Введение в математическую логику и теорию алгоритмов

Семинар № 5: Языки 1-го порядка: исчисление предикатов, компактность

Логическое следование

Мы обсуждаем язык первого порядка с некоторой сигнатурой $\Sigma = (\mathsf{Pred}, \mathsf{Func}, \mathsf{Const})$. Вспомним, что если дана интерпретация M этой сигнатуры и замкнутая формула A этой сигнатуры, то определено отношение «формула A *истинна* в интерпретации M», обозначавшееся так $M \models A$.

Пусть A — замкнутая формула, Γ — множество замкнутых формул этой сигнатуры.

Определение 1. Из множества формул Γ *следует* формула A (пишем:[1] $\Gamma \models A$), если для каждой интерпретации M имеем: если все формулы из Γ истинны в M, то формула A истинна в M: $\forall M \ \ (M \models \Gamma \Rightarrow M \models A)$.

Пример 1. Сначала неформально. Γ состоит из двух утверждений: «Все греки — мудрецы», «Сократ — грек». Утверждение A таково: «Сократ — мудрец». Читателю должно быть очевидно, что $\Gamma \models A$ (даже несмотря на то, что первая из гипотез не кажется нам верной).

Запишем это формулами. В этом примере сигнатура Σ состоит из одноместных предикатных символов G и W (греки и мудрецы), а также константы s (Сократ). Тогда формулы будут таковы:

$$\{\,\forall x\,(G(x) \to W(x)),\quad G(s)\,\} \quad \models \quad W(s).$$

Пример 2. Из аксиом групп следуют: единственность нейтрального элемента, единственность обратного.

Исчисление предикатов

Проверить, что $\Gamma \models A$ (даже в случае конечного Γ!) не представляется возможным, если использовать непосредственно определение (как перебрать всевозможные интерпретации M?). Альтернатива — сформулировать *исчисление*, позволяющее механически *выводить* из одних формул другие (и, конечно, доказать про это исчисление теорему, что оно выводит *все* следствия из заданных формул (и только следствия)).

В формулах используют два алфавита переменных: свободные $\{a_0, a_1, \dots\}$ и связанные $\{x_0, x_1, \dots\}$.

Исчисление предикатов

Аксиомы:

(A0) все аксиомы исчисления высказываний;
(A1) $\forall x\, A(x) \ \to\ A(t)$;
(A2) $A(t) \ \to\ \exists x\, A(x)$.

Правила вывода:

(MP) $\dfrac{A,\ A \to B}{B}$ правила Бернайса: (B1) $\dfrac{B \to A(a)}{B \to \forall x\, A(x)}$

(B2) $\dfrac{A(a) \to B}{\exists x\, A(x) \to B}$

(в правилах Бернайса переменная a не является свободной в формуле B)

[1] Здесь используется тот же символ $\models$, но в другом смысле! Прежний символ связывал модель M с формулой A; новый символ связывает множество формул Γ с формулой A. Для педантичного читателя — считайте, что это на самом деле другой символ, например, $\Vdash$. Использование одного и того же символа в данном случае — лишь дань традиции, от которой логики никак не могут (да и не хотят) отказаться.

Сравните следующее определение с аналогичным определением для исчисления высказываний (Семинар 2).

Определение 2. Из множества *замкнутых* формул Γ *выводима* формула A, если существует вывод из Γ формулы A. (Когда из Γ мы что-либо выводим, то формулы из Γ называем *гипотезами*.)

Вывод из Γ — это конечная последовательность формул $C_1, \ldots, C_n$, $n \geqslant 1$, в которой каждая формула C_k является либо аксиомой, либо гипотезой (из Γ), либо получена из некоторых предыдущих формул по одному из правил: (MP), (B1), (B2). Вывод считается *выводом формулы* A, если A — последняя формула в нём: $C_n = A$.

Если из Γ выводима A, то пишем: $\Gamma \vdash A$.

Если при этом $\Gamma = \varnothing$, то пишем $\vdash A$ (A *выводима*, или A является *теоремой* исчисления предикатов).

Теорема о корректности и полноте исчисления предикатов. *Для любого множества замкнутых формул Γ и любой формулы A справедливо следующее:*

$$\Gamma \vdash A \qquad \Longleftrightarrow \qquad \Gamma \models A.$$

В частности, формула выводима тогда и только тогда, когда она является общезначимой:

$$\vdash A \qquad \Longleftrightarrow \qquad \models A.$$

Задачи

1. Постройте вывод формулы $\forall x\, P(x) \to \forall y\, P(y)$.

