и др.

- **Пусть А есть код слова Т, и пусть U получается подстановкой Б вместо свободной переменной *x* в Т.**
- **Тогда обозначим через Подст (А, Б) код слова U.**
- **Функция подстановки Подст выразима в *M*.**
- **Это означает существование формулы ПОД(x, y, z), истинной тогда и только тогда, когда z = Подст(x, y).**
- **Будем использовать сокращённую запись и писать Ф(Подст(x, y)) вместо $\exists z$ (Ф(z) & ПОД(x, y, z)).**
- **Отметим, что если Г – формула с одной свободной переменной *x*, то Подст(код Г, Б) = код Г(Б).**

Гёделева диагональ

Ф – формула с одной свободной переменной *x*

Г = ¬ Ф (Подст(*x*,*x*))

Г (код Г) = ¬ Ф (Подст (код Г, код Г)) = ¬ Ф (код Г (код Г))

Теорема Тарского. Не существует формулы Ф, выражающей свойство: «быть кодом истинного в модели М утверждения».

Д. Предположим, такая формула Ф существует.

- **Пусть**: Г (код Г) – истинно. **Тогда**: Ф (код Г (код Г)) – истинно,
  ¬ Ф (код Г (код Г)) – ложно,
  Г (код Г) – ложно.

- **Пусть**: Г (код Г) – ложно. **Тогда**: Ф (код Г (код Г)) – ложно,
  ¬ Ф (код Г (код Г)) – истинно,
  Г (код Г) – истинно.

Гёделева диагональ

- Ф – формула с одной свободной переменной
- Г = ¬ Ф (Подст(*x*,*x*))
- Г (код Г) = ¬ Ф (Подст (код Г, код Г)) = ¬ Ф (код Г (код Г))

Пусть в нашей модели М для всякого исчисления над алфавитом {0,1} выразимо свойство «быть кодом выводимого в этом исчислении слова».

Теорема Гёделя. Не существует исчисления, порождающего в точности истинные формулы в нашей модели.

Д. Пусть такое исчисление существует, и Ф выражает свойство «быть кодом выводимого слова».

Пусть: Г (код Г) – истинна. **Тогда**: она выводима.

Ф (код Г (код Г)) – истинно,
¬ Ф (код Г (код Г)) – ложно,
Г (код Г) – ложно.

Пусть: Г (код Г) – ложна. **Тогда**: она не выводима.

Ф (код Г (код Г)) – ложно,
¬ Ф (код Г (код Г)) – истинно,
Г (код Г) – истинно.

Соотношение с обычной арифметикой

- Подстановка и выводимость («быть кодом выводимой формулы») могут быть выражены через приписывание, а приписывание – через +, ^{x} . Приписывание несущественно расширяет арифметику.
- Сигнатура приписывания не менее естественна, чем сигнатура сложения и умножения.
- В рассматриваемой сигнатуре могут быть +, ^{x} .
- Существуют и более богатые теории, например, теория множеств.
- Все эти утверждения мы доказывать не будем.

Естественные недоказуемые утверждения

- Важные теоремы и проблемы теории чисел, комбинаторики, математической логики, теории вычислений и т. д. можно формулировать в арифметике.
- Постепенно для многих из них удается найти доказательства, решения и т. д.
- Теорема Геделя показывает, что иногда это может быть и не так – возможны утверждения, для которых доказательство или опровержение (в теории Пеано) не будет найдено никогда.
- Однако в теореме Геделя утверждение «диагональное», «самоприменимое», «специально построенное», говорит что-то о самой теории и доказуемости и т. д.
- Есть ли «естественные» утверждения арифметики, не доказуемые и не опровержимые?

