Введение в математическую логику и теорию алгоритмов

Лекция 9

Алексей Львович Семенов

План

- Определимость
- Предваренная нормальная форма.
- Многообразия
- Неопределимость
- Группы автоморфизмов. Соответствие Галуа
- Применения теоремы Свенониуса
- Исчисления модальных логик и модели для них
- Встречавшиеся примеры и общее понятие исчисления. Идея и реализация. Действия и проверки.

Отношения, задаваемые формулами логики отношений

- Множество D
- Отношения – подмножества D^N
- Конечное число аргументов
- Имена отношений $\sum$, Зн
- Свободные переменные x_0, x_1,…
- Формулы $R(\boldsymbol{x})$ и $Q(\boldsymbol{x})$ эквивалентны в структуре M, т. е. $M \models R(\boldsymbol{x}) \equiv Q(\boldsymbol{x})$, тогда и только тогда, когда 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

$$Q_0x_0Q_1x_1\ldots\ Q_nx_n\Phi,$$

где Q – это $\forall$ или $\exists$, а в Ф кванторов нет.

- **Задача**. Дать индуктивное определение формулы, находящейся в п.н.ф.
- **Задача**. Существует алгоритм, который по всякой формуле логики отношений строит эквивалентную ей формулу (находящуюся) в п.н.ф. (ее предваренную нормальную форму).
- Можно переименовывать связанные переменные…

Предваренная нормальная форма

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

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

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

$\mathbf{Q} \in \{\forall, \exists\}$

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

Многообразия

- Класс $\mathcal{K}$ отношений на *D.* Имена отношений – ∑, Зн.
- Формулы логики отношений в сигнатуре ∑
- Все определимые отношения – замыкание $\mathcal{K}$ – многообразие определимости – все, что можно «объяснить через $\mathcal{K}$»
- Примеры, которые были:
  - «между» определимо через «больше»,
  - экспонента определима через сложение и умножение натуральных чисел.
- **Задача**. Доказать, что всякое замыкание конечного множества отношений является замыканием одного отношения.
- Решетка многообразий определимости (объединение и пересечение) – было.
- Бескванторная определимость.
- **Задача**. Элиминация кванторов в порядке рациональных чисел.

Автоморфизмы

Структура $M = \langle D, \sum, \text{Зн} \rangle$

Автоморфизм φ – биекция (взаимно-однозначное отображение) D на себя, при которой сохраняются все отношения:

(Зн P)(***a***) = (Зн P)(φ(***a***)) для всякого P из $\sum$ и всякого ***a*** – набора элементов D.

Группа Aut (M)

Автоморфизмы упорядоченных множеств (порядков)

Задача. Каковы группы автоморфизмов порядков **N, Z, Q, R** ?

Тривиальная группа…, тривиальный ответ…

Задача. Aut ($\langle$ **N+Z,** $<$ $\rangle$) = ?

Задача. Aut ($\langle$ Z, + $\rangle$) = ?

Автоморфизмы и определимость

- **Задача**. Все определимые отношения сохраняются при автоморфизмах.
- Доказательство не-определимости. Указание автоморфизма, не сохраняющего...
- Неопределимость порядка через сложение: автоморфизм **Z** – смена знака
- Можно ли определить сложение через порядок ?
- Автоморфизм **Z** – сдвиг (+1): $\varphi(\boldsymbol{x}) = x+1$
- Как быть в случае натуральных чисел?

Подмногообразия и надгруппы

- Фиксируем множество D.
- Будем рассматривать различные многообразия отношений на D.
- Каждому многообразию соответствует группа автоморфизмов, сохраняющих элементы этого многообразия.
- Каждой группе автоморфизмов соответствует многообразие отношений, которые она сохраняет.
- Больше отношений – меньше группа. Соответствие Галуа
- Было: больше аксиом – меньше моделей.
- Берем под-многообразие, получаем над-группу.

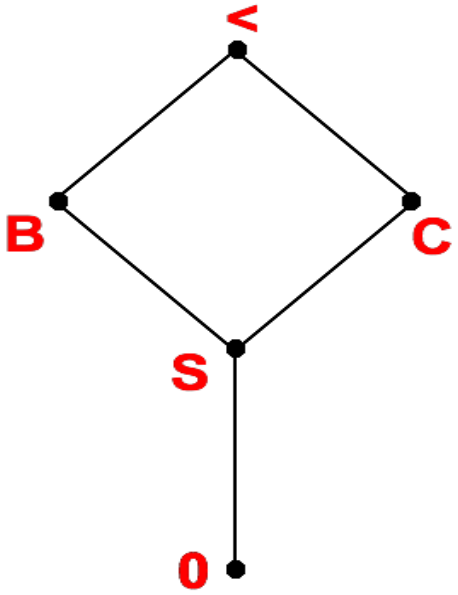
Подмногообразия в порядке на рациональных числах

