Введение в математическую логику и теорию алгоритмов

Лекция 5

Алексей Львович Семенов

Адреса лекций

- https://dl.dropboxusercontent.com/u/69927703/vml2015/slides1.ppt
- https://dl.dropboxusercontent.com/u/69927703/vml2015/slides2.ppt
- https://dl.dropboxusercontent.com/u/69927703/vml2015/slides3.ppt
- https://dl.dropboxusercontent.com/u/69927703/vml2015/slides4.ppt
- https://dl.dropboxusercontent.com/u/69927703/vml2015/slides5.ppt

План

- Теорема Тарского об определимости в арифметике действительных чисел, повторение
- Теория моделей. Начальные понятия и теоремы
- Теория и модель. Примеры
- Элементарные подструктуры и расширения
- Теорема Тарского – Вота

Истинность. Повторение и обозначения

Фиксируем сигнатуру Σ.

Формула в сигнатуре Σ – это формула, в которой все имена отношений берутся из Σ.

Структура сигнатуры Σ – M = <D, Σ, Зн>. Можем рассматривать разные структуры (D и Зн могут меняться).

M = <D, Σ, Зн> – структура, $\Phi(x_1,\ldots,x_k)$ – формула в сигнатуре Σ, все ее свободные переменные входят в цепочку $x_1,\ldots,x_k$, $a_1,\ldots,a_k$ … – интерпретация ,

$M \models \Phi(a_1,\ldots,a_k)$ означает, что значение Φ в M при данной интерпретации – истина (вместо свободных переменных x_i подставлены элементы a_i).

Векторные обозначения: **a** - набор (цепочка) элементов $a_1,\ldots,a_k$,

Утверждение – это формула без свободных переменных (иначе говоря – замкнутая),

$M \models \Phi$ означает, что утверждение Φ *истинно в* M.

Теорема Тарского (– Зайденберга)

$\mathcal{R}$ = ⟨$\mathbb{R}$, p ( ) = 0, > 0 – для всех полиномов p с целыми коэфф., *Зн*⟩

Т. Существует алгоритм, который для всякой формулы сигнатуры структуры $\mathcal{R}$ строит эквивалентную ей в этой структуре бескванторную формулу.

Доказательство теоремы Тарского – Зайденберга (повторение)

4 операции на семействах многочленов.

1. Модифицированный остаток

Дано: пара p,q многочленов от u
(с коэффициентами из $\mathbb{Z}[x_1, \ldots, x_n]$),
степень $p(u)$ не меньше степени $q(u)$.

Пусть k = (степень $p(u)$ – степень $q(u)$) + 1,
a – старший коэффициент $q(u)$.

Получаем: *модифицированный остаток от деления $p(u)$ на $q(u)$* = остаток от деления $a^k p(u)$ на $q(u)$.

Вопрос. Что дает домножение на a^k ?

Р. Попробуйте делить «столбиком». Что происходит в процессе деления?

Степень (по u) модифицированного остатка меньше степени q.

Доказательство теоремы Тарского – Зайденберга (повторение)

Определяем еще 3 операции на семействах многочленов.

2. Отбрасывание старшего члена

3. Взятие старшего коэффициента

4. Дифференцирование по *u*

При этих операциях наибольшая положительная степень аргументов уменьшается.

Диаграмма (конечного) семейства многочленов:

•Для каждого многочлена из семейства рисуется прямая, на ней отмечаются его корни.

•Строится столбец многочленов, одна под другой располагаются соответствующие прямые.

•Для каждого многочлена отыскиваются его знаки во всех корнях других многочленов и в интервалах между корнями (возможно, разных многочленов).

•Строятся столбцы найденных знаков

Доказательство теоремы Тарского – Зайденберга.

- Пусть задана формула, F – замыкание (относительно 1-4) семейства всех многочленов из нее.
- F_0 – часть F, состоящая из многочленов степени 0 по u (они представляют собой многочлены из $\mathbb{Z}[x_1, \ldots, x_n]$).
- Диаграмма для множества F_0 состоит из одного столбца.
- **Лемма.** Пусть F – семейство многочленов из $(\mathbb{Z}[x_1, \ldots, x_n])[u]$, замкнутое относительно операций 1-4.
- Тогда диаграмма семейства F в данной точке $\boldsymbol{x}$ может быть построена по диаграмме семейства F_0 в той же точке.
- То, что диаграмма множества F_0 данная, записывается бескванторной формулой (конъюнкцией знаков многочленов от $X_1, \ldots, X_n$).