Истинное, но не доказуемое в PA утверждение

Червь Беклемишева

- *Червём* будем называть произвольную цепочку натуральных чисел.
- *Нос* червя – последний элемент цепочки.
- *Голова* червя – максимальный конец цепочки (включая нос), все элементы которого не меньше носа.
- *Хвост* червя – оставшаяся начальная часть цепочки(хвост может быть пустым).
- В примерах голова – красная (нос – тёмно-красный), хвост – зелёный:

(а) **7 6 1 2 3 4 6 5 4**

(б) **7 6 1 2 3 4 6 3 4**

(в) **7 6 1 2 3 4 6 3 0 1 0 0 0**

(г) **3 7 6 7 8 9 8 4 6 3 3 4 3**

Истинное, но не доказуемое в PA утверждение

Эволюция червя

- Эволюция червя происходит по шагам. После каждого шага заново определяем, где у червя хвост, голова, нос.
- Если нос равен 0, то отрезаем его, и на следующем шаге последовательность становится на 1 короче.
- Если на (k-1)-м шаге нос не равен 0, то на k-м шаге к голове червя приделываем ещё k копий головы и в каждой из (k+1) копий нос уменьшаем на 1.
- Пример 1:

  $w_0 = \mathbf{0}$

  $w_1 = \Lambda$

  Пример 2:

  $w_0 = \mathbf{1}$

  $w_1 = \mathbf{0\ 0}$

  $w_2 = \mathbf{0}$

  $w_3 = \Lambda$

Истинное, но не доказуемое в PA утверждение
Эволюция червя. Пример 3.

- $w_0 = 2$
- $w_1 = 1\ 1$
- $w_2 = 1\ 0\ 1\ 0\ 1\ 0$ $w_3 = 1\ 0\ 1\ 0\ 1$ $w_4 = 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0$
- $w_5 = 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0$ $w_6 = 1\ 0\ 1\ 0\ 0\ 0\ 0$
- $w_7 = 1\ 0\ 1\ 0\ 0\ 0$ $w_8 = 1\ 0\ 1\ 0\ 0$
- $w_9 = 1\ 0\ 1\ 0$
- $w_{10} = 1\ 0\ 1$
- $w_{11} = 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0$
- . . .
- $w_{23} = 1\ 0$ $w_{24} = 1$ $w_{25} = 0\ 0^{25}$
- …
- $w_{50} = 0$
- $w_{51} = \Lambda$

Истинное, но не доказуемое в PA утверждение
Эволюция червя. Пример 4.

- $w_0 = 3$
- $w_1 = 2\ 2$
- $w_2 = 2\ 1\ 2\ 1\ 2\ 1$
- $w_3 = 212120\ 212120\ 212120\ 212120$
- $w_4 = 212120\ 212120\ 212120\ 21212$
- $w_5 = 212120\ 212120\ 212120\ 2121\ 111111$
- $w_6 = (212120)^3\ (2121111110)^7$
- $w_7 = (212120)^3\ (2121111110)^6\ 212111111$
- $w_8 = (212120)^3\ (2121111110)^6\ (212111110)^9$
- $w_9 = (212120)^3\ (2121111110)^6\ (212111110)^8\ 21211111$
- $w_{10} = (212120)^3\ (2121111110)^6\ (212111110)^8\ (21211110)^{11}$
- . . .

