Введение в математическую логику и теорию алгоритмов

Лекция 13

Алексей Львович Семенов

План

- Парадоксы самоприменимости
- Теорема Тарского о невыразимости истины
- Теорема Геделя о неполноте
- Теорема Геделя о недоказуемости непротиворечивости
- Программа Гильберта
- Недоказуемость «естественного» утверждения
- Сложность объекта
- Теорема Колмогорова
- Что такое случайность?

Утверждение, которое вы сейчас видите на экране, –

ложно.

Формализация

- Утверждение в формальном языке, говорящее о собственной истинности

Арифметики

Желаемое:

- Арифметика = Настоящие натуральные числа и операции (или слова…)
- Эта Арифметика полностью описывается Аксиомами.
- Все свойства натуральных чисел могут быть выведены из Аксиом.

Арифметики

Реальность:

- Существует много арифметик, не изоморфных

Настоящим натуральным числам (с операциями), но со всеми свойствами натуральных чисел.

– обсуждалось раньше (нестандартные модели с бесконечно большими элементами…)

- Не существует системы аксиом, из которых

могут быть выведены все свойства («настоящих») натуральных чисел, записываемые в логике отношений (и только они)

– тема сегодня

Кодирование

- При фиксированной сигнатуре – язык логики отношений.
- Слова в алфавите языка логики отношений кодируются в алфавите {0, 1}.
- Цепочки слов – тоже кодируются.
- Операция Код.
- Уже обсуждалось – добавить запятую и т. д.

Структура M (вариант арифметики)

Область (носитель) – слова в алфавите {0,1}.

В сигнатуре есть 0,1 и операция приписывания слов, могут быть, кроме этого, +, x и др. Слова в алфавите {0,1} – термы (но могут быть и другие термы).

Выразима функция подстановки (можно обойтись без функций, используя только символы для отношений):

• Подст: Код слова, получаемого подстановкой в формулу, кодом которой является первый аргумент, второго аргумента вместо свободной переменной *x.*

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))

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

Д. Предположим, такая формула Ф существует. Построим Г для Ф.

Пусть: Г (код Г) – истинно. **Тогда**:

Ф (код Г (код Г)) – истинно (Предпол.),
¬ Ф (код Г (код Г)) – ложно, т.е.
Г (код Г) – ложно.

- **Пусть**: Г (код Г) – ложно. **Тогда**:

Ф (код Г (код Г)) – ложно (Предпол.),
¬ 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 структуре М для всякого исчисления над алфавитом {0,1} выразимо свойство «быть кодом выводимого в этом исчислении слова».

Теорема Гёделя о неполноте. Не существует исчисления, порождающего в точности истинные в нашей структуре формулы.

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. Противоречие.

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. Противоречие.

Теорема Геделя о неполноте

- Другое доказательство
- **Задача**. Множество истинных формул – неперечислимо.
- Подсказка. Всякое перечислимое множество можно выразить в арифметике.
- **Задача**. Как из этих соображений получить Т. Геделя?

Программа Гильберта.

Полнота. Невозможна, в силу Теоремы Геделя о неполноте.

Непротиворечивость. Доказательство невозможности получить противоречие надежными, «финитными» средствами. (Как невозможность получить какую-то позицию в шахматной игре.)

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

Пусть Ф выражает свойство «быть кодом выводимого слова».

Аксиоматическая теория – исчисление, получаемое добавлением к исчислению логики отношений каких-то аксиом.

Формула Непр = ¬Ф(код 0), здесь 0 – Ложь, из нее выводится все.

Вторая теорема Гёделя о неполноте. Не существует непротиворечивой аксиоматической теории, в которой выводимо утверждение о ее непротиворечивости, то есть Непр – невыводимо.

Задача. Как может выглядеть доказательство?

Таким образом, непротиворечивость не может быть установлена не только «финитными» средствами, но даже средствами самой теории.

Соотношение с обычной арифметикой

- Сигнатура приписывания не менее естественна, чем сигнатура сложения и умножения.
- В рассматриваемой сигнатуре могут быть +, $\times$.
- Подстановка и выводимость («быть кодом выводимой формулы») могут быть выражены через приписывание, а приписывание – через +, $\times$. Приписывание несущественно расширяет арифметику.
- Более богатые структуры, например, теория где возможны кванторы по подмножествам натурального ряда.

Арифметика Пеано

Аксиомы, в добавление к аксиомам исчисления логики отношений

Аксиомы Пеано (замыкания формул)

1. Аксиомы равенства для S, +, $\times$,

2. $\neg\, S(a) = 0, \quad S(a) = S(b) \to a = b,$

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)

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

для любой формулы Φ.

(У Джузеппе Пеано аксиомы были другие.)

Практика показывает, что этого достаточно.

Программа Гильберта

- Арифметика Пеано не полна.
- Теория множеств (она будет сформулирована) – не полна (или противоречива).
- Доказательство непротиворечивости невозможно.
- Возможна ли математика?

Естественные недоказуемые утверждения

- Важные теоремы и проблемы теории чисел, комбинаторики, математической логики, теории вычислений и т. д. можно формулировать в арифметике.
- Постепенно для 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 последовательности (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 цепочка 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.

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

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}= **$(212120)^3$ $(2121111110)^6$ $(212111110)^8$ $(21211110)^{11}$**
- . . .

