Введение в математическую логику и теорию алгоритмов

Лекция 6

Алексей Львович Семенов

- Структуры и теории
- Порядки
- Изоморфизм и совпадение теорий
- Построение модели
- Следствия

Дискретный порядок с наименьшим без наибольшего

- Сигнатура 0 – предметное имя, $<$ – имя двуместного отношения
- Теория Γ_N – множество формул:
- $\forall u \neg (u < u)$ – антирефлексивность,
- $\forall u,v,w ((u<v \wedge v<w) \Rightarrow u<w)$ - транзитивность,
- $\forall u,v (u<v \vee v<u \vee u=v)$ – линейность.
- $\forall u (u=0 \vee 0<u)$,

  (0 – наименьший эл.)
- $\forall u (\exists v (u<v \wedge (\forall w (u<w \Rightarrow v=w \vee v<w))))$,

  (v – след. за u)
- $\forall u (u \neq 0 \Rightarrow (\exists v(v<u \wedge (\forall w (w<u \Rightarrow w=v \vee w<v)))))$

  (v – предшествующий u)
- **Задача**. Натуральные числа – модель теории Γ_N
- **Задача**. А целые?

Дискретный порядок с наименьшим без наибольшего

- M – произвольная модель теории $\mathbf{\Gamma}_N$, $a, b \in M$.
- a, b *близки* – $\{c \in M \mid (a \le c \le b) \vee (b \le c \le a)\}$ конечно.
- Классы эквивалентности – *галактики*, галактика $a^{\sim}$.
- **Задача.** Как устроена галактика $0^{\sim}$? Как устроены все прочие галактики?
- Порядок на галактиках: $a^{\sim} < b^{\sim} \Leftrightarrow (a^{\sim} \neq b^{\sim}) \wedge (a < b)$.
- **Задача.** Корректно ли определен порядок? (Что этот вопрос означает?) Будет ли порядок на галактиках линейным? Есть ли среди галактик наименьшая?

Дискретный порядок с наименьшим без наибольшего

- $\mathbb{N} = \langle N, \{0, 1, 2, \ldots <, +, \times\}, \mathbf{Зн_0} \rangle$.
- $R_+(n_1, n_2, n_3) \Leftrightarrow n_1 + n_2 = n_3$
- $R_\times(n_1, n_2, n_3) \Leftrightarrow n_1 \times n_2 = n_3$
- Пример: $a + b + c = d \Leftrightarrow (\exists u\, (R_+(a, b, u) \wedge R_+(u, c, d)))$
- Теория $\mathrm{Th}(\mathbb{N}) \cup \{c \neq i,\ i \in N\}$ непротиворечива.
- **Задача**. Почему?
- $\mathbb{N}^*$ – счетная модель данной теории. Нестандартная арифметика
- $\mathbb{N}^*_<$ получена из $\mathbb{N}^*$ удалением всех отношений, кроме $<$ и константы 0.
- $\mathbb{N}^*_<$ – модель теории $\mathbf{\Gamma}_{\boldsymbol{N}}$.
- **Задача.** Может ли структура $\mathbb{N}^*_<$ оказаться изоморфной $\mathbb{N}_<$?

Дискретный порядок с наименьшим без наибольшего

- $\mathbb{Q}^+_<$, - неотрицательные рациональные числа
- **Задача.** Порядок на галактиках $\mathbb{N}^*_<$ совпадает с $\mathbb{Q}^+_<$,.
- *M – правильная* подструктура модели теории $\mathbf{\Gamma}_{\boldsymbol{N}}$:

  $a^{\sim} \subset M$ при $a \in M$.
- ***Утверждение.*** *Любая счетная модель теории* $\mathbf{\Gamma}_{\boldsymbol{N}}$
- *изоморфна правильной подструктуре структуры* $\mathbb{N}^*_<$.
- **Эскиз доказательства.** Множество галактик любой счетной модели теории $\mathbf{\Gamma}_{\boldsymbol{N}}$ – не более чем счетное линейно упорядоченное множеством с наименьшим элементом.
- Такое множество изоморфно подструктуре структуры $\mathbb{Q}^+_<$.