   Вывод:
   1. $\forall x\, P(x) \to P(y)$ (аксиома (A1))
   2. $\forall x\, P(x) \to \forall y\, P(y)$ (по правилу Бернайса (B1))

2. Про Сократа: из гипотез $\forall x\,(G(x) \to W(x))$ и $G(s)$ выведите формулу $W(s)$.

   Вывод:
   1. $\forall x\,(G(x) \to W(x))$ (гипотеза)
   2. $\forall x\,(G(x) \to W(x)) \to (G(s) \to W(s))$ (аксиома (A1))
   3. $G(s) \to W(s)$ (по правилу (MP) из 1 и 2)
   4. $G(s)$ (гипотеза)
   5. $W(s)$ (по правилу (MP) из 4 и 3)

3. Без Сократа: из гипотез $\forall x\,(G(x) \to W(x))$ и $\exists y\, G(y)$ выведите формулу $\exists z\, W(z)$.

   Примечание: мы могли всюду использовать x, а не разные переменные x, y, z.

   Вывод:
   1. $\forall x\,(G(x) \to W(x))$ (гипотеза)
   2. $\forall x\,(G(x) \to W(x)) \to (G(y) \to W(y))$ (аксиома (A1))
   3. $G(y) \to W(y)$ (по правилу (MP) из 1 и 2)
   4. $W(y) \to \exists z\, W(z)$ (аксиома (A2))
   5. $G(y) \to \exists z\, W(z)$ (по силлогизму из 3 и 4, см. ниже)
   6. $\exists y\, G(y) \to \exists z\, W(z)$ (по правилу Бернайса (B2) из 5)
   7. $\exists y\, G(y)$ (гипотеза)
   8. $\exists z\, W(z)$ (по правилу (MP) из 7 и 6)

   Здесь под «силлогизмом» скрывается вывод: $A \to B, B \to C \vdash A \to C$. Этот вывод легко строится в исчислении высказываний (см. Семинар 2), приведём его:

Вывод:

1.	$A \to B$	(гипотеза)
2.	$B \to C$	(гипотеза)
3.	$(B \to C) \to [A \to (B \to C)]$	(аксиома исчисления высказываний)
4.	$A \to (B \to C)$	(по правилу (MP) из 2 и 3)
5.	$[A \to (B \to C)] \to [(A \to B) \to (A \to C)]$	(аксиома исчисления высказываний)
6.	$(A \to B) \to (A \to C)$	(по правилу (MP) из 4 и 5)
7.	$A \to C$	(по правилу (MP) из 1 и 6)

Теорема о дедукции для исчисления предикатов.
Пусть формулы в множестве Γ *и формула* A *— замкнуты, формула* B *— произвольная. Тогда*

$$\text{если } \Gamma, A \vdash B, \text{ то } \Gamma \vdash A \to B.$$

Компактность

Пусть $\Omega = (\mathsf{Pred}, \mathsf{Func}, \mathsf{Const})$ — некоторая сигнатура. Замкнутые формулы еще называют *предложениями*.

Теорией называется произвольное множество предложений (называемых ее *аксиомами*). Напоминание:

Интерпретация M называется *моделью* теории T, если T истинна в M; пишут это так: $M \models T$.

Теория T называется *выполнимой*, если существует интерпретация M, в которой истинна T.

$T \models A$ (из теории T *следует*[2] предложение A), если в каждой модели, в которой истинна T, истинно и A.

$T \vdash A$ (из теории T *выводимо* предложение A), если существует *вывод* формулы A из гипотез T.

Теорема о корректности и полноте исчисления предикатов. $T \models A \iff T \vdash A$.

Из теоремы о полноте вытекает следующий результат:[3]

Теорема о компактности (две формулировки):

1. *Если* T *— теория и* $T \models A$*, то существует конечная теория* $T' \subseteq T$*, такая что* $T' \models A$*.*

2. *Если каждое конечное подмножество теории* T *выполнимо, то вся теория* T *выполнима.*

Задачи

1. Выведите теорему компактности, пользуясь теоремой о полноте.

2. Выведите первую формулировку теоремы о компактности из второй, и наоборот.

