Введение в математическую логику и теорию алгоритмов

Лекция 10

Алексей Львович Семенов

План

- Программа Гильберта
- Непротиворечивая и полная математика.
- Логика отношений
- Исчисление логики отношений
- Исчисления
- Породимые множества
- Грамматики. Тезис Поста

Программа Гильберта

- Построение непротиворечивой и полной математики
  - Построение аксиоматической теории – исчисления («игры»)
  - Доказательство непротиворечивости и полноты «надежными», «финитными» средствами (анализом «игры»)

Логика отношений

- **Синтаксис: Индуктивное построение формул**
- **Семантика: Интерпретации**

Отношения, задаваемые формулами логики отношений (Семантика)

- Множество D
- Отношения – подмножества $D^{\mathbf{N}}$
- Конечное число аргументов
- Имена отношений $\sum$, Зн
- Свободные переменные $x_1, \dots$
- Формулы $R(\boldsymbol{x})$ и $Q(\boldsymbol{x})$ эквивалентны в структуре M т. е. $M \vDash R(\boldsymbol{x}) \equiv Q(\boldsymbol{x})$ титтк

значения $R(\boldsymbol{x})$ и $Q(\boldsymbol{x})$ (отношения в D^{N}) совпадают.

- Формулы эквивалентны, если они эквивалентны в любой структуре (данной сигнатуры).

Предваренная нормальная форма

- Формула находится в предваренной нормальной форме (п.н.ф.), если она не содержит кванторов, или имеет вид:
- $Q_1x_1\ldots Q_nx_n\Phi$, где Q – это $\forall$ или $\exists$**,** а в Φ кванторов нет.
- **Задача**. Дать индуктивное определение формулы (находящейся) в п.н.ф.
- **Задача**. Построить алгоритм, который по всякой формуле логики отношений строит формулу (находящуюся) в п.н.ф., ей эквивалентную (ее предваренную нормальную форму).
- Можно переименовывать связанные переменные…

Предваренная нормальная форма

$\models (\forall u\ \Phi[u/x]) \equiv (\forall v\ \Phi[v/x])$

$\models (\exists u\ \Phi[u/x]) \equiv (\exists v\ \Phi[v/x])$

$\models (\mathbf{Q}u\ \Phi[u/x])\ \tau\ \Psi \equiv (\mathbf{Q}u\ (\Phi[u/x]\ \tau\ \Psi))$, $\tau \in \{\wedge, \vee\}$, $\mathbf{Q} \in \{\forall, \exists\}$

$\models (\neg\ (\forall u\ \Phi[u/x])) \equiv (\exists v\ \neg\Phi[v/x])$

$\models (\neg\ (\exists u\ \Phi[u/x])) \equiv (\forall v\ \neg\Phi[v/x])$

Теоремы о логике отношений

Теорема перечислимости.

Множество общезначимых формул перечислимо: есть процесс деятельности, позволяющий для всякой общезначимой формулы когда-нибудь узнать, что она общезначима.

Теорема компактности для счетного множества утверждений.

Если любое конечное подмножество теории имеет модель, то и вся теория имеет модель.

Задача. Как обстоит дело с общезначимыми и с необщезначимыми формулами в логике высказываний?

Исчисление для логики отношений (дедуктика)

• Аксиоматическая система – индуктивное определение, формализующее практику математических доказательств.

Частные случаи тавтологий логики высказываний в логике отношений

- Возьмем тавтологию логики высказываний, например:
  $A_1 \to (A_2 \to A_1)$.   (*)
- Подставим в (*) вместо имен высказываний A_1 и A_2 формулы (замкнутые или незамкнутые) логики отношений.
- Например, вместо A_1 подставим $\forall u_1(P_5(u_1))$,
  а вместо A_2 подставим $P_4(x_1,x_1)$:
  $\forall u_1(P_5(u_1)) \to (P_4(x_1,x_1) \to \forall u_1(P_5(u_1)))$.
- То, что получилось, называется *частным случаем тавтологии* (*) логики высказываний в логике отношений.
- Любая такая формула истинна в любой структуре при любой интерпретации.
- Вместо «частный случай тавтологии…» говорим просто «тавтология».