Доказательство теоремы Тарского – Зайденберга. Доказательство Леммы

- Добавляем к F_0 многочлены из F в порядке неубывания их степеней (то есть можем добавить многочлен, если все многочлены меньшей степени уже добавлены), пока не получим всё множество F.
- (действуем снизу вверх)
- Показываем, что на каждом шаге диаграмма расширенного множества (с новым многочленом) может быть однозначно восстановлена по диаграмме предыдущего множества.

Была:

- **Задача.** Завершить доказательство Леммы.

Доказательство теоремы Тарского – Зайденберга. Доказательство Леммы

Задача. Добавляем многочлен *p*. Что происходит с диаграммой?

•Надо «добавить» все корни *p*

•Куда?

–Какие появляются строки?

–Какие появляются столбцы?

Как искать Знак *p* в корнях уже рассмотренных многочленов?

Куда добавлять корни *p*?

Р. Использование операций 1 – 4, в частности, модифицированный остаток.

<u>примеры соображений:</u>

Если в соседних корнях уже рассмотренных многочленов *p(u)* имеет одинаковые знаки, то между этими корнями нет корней *p(u)* (иначе между корнями был бы корень производной, входящей в диаграмму), и знак в промежутке тот же.

Если в соседних корнях уже рассмотренных многочленов *p(u)* положителен и отрицателен, то между этими корнями есть один корень *p(u)*. Нужно добавить три столбца

Доказательство теоремы Тарского – Зайденберга

Для всякой формулы

$\exists u\, B(u, \boldsymbol{x})$, где B – бесквантворная, мы строим эквивалентную бесквантворную:

- Выписываем семейство всех многочленов из B.
- Строим замыкание F' семейства (относительно 4-х операций).
- Берем в замыкании часть нулевой степени F_0.
- Строим (восстанавливаем) диаграмму для F, из диаграммы для F_0 (из одного столбца),
- Отбираем из диаграмм для F те, которые обращают $\exists\, u\, B(u, \boldsymbol{x})$ в истину. Берем те диаграммы из F_0, из которых они получились.
- Для каждой взятой диаграммы из F_0 записываем бесквантворную формулу, (конъюнкция утверждений о каждой клетке).
- Искомая – дизъюнкция построенных формул.

. Доказательство теоремы Тарского – Зайденберга

Преобразование произвольной формулы в бескванторную идет индукцией по построению («изнутри»)

Если при построении мы навешивали квантор $\exists$, то теперь мы его навешиваем и сразу избавляемся.

Мы заменяем всякую формулу

$\forall u\, B(u, \boldsymbol{x})$ на эквивалентную

$\neg\exists u \neg B(u, \boldsymbol{x})$.

Со связками – очевидно.

Модель теории. Семантические свойства.

Теория – множество утверждений (формул без своб. перем.)

Структура M – *модель* теории Г, если M $\models \Phi$ для любой $\Phi \in$ Г.

Теория, у которой есть модель, называется *совместной (*или *семантически непротиворечивой)*.

Теория, у которой нет моделей, называется *несовместной (*или *семантически противоречивой)*.

Замкнутая формула Φ *семантически следует* из теории Г, если формула Φ истинна в любой модели теории Г.

- Обозначение: Г $\models \Phi$.

Теория Г *семантически полна*, если для любого утверждения Φ в той же сигнатуре Г $\models \Phi$ или Г $\models \neg\Phi$.

- Будем опускать слово «семантически».

Примеры теорий

В сигнатуре есть = и др.

$\exists u_1,\ldots,u_n \forall v\ (v=u_1 \vee \ldots \vee v=u_n)$

• Структуры, содержащие не более n элементов.

• **Задача**. Бывают ли теории, у которых нет бесконечных моделей, но для каждого натурального n есть модель, содержащая n элементов?

Линейный порядок

Система аксиом Г

$\forall u\ (\neg R(u, u))$ – антирефлексивность

$\forall u,v\ (R(u,v) \vee R(v,u) \vee u = v)$ – трихотомия

$\forall u,v,w\ ((R(u,v) \wedge R(v,w)) \rightarrow R(u,w))$ – транзитивность,

Модели – структуры, в которых отношение R задает линейный порядок

Будем писать < вместо R

Задача. Следствие из аксиом:

$\forall u,v\ \neg(u<v \wedge v<u)$ – антисимметричность.