Теории с равенством и нормальные модели

Пусть в сигнатуре Ω имеется двуместный предикатный символ «равенства» $=$. Пусть T — теория в сигнатуре Ω.

При изучении теорий с равенством обычно ограничиваются ***нормальными*** интерпретациями $M = (D, *)$, в которых символ $=$ интерпретируется

[2] Помним о двух *разных* смыслах употребления символа $\models$, см. предыдущий семинар!

[3] К. Гёдель в 1930 году доказал теорему компактности как следствие теоремы о полноте исчисления предикатов, и лишь для счетных сигнатур Ω. Академик А. И. Мальцев независимо в 1936 году доказал компактность другими методами, причем для сигнатур Ω произвольной мощности.

стандартно, как совпадение элементов носителя: $=^* = \{\langle e, e\rangle \mid e \in D\}$. Соответственно модифицируется понятие логического следования: $T \models A$ теперь определяется так: в каждой *нормальной* интерпретации, в которой истинна теория T, истинно и предложение A.

При этом остаются верными (но требуют отдельного доказательства) **теорема о корректности и полноте**, а также следующий из нее **принцип компактности**.

Задачи

3. В сигнатуре, состоящей лишь из равенства, напишите замкнутые формулы A_n, B_n, C_n, такие что для любой нормальной интерпретации $M = (D, *)$ имеем:

$$M \models A_n \Leftrightarrow |D| \geqslant n; \qquad M \models B_n \Leftrightarrow |D| \leqslant n; \qquad M \models C_n \Leftrightarrow |D| = n.$$

4. Пусть T — теория с равенством, $\mathbb{K}$ — класс всех ее ***нормальных*** моделей.

   В этом случае еще говорят, что теория T *аксиоматизирует* класс моделей $\mathbb{K}$.

   (a) Напишите систему аксиом, класс нормальных моделей которой — модели из $\mathbb{K}$ размера $\leqslant 3$; $\geqslant 5$; $= 7$.

   (b) Напишите систему аксиом, класс нормальных моделей которой — все бесконечные модели из $\mathbb{K}$.

5. Пусть T и $\mathbb{K}$ — как в предыдущей задаче. Пусть в $\mathbb{K}$ имеются сколь угодно большие *конечные* модели:

$$\forall n \geqslant 1\ \exists \text{ конечная модель } M = (D, *) \in \mathbb{K}, \text{ у которой мощность носителя } |D| \geqslant n.$$

   Обозначим: $\mathbb{K}_{<\infty}$ — класс всех конечных моделей из $\mathbb{K}$, $\mathbb{K}_\infty$ — класс всех бесконечных моделей из $\mathbb{K}$.

   (a) Приведите примеры таких теорий T.

   (b) Докажите, что тогда в $\mathbb{K}$ непременно есть и бесконечная модель, то есть $\mathbb{K}_\infty \neq \varnothing$.

   Указание: Каждое конечное подмножество теории $T \cup \{A_n \mid n \geqslant 1\}$ имеет модель (почему?). В силу компактности, вся теория имеет модель M; причем M непременно будет бесконечной.

   (c) Докажите, что класс $\mathbb{K}_{<\infty}$ невозможно *аксиоматизировать*.[4]

   Указание: Если бы теория Γ аксиоматизировала класс моделей $\mathbb{K}_{<\infty}$, то у этой теории по предыдущему пункту имелась бы бесконечная модель; но в $\mathbb{K}_{<\infty}$ их нет.

   (d) Докажите, что класс $\mathbb{K}_\infty$ невозможно *конечно аксиоматизировать*.[5]

   Указание: Допустим конечная теория $\Gamma = \{F_1, \ldots, F_s\}$ аксиоматизирует класс $\mathbb{K}_\infty$. Обозначим формулу $F := F_1 \wedge \ldots \wedge F_s$. Теория $T \cup \{A_n \mid n \geqslant 1\}$ тоже аксиоматизирует класс $\mathbb{K}_\infty$, см. задачу 4(b). Тогда $T \cup \{A_n \mid n \geqslant 1\} \models F$ (почему?). В силу компактности (задача 1), $\exists$ конечная теория $T' \subseteq T$ и $n \geqslant 1$, такие что $T' \cup \{A_1, \ldots, A_n\} \models F$. У теории $T' \cup \{A_1, \ldots, A_n\}$ есть *конечная* модель M (почему?). Тогда $M \models F$. Тем самым $M \in \mathbb{K}_\infty$, чего не может быть, ибо M — конечная модель.