Исчисление логики отношений

- Фиксируем сигнатуру $\Sigma = \langle Pr \rangle$.
- Исчисление (одно для данной сигнатуры) задаётся *аксиомами* (являющимися формулами сигнатуры Σ) и *правилами вывода*.
- **Аксиомы**:

A1. частные случаи тавтологий логики высказываний,

A2. формулы вида $\forall u\ \Phi[u/x] \to \Phi[t/x]$,

A3. формулы вида $\Phi[t/x] \to \exists u\ \Phi[u/x]$,

где Φ – формула, x – свободная переменная ($x \in FVar$), u – связанная переменная ($u \in BVar$), не входящая в Φ, t – свободная переменная.

Исчисление логики отношений

Правила вывода:

R1 $$\frac{\Phi, \quad \Phi \to \Psi}{\Psi}$$ (modus ponens, (MP))

R2 $$\frac{\Phi \to \Psi}{\Phi \to \forall u\, \Psi[u/x]}$$

R3 $$\frac{\Psi \to \Phi}{\exists u\, \Psi[u/x] \to \Phi}$$

<u>Индуктивное определение.</u>

Аксиомы выводимы.

Если уже выведены формулы, написанные в верхней части правила, то написанная внизу формула - выводима.

В R2, R3 x не входит в Φ.

Правила R2 и R3 называются правилами Бернайса.

Примеры выводов

Пример 1. (1) $\vdash \forall u\ P(x)\ [u/x] \to P(x)\ [x/x]$ (аксиома А2)

$\vdash \forall u\ P(u) \to P(x)$ (аксиома А2)

(2) $\vdash \forall u\ P(u) \to \forall v\ P(v)$ (по правилу R2 из (1))

(В этом выводе P – имя одноместного отношения.)

Пример 2. Пусть Φ - любая формула в нашей сигнатуре.

(1) $\vdash (\forall u\ \Phi[u/x] \to \Phi) \to ((\Phi \to \exists u\ \Phi[u/x]) \to (\forall u\ \Phi[u/x] \to \exists u\ \Phi[u/x]))$

(Частный случай тавтологии

$(A \to B) \to ((B \to C) \to (A \to C))$.)

(2) $\vdash \forall u\ \Phi[u/x] \to \Phi$ (А2, Φ – это $\Phi[\ x/x\ ]$)

(3) $\vdash (\Phi \to \exists u\ \Phi[u/x]) \to (\forall u\ \Phi[u/x] \to \exists u\ \Phi[u/x])$

(по МР из (2) и (1))

(4) $\vdash \Phi \to \exists u\ \Phi[u/x]$ (А3)

(5) $\vdash \forall u\ \Phi[u/x] \to \exists u\ \Phi[u/x]$ (по МР из (4) и (3))

Пример вывода (повторение)

Пример 3. (Используем обычное обозначение для двуместного отношения «меньше или равно».)

(1) $\vdash \forall u\,(u \leq y) \to x \leq y$ (A2, терм $t = x$)

(2) $\vdash x \leq y \to \exists v\,(x \leq v)$ (A3, терм $t = y$)

(3) $\vdash \big(\forall u\,(u \leq y) \to x \leq y\big) \to$

$$\to \Big(\big(x \leq y \to \exists v\,(x \leq v)\big) \to \big(\forall u\,(u \leq y) \to \exists v\,(x \leq v)\big)\Big)$$

(частный случай тавтологии $(A \to B) \to \big((B \to C) \to (A \to C)\big)$)

(4) $\vdash (x \leq y \to \exists v\,(x \leq v)) \to (\forall u\,(u \leq y) \to \exists v\,(x \leq v))$ (по MP из (1) и (3))

(5) $\vdash \forall u\,(u \leq y) \to \exists v\,(x \leq v)$ (по MP из (2) и (4))

(6) $\vdash \forall u\,(u \leq y) \to \forall u\,\exists v\,(u \leq v)$ (по R2 из (5))

(7) $\vdash \exists v\,\forall u\,(u \leq v) \to \forall u\,\exists v\,(u \leq v)$ (по R3 из (6))

Заметим, что полученная формула – общезначима.

Истинность выводимого

Теорема об истинности выводимого. Всякая выводимая формула является общезначимой.

Структура доказательства (индукция по построению).