Дискретный порядок с наименьшим элементом

- ***Утверждение.*** *Любая правильная подструктура M структуры* $\mathbb{N}^*_<$ *является элементарной подструктурой.*
- Если $\boldsymbol{a} \in M$, $\mathbb{N}^*_< \vDash \mathbf{\Phi}\,(\boldsymbol{a}, b)$ для некоторого $b \in \mathbb{N}^*_<$, то
- $\mathbb{N}^*_< \vDash \mathbf{\Phi}(\boldsymbol{a}, b')$ для некоторого $b' \in M$. (Тарский – Воот)
- $\mathbb{N}_< \vDash \forall \boldsymbol{u}\, (\exists v\, \mathbf{\Phi}(\boldsymbol{u},v) \to \exists v'\, (\mathbf{\Phi}(\boldsymbol{u},v') \wedge \forall w\, (w < v' \to \neg\mathbf{\Phi}(\boldsymbol{u},w))))$

  (существование наименьшего – верно в нат. числах)
- $\mathbb{N}^*_< \vDash \mathbf{\Phi}\,(\boldsymbol{a}, b') \wedge \forall w\, (w < b' \to \neg\mathbf{\Phi}(\boldsymbol{a}, w))$, $b' \in \mathbb{N}^*_<$
- Пусть $b' \notin M$. Построим ψ: $\mathbb{N}^* \to \mathbb{N}^*$.
- $\psi(a) = a$, при $a \in M$, $\psi(a)$ – предыдущий к a, при $a \notin M$.
- ψ – автоморфизм $\mathbb{N}^*_<$.
- $\mathbb{N}^*_< \vDash \mathbf{\Phi}(\psi(\boldsymbol{a}), \psi(b'))$
- $\mathbb{N}^*_< \vDash \mathbf{\Phi}(\boldsymbol{a}, \psi(b'))$, $\psi(b') < b'$. Противоречие.

Дискретный порядок с наименьшим без наибольшего

- ***Утверждение.*** *Теория* $\mathbf{\Gamma}_N$ *полна.*
- **Д.** Пусть M_1 и M_2 – две неэквивалентные модели теории $\mathbf{\Gamma}_N$.
- Они бесконечны, по теореме Лёвенгейма – Сколема их можно выбрать счётными.
- Каждая из них изоморфна правильной подструктуре
- структуры $\mathbb{N}^*_<$.
- Все правильные подструктуры эквивалентны (они даже элементарные подструктуры).
- Противоречие.

Таким образом, мы указали полную теорию, у которой есть неизоморфные счетные модели (не категоричную в счетной мощности).

Теория (система аксиом).

Истинность в структуре.

- Фиксируем сигнатуру Σ
- Множество утверждений (замкнутых формул) мы называем *теорией* или *системой аксиом*.
- Структура M является *моделью* теории Г, если формулы из Г в ней истинны.
- Мы будем пытаться построить модель произвольной теории!

Построение модели

Фиксируем сигнатуру Σ, имена предметов и отношений

Будем рассматривать формулы без равенства

Связки: дизъюнкция, отрицание, существование

Упорядочение формул, множеств формул, пар…

Усложнение понятия модели:

Пары множеств утверждений $< A^+, A^- >$,

A^+ - положительное множество, положительные утверждения,
A^- - отрицательное множество, отрицательные утверждения

(нам нужно будет следить не только за истинными, но и за ложными формулами)

Структура M является *моделью* пары $< A^+, A^- >$, если
в M все формулы из A^+, истинны, а
все формулы из A^- ложны.

Если множества пары пересекаются, то моделей у пары нет.

Строим дерево,

- **вершины v - пары $< A^{+}_{v}\ ; A^{-}_{v} >$.**

(пары могут повторяться, но вершины все равно разные)

По ходу построения множество имен предметов в сигнатуре будет расширяться. Новые имена – из фиксированного счетного алфавита имен C.