- $xB(y,z) \Leftrightarrow (y < x < z) \vee (z < x < y)$ – между
- $C(x,y,z) \Leftrightarrow (x < y < z) \vee (z < x < y) \vee (y < z < x)$ – цикл
- $(x,y)S(zt) \Leftrightarrow (zB(x,y) \wedge \neg tB(x,y)) \vee (\neg zB(x,y) \wedge tB(x,y)) \Leftrightarrow$

$\Leftrightarrow (C(x,y,z) \wedge \neg C(x,y,t)) \vee (\neg C(x,y,z) \wedge C(x,y,t))$ – зацепление

Задача (Теорема Мучника – Семенова).
Есть ли еще подмногообразия?

Андрей Мучник
(24.02.1958 - 18.03.2007)



Различение многообразий

Пример. Как устроены подмногообразия в $\langle Q, < \rangle$?

Изучим надгруппы группы $\Gamma_{Q,<}$ – это все монотонно

возрастающие биекции.

Задача. Установить соответствие между подмногообразиями,

порождёнными =, S, C, B и следующими группами:

1. Группа, порождённая биекциями $\Gamma_{Q,<}$ и сменой знака.
2. Группа, порождённая $\Gamma_{Q,<}$ и отображением, которое перекладывает (меняет местами) два (бесконечных) интервала $(-\infty, \alpha)$ и $(\alpha, +\infty)$,

   то есть монотонно возрастающим образом отображает каждый из них на другой, причём α – иррациональное число, например, π.
3. Группа, порождённая элементами из 1 и 2.
4. Группа всех биекций Q.

Задача. Есть ли ещё надгруппы?

Задача. Доказать теорему.

Теорема Свенониуса

- «Теорема полноты» для определимости
- Теорема Геделя: все, что истинно во всех моделях, – выводимо.
- Теорема Свенониуса: все, что выдерживает автоморфизмы элементарных расширений, – определимо.

Определимость в порядке на натуральных числах

- Формула $\Phi(x)$ с одной свободной переменной.
- Модель $\langle \mathbf{N+Z}, < \rangle$ элементарно эквивалентна $\langle \mathbf{N}, < \rangle$.
- Сдвиг на 1 в компоненте $\mathbf{Z}$ – автоморфизм, значит на второй компоненте Φ постоянна. Значит, верна формула, что начиная с некоторого места Ф истинна, или верна формула, что начиная с некоторого места Ф ложна.
- Значит, на N формула $\Phi(x)$ также постоянна, начиная с некоторого натурального числа, то есть задает конечное множество или дополнение к нему.
- Мы воспользовались автоморфизмом элементарного расширения.
- **Задача**. Сформулировать и доказать аналогичное утверждение для формул с несколькими свободными переменными.

Модальные логики, задаваемые исчислениями

Исчисление *K* (Крипке)

Правила вывода:

- Тавтологии – выводимы.
- Все формулы $(\Box (A \to B)) \to (\Box A \to \Box B)$
  – выводимы.
- Если A – выводима, то
  – $\Box A$ – выводима (необходимость),
  – подстановка в A формул вместо имен – выводима (подстановка).
- Если A и $A \to B$ – выводимы, то
  B – выводима (modus ponens – MP).

Модальные логики, определяемые классами шкал

- Для каждого класса шкал можно рассмотреть класс формул, истинных во всех этих шкалах. Этот класс формул определяется заданным классом шкал.
- Бывает так, что достаточно рассмотрения одной определяющей шкалы.
- В частности, M^K – определяющая шкала для класса всех формул, выводимых в K .

Модальные логики, задаваемые исчислениями

Символ ◊ («возможно») вводится как сокращение для $\neg \Box \neg$, то есть $\Diamond A$ – *это* $\neg \Box \neg A$.

Примеры логик, классов шкал и определяющих шкал (*R* – отношение достижимости, A – пробегает множество всех формул).

- ***Логика универсальной модальности (”всегда”, ”всюду”)*:**
- S5 = $K \cup \{\Box A \to A;\ \Box A \to \Box\Box A;\ \Diamond \Box A \to A\}$
- Условие на шкалы: отношение достижимости рефлексивно, транзитивно и симметрично.
- Определяющая шкала: (N, R); $R = N \times N$.

- ***Логика «предсказуемого завтра»*:**
  $SL = K \cup \{ \Box A \equiv \Diamond A \}$.
- Условие на шкалы: $\forall s \, \exists! \, t \;\; R(s; t)$.
- Определяющая шкала: $(N; R)$;

  $R(s; t) \Leftrightarrow t = s + 1$.