[4] То есть не существует такой теории Γ, что $\mathbb{K}_{<\infty}$ — в точности класс всех нормальных моделей теории Γ.

[5] То есть не существует такой *конечной* теории Γ, что $\mathbb{K}_\infty$ — в точности класс всех нормальных моделей теории Γ.

Домашнее задание

6. Аксиоматизируйте следующие классы нормальных моделей:
   а) все линейно упорядоченные множества[6] размера 7;
   б) все бесконечные линейно упорядоченные множества.
   в) Можно ли аксиоматизировать все бесконечные линейно упорядоченные множества?

7. Докажите:
   а) нельзя аксиоматизировать класс всех конечных групп;
   б) нет конечной аксиоматики класса всех бесконечных групп.

8. Выпишите аксиомы теории полей в виде предложений сигнатуры $(+, \times, 0, 1, =)$.

   Характеристика поля F — это наименьшее число $n \geqslant 1$, такое что сумма n единиц равна 0. Если его не существует, то говорят, что F — поле характеристики 0.

   (a) Аксиоматизируйте класс всех полей фиксированной характеристики $n \geqslant 1$.

   (b) Докажите, что класс всех полей всевозможных характеристик $n \geqslant 1$ не аксиоматизируем.

   (c) Аксиоматизируйте класс всех полей характеристики 0.

   (d) Докажите, что класс всех полей характеристики 0 не конечно аксиоматизируем.

[6] Напомним, что *линейно упорядоченным множеством* называется множество с бинарным отношением на нем $(D, <)$, где отношение $<$ иррефлексивно, транзитивно и *линейно* (любые два различных элемента сравнимы). Можно дать аналогичное определение для нестрогого линейного порядка $\leqslant$ (какие аксиомы для этого понадобятся?); от одного определения легко перейти к другому.

Для самостоятельного разбора

Вероятно, этот материал будет упомянут и на лекции.

9. **Нестандартная модель арифметики.** Обозначим[7] **TA** — множество всех замкнутых арифметических формул (то есть формул сигнатуры $+, \times, =, <$), истинных в *стандартной интерпретации* $(\mathbb{N}, +, \times, =, <)$.

   (a) Докажите, что у теории **TA** имеется нормальная интерпретация, не изоморфная $\mathbb{N}$. Такие интерпретации называются *нестандартными моделями арифметики.* Обозначим одну из них через $M = (D, *)$.

   Указание: добавьте в сигнатуру константу c и рассмотрите аксиомы $0 < c$, $1 < c$, ...

   (b) **Принцип переноса.** Если арифметическое предложение (без c) истинно в $\mathbb{N}$, то оно истинно и в M.

   В частности, нестандартная модель M начинается с «конечных чисел» 0,1,2,..., между которыми нет других элементов.

   (c) В нестандартной модели M назовем *галактикой* всякое подмножество вида $\{e \in D\colon |e - a| \text{ конечно}\}$, для некоторого элемента $a \in D$. То есть галактику составляют всякий набор элементов данной модели, отстоящих друг от друга на конечное число «шагов». Например, множество «стандартных» чисел $\{0, 1, 2, \ldots\}$, упомянуте выше, составляет в M галактику (называемую *стандартной*). Остальные галактики называют *нестандартными.*

   Докажите, что в нестандартной модели галактик бесконечно много.

Домашняя задача:

10. Пусть M — (любая) нестандартная модель арифметики.

    Для двух галактик G и H полагаем $G \prec H$, если $\forall a \in G\ \forall b \in H\ a < b$. Докажите:

    (a) Любые две галактики сравнимы по данному отношению $\prec$.

    (b) Внутри каждой нестандартной галактики элементы упорядочены по типу $\mathbb{Z}$.

    (c) Докажите, что отношение $\prec$ на множестве всех бесконечных галактик — плотный линейный порядок без первого и последнего элемента.

    (d) Суммы $a + b$, когда a пробегает одну галактику, b — другую галактику, образует галактику.

    (e) Почему перемножать галактики аналогичным образом нельзя?

[7] Это множество называется *истинной арифметикой*, англ. *true arithmetic*, откуда и обозначение **TA**.