Идея: «разбираем» утверждения из A^{+}_{v} ; A^{-}_{v} получаем «более простые». Для каждого более простого строим своего потомка в дереве.

- Одно из множеств потомка (положительное или отрицательное) совпадает с соответствующим множеством родителя, другое может увеличиться.
- Содержательно: истинность положительных и ложность отрицательных формул определяется значением формул из их потомков. Мы накапливаем информацию для модели по пути.

Продолжаем дерево в вершине $v = < A^{+}_{v} ; A^{-}_{v} >$

Строим следующие вершины

Положительное множество пересекается с отрицательным. (Содержательно: зашли в тупик.)

•Эта вершина становится листом дерева – 0 потомков, продолжить нельзя.

Пусть множества в паре не пересекаются

•Выбираем формулу $F \in A^{+}_{v} \cup A^{-}_{v}$:

•Если F – атомная, потомок один – та же пара.

Потомки. Формула *F*

Пусть множества в паре не пересекаются

•Выбираем утверждение $F \in A^{+}_{v} \cup A^{-}_{v}$:

•F – **атомная**, потомок один – та же пара.

•**Отрицание** утверждения – переносим само утверждение в «противоположное» множество.

•**Отрицательная дизъюнкция** – помещаем в отрицательное множество оба ее члена,

Во всех этих случаях потомок один.

Положительная дизъюнкция. Два потомка:

•Для каждого члена дизъюнкции – свой потомок

•Добавляем в положительное множество потомка этот член

В этом случае – потомка два.

Потомки. Формула *F*

В случае кванторов мы используем предметные имена – из исходной сигнатуры и новые.

$\exists u\, \Phi[x/u]$ из отрицательного множества.

•добавляем в отрицательной множество $\Phi[c/u]$ для всех имен *c*, которые входят в формулы данной вершины.

Потомок – один.

$\exists u\, \Phi[x/u]$ из положительного множества

•в него добавляем «пример» $\Phi[c/u]$, где *c* – константа, которой нет в формулах данной вершины.

Потомок – один.

Последовательность деревьев (растущее дерево)

Строим последовательность деревьев. В каждом цикле достраиваем все концевые вершины

Выбираем из непересекающихся пар очередную в некотором упорядочении.

Задача. Описать упорядочение (множества формул могут быть бесконечными)

Добавляем потомков

- Расширяющаяся последовательность деревьев

Когда она бесконечна?

Последовательность деревьев (растущее дерево)

Пара $< A^{+};A^{-} >$ конечно совместна, если любая пара $< B^{+};B^{-} >$, где B^{+}, B^{-} – конечные подмножества A^{+} и A^{-}, имеет модель.

Лемма. Если в некотором листе v дерева пара $< A^{+}_{v} ;A^{-}_{v} >$ конечно совместна, то у одного из потомков v в дереве соответствующая пара тоже конечно совместна.

Д. Прямая проверка. Задача.

Конечные подмножества потомков, откуда они?

Берем конечные подмножества в предке, включающие всё для потомков.

Берем модель для этих подмножеств в предке. Выбираем нужного потомка, с учетом того, из какого утверждения потомки получились. В случае квантора имя предмета интерпретируем как надо…

Сл. Если пара $< A^{+};A^{-} >$ конечно совместна, то последовательность деревьев бесконечна.

Основная лемма. Если последовательность деревьев, соответствующая паре множеств $< A^{+};A^{-} >$, бесконечна, то пара $< A^{+};A^{-} >$ имеет модель.

•**Д.**

•**Лемма Кёнига.** В бесконечном дереве с конечным ветвлением есть бесконечный путь.

•Рассмотрим дерево с конченым ветвлением = объединение всех деревьев последовательности. По лемме Кёнига в нем есть бесконечный путь $v_0 < v_1 < ....$

•Положим $A^{+}_{*} = \cup\{A^{+}_{v_i}\}$, $A^{-}_{*} = \cup\{A^{-}_{v_i}\}$.

