Листок 2

Логика первого порядка, исчисление предикатов (ИП)

Рассмотрим более сложную и содержательную чем ИВ формальную теорию.

Новое в алфавите: кванторы – о кванторах можно думать как об обобщениях конъюнкции и дизъюнкции на случай, когда переменные «пробегают» бесконечное множество значений: квантор всеобщности $\forall$ есть обобщение $\wedge$, квантор существования $\exists$ есть обобщение $\vee$.

В содержательных теориях (арифметика, теория групп, теория линейно упорядоченных множеств и т. д.) мы сталкиваемся с *функциями* и с *отношениями* на некотором *множестве переменных*. n-арная функция на множестве переменных S — это отображение $f : S^n \to S$; n-арное отношение на множестве переменных S — это подмножество S^n или, что то же самое, функция $F : S^n \to \{0,1\}$.

Для формализации теорий используется язык *логики первого порядка.* Алфавит формальной системы состоит из переменных, функциональных букв, для каждой из которых указано натуральное (в том числе нуль) число, называемое арностью, предикатных букв, тоже с арностью, логических связок (будем использовать набор $\to, \neg$), квантора $\forall$ ($\exists$, формально, не нужен, так как $\exists x A \equiv \overline{\forall x \overline{A}}$) и служебных символов (скобки и запятая). На интуитивном уровне можно думать о соответствии: функциональных букв и функций на множестве, предикатных букв и отношений на множестве, арности и количества аргументов.

Для определения формул в теории сперва выделяют отдельный класс строк в языке, называемых *термами.* Термы определяются рекурсивно как переменные и функции (функциональные буквы подходящей арности) от термов. Интуитивно можно думать о терме, как о некотором объекте теории: например, в теории групп элементы группы, константа 1 и произведение элементов группы являются термами. Затем определяются формулы: предикаты от термов (предикатные буквы подходящей арности), а также логические функции от формул и *навешивание квантора по переменной* на формулу есть формулы. Неформально: формулы являются утверждениями. К примеру, в теории групп формулами являются выражения вида «элемент группы a равен произведению b и c», «для любых элементов группы a и b верно, что $ab = ba$».

В формуле $\forall x A$ формула A есть область действия квантора по переменной x, вхождение x в область действия квантора по x называется *связанным*, любое другое вхождение x в формулу — *свободным.* Из-за наличия связанных и свободных вхождений переменных, замена одной переменной в формуле на другую (на терм) может приводить к коллизиям имён и к изменению логического смысла формулы. В связи с этим вводится определение: *терм t* называется *свободным для переменной x в формуле A*, если никакое свободное вхождение x в A не лежит в области действия квантора по переменной, входящей в терм t. В этом случае можно заменить x на t с сохранением смысла формулы.

Неформальный пример: утверждение $\exists x\, xy < 0 \vee y = 0$ истинно для любого y при рассмотрении вещественных чисел. Поскольку оно истинно для любого y, выражения вида $\exists x\, x \sin z < 0 \vee \sin z = 0$, $\exists x\, xy^2 < 0 \vee y^2 = 0$, $\exists x\, x \cdot (y + z + t) < 0 \vee y + z + t = 0$ верны для любых y, z, t. Однако, выражение $\exists x\, x \cdot x < 0 \vee x = 0$ ложно – подставить вместо x терм x (или терм x^3) нельзя, потому что квантор по x "мешает".

Аксиоматика теории может задаваться, как и в случае ИВ, множеством различных, эквивалентных друг другу способов. Под $A(t/x)$ будем понимать формулу, полученную заменой всех свободных вхождений переменной x в формуле A на терм t.

Будем рассматривать систему схем аксиом:

$\mathbf{Ax1}: A \to (B \to A)$

Ax2 $: (A \to (B \to C)) \to ((A \to B) \to (A \to C))$

Ax3 $: (\overline{B} \to \overline{A}) \to ((\overline{B} \to A) \to B)$

Ax4 $: \forall x A \to A(t/x)$, если терм t свободен для переменной x в формуле A

Ax5 $: \forall x(A \to B) \to (A \to \forall x B)$, если формула A не содержит свободных вхождений x

Кроме этих, в теории первого порядка могут быть иные аксиомы (они называются *собственными аксиомами* для теории), разные для каждой новой теории (у теории групп, выраженной в языке первого порядка, свои, у формальной арифметики — свои); если собственных аксиом нет, теория первого порядка называется исчислением предикатов первого порядка (ИП).

Правила вывода:

(modus ponens, **MP**) $\begin{array}{l} A \to B \\ A \\ \therefore B \end{array}$

(обобщение, **Gen**) $\begin{array}{l} A \\ \therefore \forall x A \end{array}$

Для ИП верна **теорема о дедукции** в ослабленном виде.