Линейный порядок без наибольшего элемента

$\forall u\ (\neg(u < u))$

$\forall u,v\ (u < v \ \vee \ v < u \ \vee \ u = v)$

$\forall u,v,w\ ((u < v \ \wedge \ v < w) \rightarrow u < w))$

(Это была **Г**.)

$\forall u\ \exists v\ (u < v)$

• Примеры моделей – к известному числовому множеству добавлено равенство и порядок:

$Q_<$, $R_<$, $N_<$, $Z_<$.

Задача. Доказать, что все модели бесконечны.

Теория Γ_Q. Плотный линейный порядок без первого и последнего элемента.

$\forall u\ (\neg(u < u))$

$\forall u,v\ (u < v \ \vee \ v < u \ \vee \ u = v)$

$\forall u,v,w\ ((u < v \ \wedge \ v < w) \rightarrow u < w)$

$\forall u,v\ (u < v \rightarrow (\exists w\ (u < w < v)))$ – плотность

$\forall u\ \exists v\ (v < u)$ – неограниченность снизу

$\forall u\ \exists v\ (u < v)$ – неограниченность сверху

Задача. Какие бывают модели?

Задача. Можно ли что-то добавить, чтобы отделить $Q_<$ от $R_<$ (т.е., чтобы первая структура была моделью, а вторая – нет)?

Теория Γ_N: Дискретный линейный порядок с наименьшим элементом.

1. $\forall u\ (\neg(u < u))$
2. $\forall u,v\ (u < v \ \vee \ v < u \ \vee \ u = v)$
3. $\forall u,v,w\ ((u < v \ \wedge \ v < w) \rightarrow u < w)$
4. $\forall u\ \exists v\ (u < v)$
5. $\forall u\ (0 < u \ \vee \ u = 0)$
6. $\forall u\ (\exists v\ (u < v \ \wedge \ (\forall w\ (u < w \rightarrow (v{=}w \vee v{<}w)))))$
7. $\forall u(u \neq 0 \rightarrow (\exists v(v{<}u \wedge (\forall w(w{<}u \rightarrow w{=}v \vee w < v)))))$

Задачи:

- Что эта теория «означает» (смысл)?
- Какие у нее бывают модели (денотат)?

Изоморфизм

«Одинаковость» структур

Изоморфизм множеств – равномощность

Векторные обозначения: **a** – цепочка элементов $a_1, \ldots, a_k$, Λ – пустая цепочка. $D^* = \{\Lambda\} \cup D \cup D^2 \ldots$

Изоморфизм структур $M_1 = \langle <D_1, \Sigma, \mathbf{Зн}_1 \rangle$ и $M_2 = \langle D_2, \Sigma, \mathbf{Зн}_2 \rangle$ - это взаимно однозначное отображение ψ: D_1 на D_2 при котором:

Для любых $P \in \Sigma$, $\boldsymbol{a} \in D_1^*$,
$\mathbf{Зн}_1(P)(a) \Leftrightarrow \mathbf{Зн}_2(P)(\psi(a))$.

Задачи:

- Изоморфны ли структура положительных рациональных и всех рациональных чисел с порядком?
- Изоморфны ли две любые счетные модели Γ_Q?
- Р. Челночный процесс. (Как в теореме Кантора – Бернштейна)
- Бывают ли модели теории Γ_Q, равномощные R, но не изоморфные $\mathbb{R}_<$?

Теории и структуры

M – структура

• Th_M – теория структуры = множество утверждений, истинных в структуре *M*.

Теория класса структур = множество утверждений, истинных в каждой структуре класса

Пусть

• m – класс структур,

• φ – теория.

Определим отображения:

• Th (m) – теория класса структур m,

• Mod (φ) – класс всех моделей теории φ.

•Th, Mod – соответствие Галуа (анти-монотонное).

Тогда $m \subseteq Mod(\varphi) \Leftrightarrow Th(m) \supseteq \varphi$.

Эквивалентность

Структуры M_1 и M_2 (*элементарно) эквивалентны*, если их теории совпадают.

Задача. Почему изоморфные структуры эквивалентны?