Построение модели

- Определим структуру M так, что носителем M являются имена предметов из $A^{+}_{*} \cup A^{-}_{*}$, атомная формула истинна в M, если она принадлежит A^{+}_{*} . Индукцией по построению формулы докажем, что:
- **если формула принадлежит A^{+}_{*} , то она истинна в M, если формула принадлежит A^{-}_{*} , то ложна.**
- Очевидно для всех случаев, кроме $\exists u\ F(u) \in A^{-}_{*}$.
- Пусть $\exists u\ F(u) \in A^{-}_{*}$ и $c \in M$. Символ c встречается в некоторой вершине v_i . Мы должны предусмотреть рассмотрение формулы $\exists u\ F(u)$ в дальнейшем, тогда у нас появится в A^{-} и не исчезнет $F(c)$
- **Задача**. Как выбирать формулы, чтобы гарантировать ложность $F(u)$ для всякого элемента $c \in M$?

Основные теоремы логики отношений

Теорема компактности для счетного множества формул.

Если пара множеств $< A^+; A^- >$ конечно совместна, то она имеет модель.

Общезначимые формулы – истинные в любой структуре (данной сигнатуры)

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

Доказательство.

Формула F общезначима, если пара $< \varnothing; \{F\} >$ не имеет модели. Если модели нет, то последовательность конечна.

•Наш процесс построения цепочки гарантирует, что конечность цепочки будет выяснена на конечном шаге.

Исчисление для логики высказываний?

- Описание способа получения всех общезначимых формул и только их.
- Некоторый способ был описан – построение модели (для отрицания).
- Более явный – «классический» способ

Частные случаи тавтологий логики высказываний в логике отношений

- Возьмем тавтологию логики высказываний, например:

  $A_1 \to (A_2 \to A_1)$. (*)

- Подставим в (*) вместо логических переменных A_1 и A_2 любые (замкнутые или незамкнутые) формулы логики отношений:
- Например, вместо A_1 подставим $(\forall u_1(P_5(u_1)))$,

  а вместо A_2 подставим $(\exists u_1(P_4(u_1,u_1)))$:

  $(\forall u_1(P_5(u_1))) \to ((\exists u_1(P_4(u_1,u_1))) \to (\forall u_1(P_5(u_1))))$.
- То, что получилось, называется *частным случаем тавтологии* (*) логики высказываний в логике отношений.
- Любая такая формула общезначима (истинна в любой структуре и в любой интерпретации).
- Иногда вместо «частный случай тавтологии…» мы будем говорить просто «тавтология».

Исчисление логики отношений

- Фиксируем сигнатуру $\Sigma = <Ob, Pr>$.
- Исчисление (одно для данной сигнатуры) задаётся *аксиомами* (являющимися некоторыми формулами сигнатуры Σ) и *правилами вывода*.
- **Аксиомы**:

  A1. частные случаи тавтологий логики высказываний,

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

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

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

Исчисление логики отношений

Правила вывода:

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

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

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

Если уже выведены формулы, написанные в верхней части правила, то правило разрешает вывести формулу, написанную внизу.

В R2, R3 x не входит в Φ.

Правила R2 и R3 называются правилами Бернайса.

Примеры выводов

Пример 1. (1) $\vdash \forall u\, P(u) \to P(x)$ (аксиома A2)

(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 конкретная формула в нашей сигнатуре.

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

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

(2) $\vdash \forall u\, \Phi[x/u] \to \Phi$ (A2, Φ – это $\Phi[\,x/x\,]$)

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

(по MP из (2) и (1))

(4) $\vdash \Phi \to \exists u\, \Phi[x/u]$ (A3)

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

Примеры вывода

Пример 3.

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

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

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

$\to \Big(\big(x<y \to \exists v\,(x<v)\big) \to \big(\forall u\,(u<y) \to \exists v\,(x<v)\big)\Big)$ (частный случай тавтологии $(A \to B) \to \big((B \to C) \to (A \to C)\big)$)

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

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

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

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

Заметим, что полученная формула – общезначима.