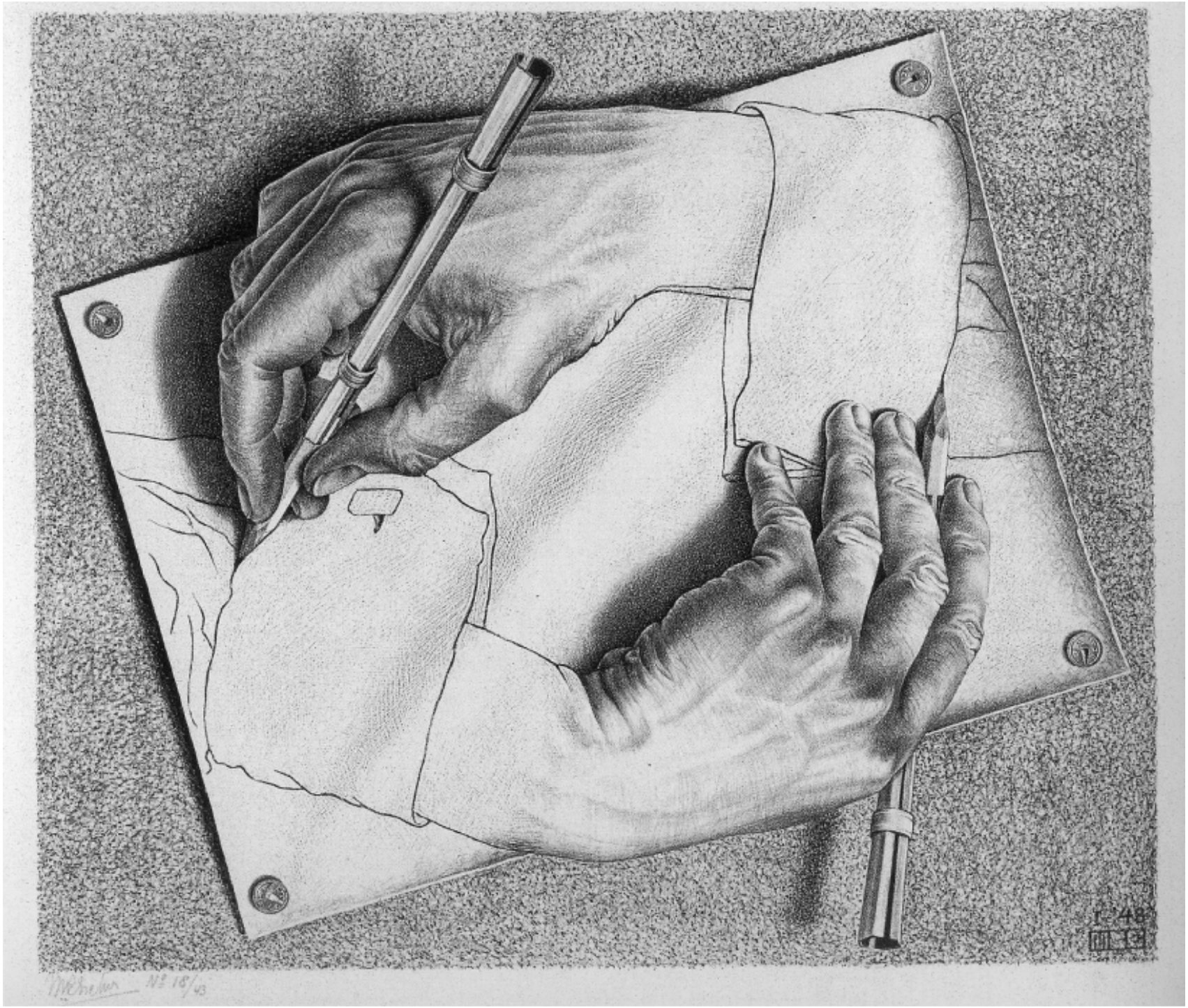
Истинное, но не доказуемое в PA утверждение

- **Утверждение.** Любой червь в процессе эволюции рано или поздно (но скорее поздно, чем рано) исчезнет (превратится в пустую последовательность).
- **Утверждение.** Предыдущее утверждение истинно, но не доказуемо в арифметике Пеано PA.

Теорема Гёделя

- Пропасть между доказуемостью и истинностью, между математикой и реальностью

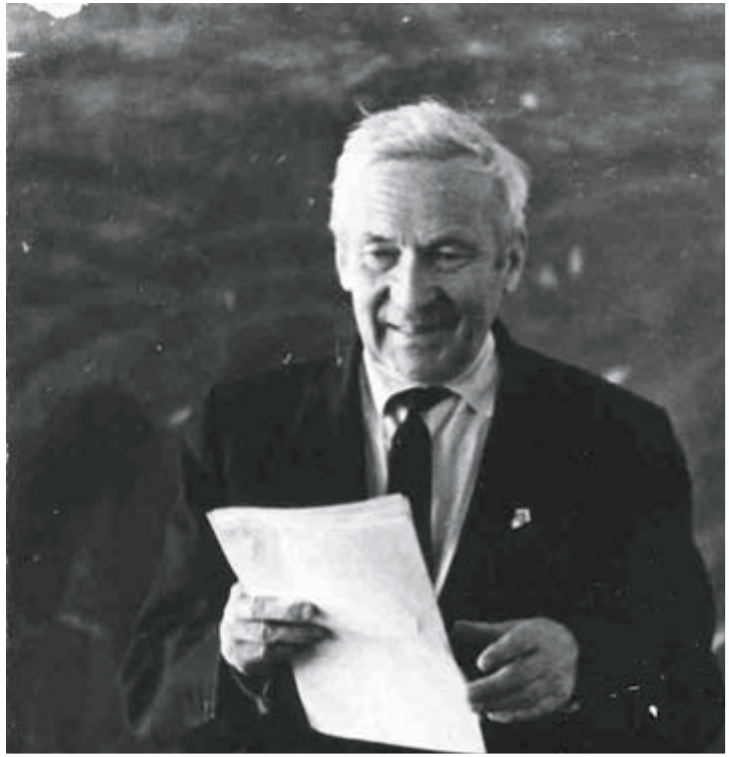
В 1999 году
"Time magazine"
провозгласил
Гёделя
самым великим
математиком XX века
и включил его в список
"Ста великих людей
столетия".