• Индукцией по построению (не обязательно замкнутой) формулы Ф:

• $M_1 \models \Phi(a) \Leftrightarrow M_2 \models \Phi(\psi(a))$

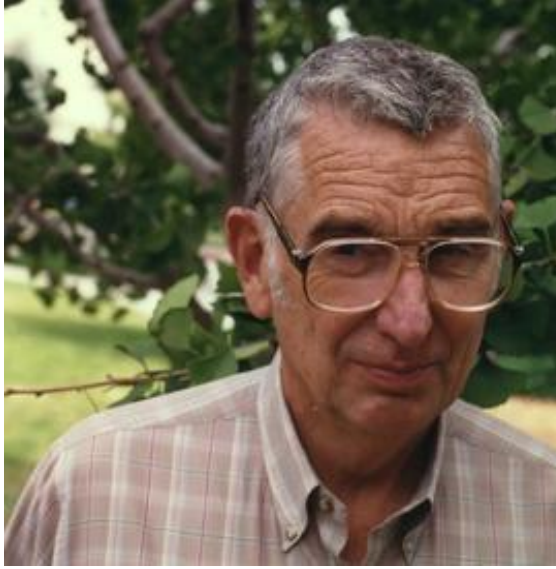
Задача. Бывают ли эквивалентные неизоморфные структуры?

Подструктура. Элементарная подструктура и элементарное расширение

- $M = \langle D, \Sigma, \mathbf{Зн} \rangle$, $D_1 \subseteq D$.
- *Подструктура* $M_1 = \langle D_1, \Sigma, \mathbf{Зн}_1 \rangle$, $\mathbf{Зн}_1$ для каждого символа получается ограничением **Зн** для этого символа на D_1
- M_1 – *элементарная подструктура* M :
  $M \models \Phi(\boldsymbol{a}) \Leftrightarrow M_1 \models \Phi(\boldsymbol{a})$
  для любых формул Ф и любых наборов $\boldsymbol{a} \in D_1{}^*$.
  M – *элементарное расширение* M_1.
  Очевидно M эквивалентна M_1.
- **Задача**. Бывают ли такие структуры M и M_1, что
  (1) M_1 – подструктура M, и
  (2) M_1 эквивалентна M, но
  (3) M_1 не является элементарной подструктурой M?

Конеци 5-й лекции

Критерий Тарского – Вота



Пусть $M_1 = \langle D_1, \Sigma, \mathbf{Зн}_1 \rangle$ – подструктура структуры $M = \langle D, \Sigma, \mathbf{Зн} \rangle$, $D_1 \subseteq D$.
Следующие два условия эквивалентны:

(1) M_1 – элементарная подструктура структуры M

(2) для любой формулы $\Phi(\boldsymbol{x}, y)$ и любого набора $\boldsymbol{a} \in D_1^*$ если
$M \models \Phi(\boldsymbol{a}, b)$ для некоторого $b \in D$, то
$M \models \Phi(\boldsymbol{a}, b')$ для некоторого $b' \in D_1$.

Задача. (1) $\longrightarrow$ (2)

Р. совсем просто

Роберт Вот (04.04.1926 – 02.02.2002)

Критерий Тарского – Вота

(2) $\rightarrow$ (1). Индукция по построению

$M_1 \models \Phi(\boldsymbol{a}) \Leftrightarrow M \models \Phi(\boldsymbol{a}), \boldsymbol{a} \in D_1^*$

Рассмотрим случай, когда $\Phi = \exists u\, \Psi(\boldsymbol{x},u)$

$\Rightarrow$. $M_1 \models \exists u\, \Psi(\boldsymbol{a},u) \Rightarrow$

$M_1 \models \Psi(\boldsymbol{a},b')$ для некоторого $b' \in D_1 \Rightarrow$

$M \models \Psi(\boldsymbol{a},b') \Rightarrow M \models \exists u\, \Psi(\boldsymbol{a},u)$

$\Leftarrow$. $M \models \exists u\, \Psi(\boldsymbol{a},u)$.

$M \models \Psi(\boldsymbol{a},b)$ для некоторого $b \in D \Rightarrow$

$M \models \Psi(\boldsymbol{a},b')$ для некоторого $b' \in D_1 \Rightarrow$

$M_1 \models \Psi(\boldsymbol{a},b') \Rightarrow M_1 \models \exists u\, \Psi(\boldsymbol{a},u)$

Задача. Провести полное доказательство критерия Тарского – Вота.

Теорема Лёвенгейма – Сколема об элементарной подмодели.

Т. Любая бесконечная структура с конечной или счетной сигнатурой содержит счетную элементарную подструктуру.

Д. Строим цепь $M_0 \subseteq M_1 \subseteq \ldots$ счётных подструктур M.

• M_0 произвольно. (Для $M_i = \langle D, \Sigma, \mathbf{Зн} \rangle$ пишем M_i вместо D.)