- ***Логика «неопределенного завтра»***:
  $D = K \cup \{ \Box A \rightarrow \Diamond A \}$.
- Условие на шкалы: $\forall s \, \exists t \; R(s; t)$.
- Определяющая шкала: $(N^*; R)$, где N^* — слова в алфавите N; $R(s; t) \Leftrightarrow |t|=|s|+1$ и t — продолжение s.

Задача. Доказать сделанные о модальных логиках утверждения.

Неожиданный экзамен

- В субботу преподаватель объявил, что на следующей неделе будет экзамен, но накануне экзамена студенты не будут знать, когда он будет.
- Вывод: «Экзамена не будет».
- Экзамен состоялся в среду.

Исчисления

- Исчисление логики отношений
- Исчисления модальной логики
- Исчисление (индуктивное определение) формул

Строим общее понятие исчисления

Общее понятие исчисления. Предварительные определения

- Цепочка = конечная последовательность, в частности, последовательность может быть и пустой (пустая последовательность обозначается «Λ»). Длина цепочки – число элементов в ней.
- Алфавит = конечное множество символов.
- Слово (в данном алфавите) – конечная последовательность символов (частный случай цепочки).
- Ансамбль слов в данном алфавите – все слова. Часто алфавит = {0, 1}.
- Ансамбль цепочек слов в данном алфавите – все цепочки слов.

Действия и проверки. Описания

- Действие – исходное понятие. Действие:
  - описано на понятном человеку языке, может осуществляться и человеком, и каким-то устройством,
  - можно применить к любому исходному данному из фиксированного ансамбля слов или цепочек слов, при этом ясно, что всегда получается результат применения – элемент (возможно, другого) фиксированного ансамбля слов.
- Действие – задает всюду определенную функцию.
- Проверка – действие с результатом 0 или 1.
- Проверка задает множество (где она дает 1).

- Эмиль Борель (7.01.1871 — 3.02.1956) (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. Создаваемые слова

- Исчисление в данном алфавите – это пара из двух проверок:
- <проверка создания, проверка окончания>.
- Проверка создания применяется к цепочке слов, проверка окончания – к слову.
- Создаваемое исчислением слово определяется так:

  Если цепочка слов $a_0, \ldots, a_n$ принадлежит проверке создания

  и все элементы этой цепочки, кроме последнего, – создаваемы, то и последний элемент создаваем.
- Если проверке создания принадлежит цепочка из одного элемента, то его называют начальным объектом (в некоторых контекстах – аксиомой).
- **Задача**. Что, если таких у данного исчисления нет?

Исчисления. Породимые множества

- Слово порождаемо данным исчислением, если оно создаваемо и лежит в проверке окончания.
- Множество, порождаемое исчислением, состоит из всех порождаемых им слов.
- Породимое множество – множество, порождаемое каким-то исчислением.

Вывод

- Фиксируем исчисление.
- Если $a_0, \ldots, a_n$ – лежит в проверке создания, то говорим, что a_n создается из $a_0, \ldots, a_{n-1}$ (в данном исчислении).
- Вывод слова a – цепочка слов S, каждое из которых создается из какой-то цепочки слов, встретившихся в S раньше.
- **Задача**. Слово создаваемо 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) слов (и только их)?

Теоремы замкнутости для исчислений

Т. Объединение и пересечение породимых множеств породимы.

• **Д**. Пересечение.

• А: <Проверка создания А, Проверка окончания А>,

• Б: < Проверка создания Б, Проверка окончания Б>.

• **Идея**:

• Создаем слова, следуя Проверке А и следуя Проверке Б,

• Потом отбираем то, что создано и по той, и по другой проверке.

• Проблема: как разделить два множества?

• Выход: Метки для объектов, создаваемых по разным проверкам: Ах, Бу. Считаем, что символы А и Б в алфавит исчисления не входят.

Продолжение. Породимость пересечения

- Припишем ко всем элементам цепочки, входящей в две Проверки создания, в начале символы А или Б.
- Объединим полученные проверки.
- Добавляем в множество все тройки <Ах, Бх, х>.
- Проверка окончания?
- Пересечение проверок окончания А и Б.

Задача. Почему пересечение проверок – проверка?

Задача. Доказать теорему для объединения.

Породимость дополнения?

- В самом определении породимости говорится, как создавать новые объекты, и никак не видно, как можно установить не-породимость (и не-создаваемость).
- Математик, пытаясь установить, что что-то нельзя доказать, часто формулирует отрицание этого утверждения и пытается доказать это отрицание. (Тогда само утверждение – не породимо.)
- Иногда он берет даже более сильное негативное утверждение, например, указывая конкретный контрпример.
- Всегда ли можно доказать или утверждение, или его отрицание? (Уверенность Гильберта.)
- Породимые множества могут и никак не быть связаны с логикой, это могут быть совсем не множества формул.