- A1 Частные случаи тавтологий логики высказываний – общезначимы.
- A2 Формулы вида $\forall u\, \Phi[u/x] \to \Phi[\, t\, /\, x]$ – общезначимы.
- A3 Формулы вида $\Phi[\, t\, /\, x] \to \exists u\, \Phi[u/x]$ – общезначимы.
- R1 Если формулы Φ и $\Phi \to \Psi$ общезначимы, то формула Ψ – общезначима.
- R2 Если формула $\Phi\to\Psi$ общезначима и Φ не содержит x, то формула $\Phi \to \forall u\, \Psi[u/x]$ – общезначима.
- R3 Если формула $\Psi\to\Phi$ общезначима и Φ не содержит x, то формула $\exists u\, \Psi[u/x] \to \Phi$ – общезначима.

Доказательство рассматривает определение истинности, значения на последовательности, и т. д.

Выводимость истинного

- **Теорема Гёделя о полноте**. Общезначимость в логике отношений совпадает с выводимостью в исчислении логики отношений.
- **Задача**. Доказать теорему.

Общее понятие исчисления. Предварительные определения

- Цепочка = конечная последовательность, которая может быть и пустой – Λ. Длина цепочки – число элементов в ней.
- Алфавит = конечная цепочка символов
- Слово (в данном алфавите) – цепочка символов этого алфавита.
- Ансамбль слов в данном алфавите – все слова. Часто: 0 1
- Ансамбль цепочек слов в данном алфавите – все цепочки слов.
- Ансамбль списков в данном алфавите – все списки, элементами которых являются слова или списки (индуктивное определение).
- **Задача**. Дать подробные индуктивные определения для понятий с этого экрана.

Действия и проверки. Описания

- Действие – исходное понятие. Действие:
  - Слово, являющееся текстом на понятном человеку языке;
  - может выполняться и человеком, и каким-то устройством,
  - можно применить к любому исходному данному из фиксированного ансамбля, при этом ясно, что всегда получается результат применения – элемент (возможно, другого) фиксированного ансамбля.
- Действие – задает всюду определенную функцию
- Проверка – действие с результатом 0 или 1
- Проверка задает характеристическую функцию множества (где она дает 1), мы говорим, что она допускает его элементы (а другие – не допускает)

Исчисления. Создаваемые объекты

- Исчисление в данном ансамбле – это пара из двух проверок:
- <проверка создания, проверка окончания>.
- проверка создания применяется к цепочке объектов, проверка окончания – к объекту.
- создаваемый исчислением объект индуктивно определяется так:

  Если проверка создания допускает цепочку объектов $a_1, \ldots a_n$ и все элементы этой цепочки, кроме последнего – создаваемы, то и последний элемент создаваем.

- Если проверка создания допускает цепочку из одного элемента, то его называют начальным объектом (в некоторых контекстах – аксиомой).
- **Задача**. Что, если таких у данного исчисления нет?

Исчисления. Породимые множества

- Объект <u>порождаем данным исчислением</u>, если он создаваем и его допускает проверка окончания.
- Исчисление порождает множество из всех порождаемых им объектов – множество, <u>порождаемое</u> этим исчислением.
- <u>Породимое</u> множество – множество, порождаемое каким-то исчислением.

Эмиль Пост
(11.02.1897 — 21.04.1954)

Вывод

- Фиксируем исчисление.
- Если $a_1, \ldots, a_n$ – допускается проверкой создания, то говорим. что a_n <u>создается из</u> $a_1, \ldots, a_{n-1}$ (в данном исчислении).
- <u>Вывод</u> объекта а – цепочка объектов S, каждый из которых создается из какой-то цепочки объектов, встретившихся в S раньше него.
- **Задача**. Объект создаваем тогда и только тогда, когда у него имеется вывод.
- **Задача**. Пусть дано исчисление. Как организовать процесс выписывания всех выводов?
- **Задача**. Пусть дано исчисление. Как организовать процесс выписывания всех порождаемых (в нем) объектов (и только их)?

Примеры

Почему исчисление *K* модальной логики – это исчисление?

Проверка создания допускает:

- Цепочки из одной формулы (аксиомы)
  - Тавтологии
  - Все формулы $\square(A \to B) \to (\square A \to \square B)$.
- Цепочки из двух формул

  $\langle A, \square A \rangle$

  <*A,* подстановка в *A* формул вместо имен>.
- Цепочки из трех формул

  $\langle A, A \to B, B \rangle$.

Проверка окончания

Все подходит.

Задача. Описать все проверки подробно.

Задача. Почему определение формулы – это исчисление.

Теоремы замкнутости для исчислений

Т. Объединение и пересечение породимых множеств породимы.

Д. Объединение.