• На i -ом шаге берем все формулы $\Phi(x,y)$, все $\boldsymbol{a} \in M_i{}^*$.
Если $M \models \Phi(a,b)$, для какого-то $b \in M$, помещаем в M_{i+1} это b.

• $M' = \cup M_i$ – счетное множество.

Задача.

• Как определяется D' для M' ?

• Доказать что M' – элементарная подструктура.

• Еще один метод – «Объединение цепи».

Туральф Альберт Скулем (*Thoralf Albert Skolem*), 1887—1963

Леопольд Лёвенгейм
Leopold Löwenheim
26.06.1878 – 5.05.1957

Теорема компактности

А.И. Мальцев (14.11.1909—07.07.1967)

Т. (Гедель, Анатолий Иванович Мальцев)

Если любое конечное подмножество теории совместно, то теория совместна.

Как доказать теорему компактности?

Следствие. Если утверждение является следствием теории, то это утверждение является следствием некоторого конечного подмножества данной теории.

Задача. Вывести следствие из теоремы компактности.

Полные теории

Γ – $\Gamma \models \Phi$ или $\Gamma \models \neg\Phi$ для любого утверждения Φ.

Задача. Почему любую совместную теорию можно расширить до полной?

Задача. Th_M – полна.

Задача. Теория полна тогда и только тогда, когда две любые модели теории эквивалентны.

Задача.

•Являются ли теории Γ_Q, Γ_N полными?

• Существуют ли у них неизоморфные счетные модели?

Теорема Лёвенгейма – Сколема об элементарном расширении.

- **Теорема.** Для любой бесконечной структуры с конечной или счётной сигнатурой существует элементарное расширение сколь угодно большой мощности.
- **Доказательство.** Расширяем структуру.
- M = <D, Σ, Зн>, сигнатура Σ_M содержит имена для всех элементов из D, сопоставление Зн естественно продолжено до Зн'. $Th_M(M)$ – теория соответствующей структуры, M элементарно вложима в модели этой теории.
- Новые имена предметов {c} – произвольной мощности, $\Gamma = Th_M(M) \cup \{c \neq d\}$.
- Γ совместна (компактность).
- Мощность модели Γ не меньше мощности множества новых имен.

ω-категоричные теории

- О. Все счетные модели изоморфны

Задача. Доказать ω-категоричность плотного порядка без первого и последнего

  – Изоморфизм – челнок.

Признак Лося – Воота

- Совместная теория с конечной или счётной сигнатурой, не имеющая конечных моделей и категоричная в счётной мощности, полна.

Задача. Доказать признак Лося – Воота.

Задача. Определить категоричность в произвольной мощности.

- Совместная теория с конечной или счётной сигнатурой, не имеющая конечных моделей и категоричная в некоторой бесконечной мощности, полна.

Дискретный порядок с наименьшим

M – произвольная модель теории Γ_N, $a, b \in M$.
a, b *близки* – $\{c \in M \mid a \le c \le b$ или $b \le c \le a\}$ конечно.

• Классы эквивалентности – *галактики*, галактика $\tilde{a}$.

Задача. Как устроена галактика $\tilde{0}$? Как устроены все прочие галактики?

• Порядок на галактиках: $\tilde{a} < \tilde{b}$ – $\tilde{a} \neq \tilde{b}$ и $a < b$.

Задача. Корректно ли определен порядок? Будет ли порядок на галактиках линейным? Есть ли среди галактик наименьшая?

Дискретный порядок с наименьшим

$\mathrm{N} = \langle N, \{0,1,2,\ldots,<,+,\times\}, \mathbf{Зн}_0 \rangle$.

$R_+(n_1,n_2,n_3) \Leftrightarrow n_1+n_2 = n_3$

$R_\times(n_1,n_2,n_3) \Leftrightarrow n_1 \cdot n_2 = n_3$

$a + b + c = d \Rightarrow (\exists u\,(R_+(a,b,u) \wedge R_+(u,c,d)))$

Теория $\mathrm{Th}_{\mathbf{N}} \cup \{c \neq i \mid i \in \mathrm{N}\}$ совместна.
N^* – счетная модель данной теории.
$\mathrm{N}^*_<$ получена из N^* удалением всех отношений, кроме $<$ и константы 0.

Задачи.

• $\mathrm{N}^*_<$ – модель теории $\Gamma_{\mathbf{N}}$.
Может ли структура $\mathrm{N}^*_<$ оказаться изоморфной $\mathrm{N}_<$?