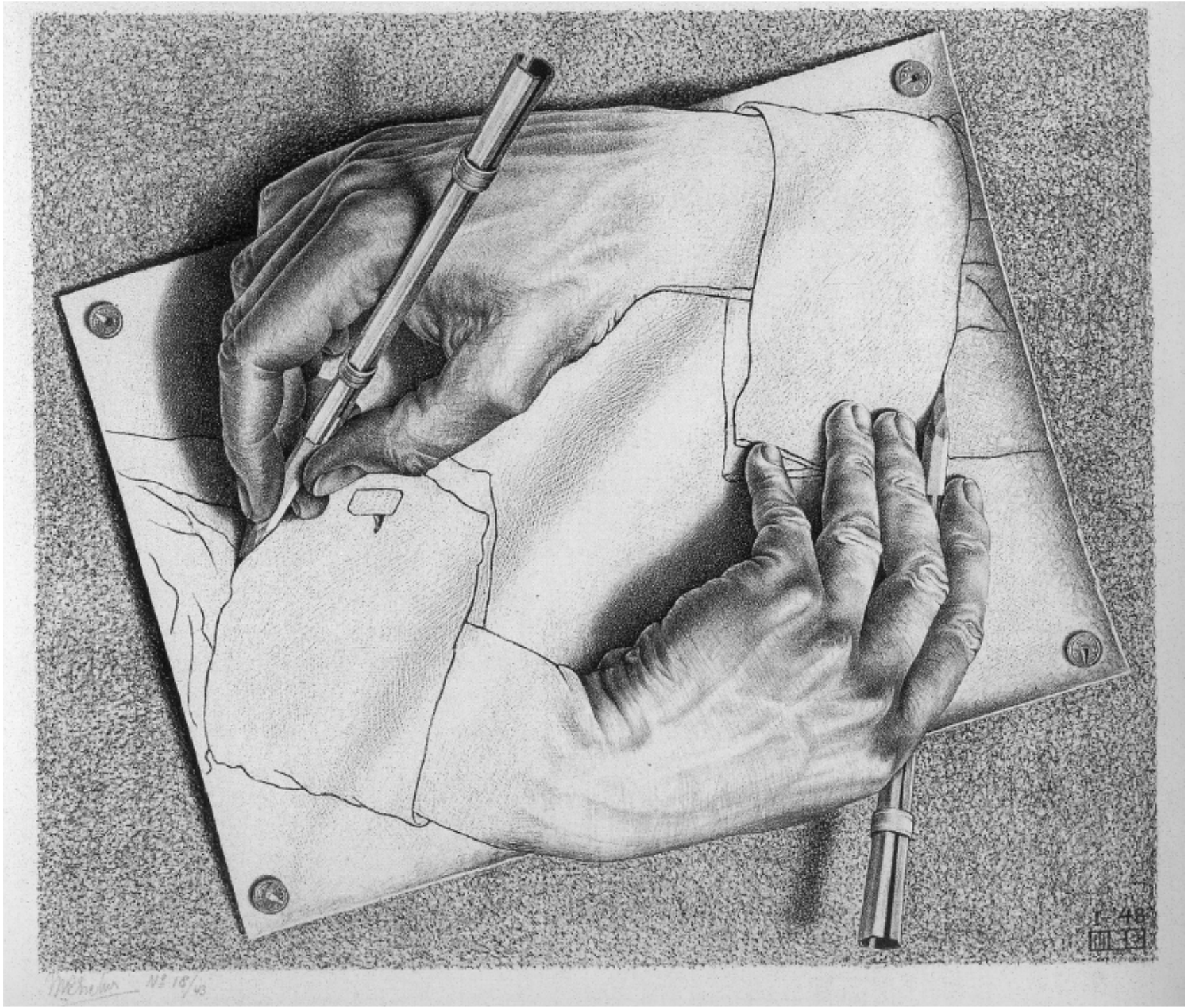
Истинное, но не доказуемое в PA утверждение

- **Утверждение.** Любой червь в процессе эволюции рано или поздно (но скорее поздно, чем рано) исчезнет (превратится в пустую цепочку).
- **Задача**. Доказать утверждение.
- **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".



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

Сложность. Подход теории алгоритмов

Сложность объекта

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

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 объекта x при данном способе f описания*

$$K_f(x) = \min \{|y| \mid f(y) = x\},$$

где $|y|$ – длина слова y;

если y нет, то $\min = \infty$.

Сложность объекта

- Способы описания бывают разные.
- Есть ли способ описания, дающий самые короткие описания?
- Нет (очевидно):

  f(0) = «сложный» при другом описании объект.
- Можно ли получать описания, самые короткие «с точностью до» дополнительного слагаемого?
- Да. Точная формулировка:
- **Теорема Колмогорова**. Существует способ описания u, такой, что для любого способа описания f найдется такое число C, что для всякого объекта x выполнено:

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

Теорема Колмогорова

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

- Д. Фиксируем некоторый вариант задания вычислимых функций алгоритмами, например, алгоритмами Маркова.
- Как мы видели, 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. Тогда:

  u(<p,y>) = x

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

Кодирование пар

- Нужно добиться экономии по второму аргументу.
- Просто py?
- Где заканчивается p?
- Можно удвоить каждый символ p, а после p поставить 01.
- Тогда $|\langle p,y\rangle| = 2+2|p|+|y|$.
- Цель достигнута: $C = 2+2|p|$.
- Теорема Колмогорова доказана.
- **Задача**. Можно ли короче (достаточно знать длину p)?
- **Задача**. Почему нельзя короче, чем $|p|+|y|$?

Применение сложности объектов (колмогоровской сложности)

- Случайность
- Бросание монеты
- 01101001010111001001 01…
- 01010101010101010101 01…
- Вторая последовательность неслучайна?
- Вероятность

одинакова.

- Сложность

разная.

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