- А: <Проверка создания А, Проверка окончания А>,
- Б: < Проверка создания Б, Проверка окончания Б>.

Идея:

- Создаем слова, следуя Проверке А и следуя Проверке Б,
- Берем то, что создано или по той или по другой проверке.
- Проблема: как не перемешивать «по ходу дела» проверки А и Б?
- Выход: Метки для объектов, создаваемых по разным проверкам: Ах, Бу. Считаем, что символы А и Б в алфавит исчисления не входят.

Продолжение. Породимость объединения

- Припишем ко всем элементам цепочки, входящей в ту или иную Проверку создания, в начале символы А или Б.
- Объединим полученные проверки.
- Проверка создания допускает еще все пары <Ах,х>, где проверка окончания А допускает х, и пары <Бх, х>, где проверка окончания Б допускает х.
- **Задача**. Проверка окончания?

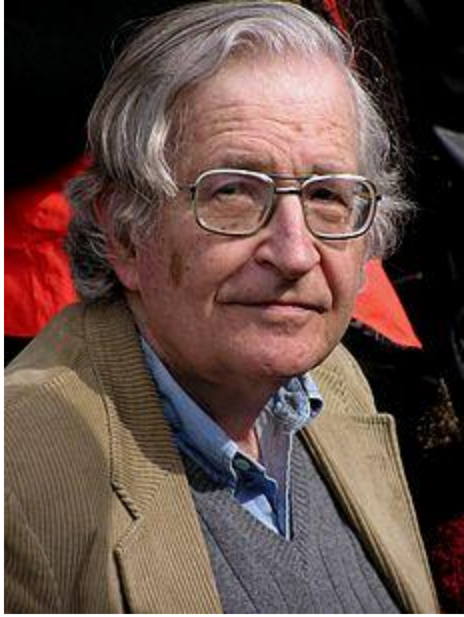
Задача. Почему пересечение проверок – проверка?

Задача. Доказать теорему для пересечения.

Задача. Как обстоит дело с дополнением?

Грамматики

(Ноам Хомски, 07.12.1928 -)



Определение.

Грамматика Г – это цепочка $\langle\Sigma,\Omega,\Pi,S\rangle$

Σ – основной алфавит Г

Ω – вспомогательный алфавит Г

S – начальный символ Г, $S \in \Omega$

$\Sigma\cap\Omega=\emptyset$, объединение Σ и Ω – это алфавит Г, обозначим его Δ.

П – это конечное множество пар слов в алфавите Δ. Эти пары называются заменами.

Грамматика

определяет исчисление Г*

Проверка создания Г* допускает:

- S
  - Всякий вывод в исчислении начинается с S.
- Для каждой замены <u,v> из П все пары вида <tup,tvp>, где t,p – произвольные слова в алфавите Δ
  - Один шаг вывода состоит в замене в слове некоторого входящего в него u на v.

Правило окончания для грамматики Г допускает все слова в алфавите Σ.

- Порождаемые слова не могут содержать букв из вспомогательного алфавита.

Описание грамматики – слово в конечном алфавите.

Примеры грамматик

- В них, следуя традиции, и для наглядности используется символ стрелочки в заменах и выводах.
- **Задача.** Как породить все цепочки из 0 и 1?
- **Решение.** $\Gamma = \langle \Sigma, \Omega, \Pi, S \rangle$, основной алфавит $\Sigma = \{0, 1\}$, вспомогательный алфавит $\Omega = \{S\}$,

  $\Pi = \{S \to S0,\ \ S \to S1,\ \ S \to \Lambda\}$.

  Пример вывода: $S \to S0 \to S10 \to S010 \to S0010 \to 0010$.
- **Задача.** Как породить все десятичные числа? (Пример десятичного числа: -3.141592.) Как породить все свободные переменные логики отношений?
- **Задача.** Что делает грамматика с основным алфавитом $\{a\}$, вспомогательным $\{S, B, M, E\}$ и правилами
- $\Pi = \{S \to BaE,\ B \to BM,\ Ma \to aaM,\ ME \to E,\ B \to \Lambda,\ E \to \Lambda\}$?
- **Задача.** Как породить все слова, состоящие из одинакового количества букв *a* и *b* ?
- **Задача.** Построить множество, которое породить грамматикой нельзя.

Тезис Поста (вариант).

Всякое породимое множество порождается некоторой грамматикой.

Соответствие между интеллектуальной реальностью и теоретико-множественной математикой