Наименьше число, которое нельзя описать короче, чем десятью словами.

Сложность объекта

- да, да, да, …, да (1 млн. раз)
- На экране нет миллиона «да».
- Есть описание объекта.
- Сложность объекта
  – минимальная длина
  его описания.
- **Андре́й Никола́евич Колмого́ров**
  25.04.1903 – 20.10.1987



Сложность объекта

- Что такое описание?
- Аргумент для
  - машины,
  - алгоритма,
  - вычислимой функции, дающей объект.
- Вычислимая функция (дающая объект по его описанию) – способ описания.

Будем считать, что объекты и описания – двоичные слова.

- *Сложность при данном способе описания:*

$K_f(x) = \min \{|y| \mid f(y)=x\}$,
где $|y|$ – длина слова y;
если такого y, что f(y)=x, нет, то min = ∞.

Сложность объекта

- Описания бывают разные.
- f(0) = «сложный» объект (один).
- Есть ли способ описания, дающий самые короткие описания?
- Нет (очевидно).
- Можно ли получать описания, самые короткие «с точностью до» дополнительного слагаемого?
- **Теорема Колмогорова**. Существует способ описания u, такой, что для любого способа описания f найдется такое число C, что для всякого объекта x выполнено:

$$K_u(x) \le K_f(x) + C.$$

Идея доказательства: сообщать способ описания вместе с описанием.

Теорема Колмогорова

$$K_u(x) \le K_f(x) + C$$

- Д. Фиксируем некоторый вариант задания вычислимых функций алгоритмами, например, алгоритмами Маркова.
- Как мы видели на второй лекции, существует универсальная функция u:
  для всякой вычислимой функции f, если p – задание (программа) f, то для всех y: f(y) = u(<p,y>).
- Возьмем произвольное x и такое y, что f(y) = x.

  $K_u(x) \le |\langle p,y\rangle|$, y можно взять самым коротким.
- Осталось доказать, что $|\langle p,y\rangle| \le |y| + C$.
- Здесь C может зависеть от p, но не от x.
- Каким нужно взять кодирование пар?

Кодирование пар

- Уже было на 1-ой лекции.
- Нужно добиться экономии по второму аргументу.
- Просто *py*? Где заканчивается *p*?
- Можно удвоить каждый символ *p*, а после *p* поставить 01. Дальше может идти *y*.
- Тогда $|\langle p,y\rangle| = 2+2|p|+|y|$.
- Цель достигнута: $C = 2+2|p|$.
- Теорема Колмогорова доказана.

Можно ли короче (достаточно знать, где кончается *p*)?

- Почему нельзя короче, чем $|p|+|y|$?

Применение сложности объектов (колмогоровской сложности)

- Случайность
- Бросание монеты
- 011010010101111001001010…
- 010101010101010101010101…
- Вторая последовательность неслучайна?
- Вероятность

одинакова.

- Сложность

разная.

- Последовательность случайна, если ее (колмогоровская) сложность – максимальна.
- Информация в одном объекте о другом…

http://www.youtube.com/watch?v=j4cYiCq_Hvc

Введение в математическую логику и теорию алгоритмов

Лекция 10

3 ноября 2012 г.

Изменения внесены 8 ноября 2012 г.