Если $\Gamma \vdash A \to B$, то $\Gamma, A \vdash B$.

Если $\Gamma, A \vdash B$ и в выводе B не применяется правило обобщения к свободным переменным формулы A, то $\Gamma \vdash A \to B$.

Для присвоения формулам ИП смысла их требуется проинтерпретировать. *Сигнатурой* теории первого порядка называется совокупность её функциональных и предикатных символов. Фактически, сигнатура фиксирует алфавит теории. Пусть для сигнатуры σ задано некоторое непустое множество M (это множество называется *носителем* теории). Помимо этого задано отображение, сопоставляющее каждому функциональному символу $f \in \sigma$ функцию f_M на M, при этом арность f должна совпадать с количеством аргументов f_M; аналогично, каждому предикатному символу $P \in \sigma$ сопоставляется отношение P_M на M соответствующей арности. Это отображение тогда называется *интерпретацией* σ на M.

Формула без свободных вхождений переменных называется *замкнутой*. В заданной интерпретации замкнутые формулы являются истинными или ложными. Замыканием формулы A называется формула $\forall x_1 \dots \forall x_n A$, полученная навешиванием квантора всеобщности по свободным переменным формулы A.

Для придания смысла истина/ложь незамкнутой формуле используется понятие *оценки*. Говорят, что задана оценка в интерпретации, если задано отображение каждой индивидуальной переменной в алфавите в носитель теории M. После задания оценки значение истина или ложь можно присвоить любой формуле.

Формула ИП называется *общезначимой*, если её замыкание истинно в любой интерпретации или, что эквивалентно, если она истинна в любой интерпретации при любой оценке. Формула называется *выполнимой*, если её замыкание истинно в некоторой интерпретации. Невыполнимость формулы эквивалентна общезначимости её отрицания. Общезначимые формулы — обобщение тавтологий, более конкретно: каждая тавтология ИВ есть общезначимая формула (однако, не каждая общезначимая формула представима в виде тавтологии ИВ).

Формулы A и B называются эквивалентными, если формула $A \equiv B$ общезначима.

Для ИП существуют и доказаны теоремы, аналогичные теоремам ИВ.

Теорема о корректности ИП: в ИП выводимы только общезначимые формулы.

Теорема о полноте ИП (Гёдель): всякая общезначимая формула выводима в ИП.

Формула называется предварённой нормальной формой, если она имеет вид $\complement x \dots \complement z A$, где каждый символ $\complement$ есть некий квантор (существования или всеобщности), а формула A не содержит кванторов. Для любой формулы существует эквивалентная ей предварённая нормальная форма.

При приведении формул к предварённой нормальной форме можно использовать замены подформул на равносильные:

1. $\overline{\forall v A(v)} \Leftrightarrow \exists v \overline{A(v)}$

2. $\overline{\exists v A(v)} \Leftrightarrow \forall v \overline{A(v)}$

В следующих формулах B не зависит от v:

3. $\forall v A(v) \vee B \Leftrightarrow \forall v (A(v) \vee B)$

4. $\exists v A(v) \wedge B \Leftrightarrow \exists v (A(v) \wedge B)$

В этих формулах $A(v)$ не зависит от u и $A(u)$ не зависит от v.

5. $\forall v A(v) \Leftrightarrow \forall u A(u)$

6. $\exists v A(v) \Leftrightarrow \exists u A(u)$

Рассмотрим процедуру *сколемизации* формулы: возьмём формулу в предварённой нормальной форме, рассмотрим в ней первый слева квантор существования (пусть по переменной z), перед ним n кванторов всеобщности. Удалим из формулы квантор существования, каждое вхождение переменной z заменим на новую (отсутствующую в изначальной сигнатуре) функциональную букву f арности n, аргументами при этом подставим переменные под кванторами всеобщности.

Пример: $\forall x \forall y \exists z \forall t A$ заменяется на $\forall x \forall y \forall t A(f(x,y)/z)$.

Описанная процедура называется сколемизацией. Теорема Сколема утверждает, что невыполнимость замкнутой формулы равносильна невыполнимости её сколемизации. Сколемизация позволяет избавиться от всех кванторов существования в формуле ценой расширения сигнатуры. Для формул, полученных после сколемизации, существует необходимый признак невыполнимости.

Если в предварённой нормальной форме $\psi = \complement x \dots \complement z A$ первый квантор есть квантор существования, а всего есть n блоков одноимённых кванторов (сперва сколько-то кванторов существования, затем сколько-то кванторов всеобщности, затем сколько-то кванторов существования и так n раз), формулу ψ относят к классу Σ_n.

Если верно то же самое, но первый блок состоит из кванторов всеобщности – это называется классом Π_n.

Проверка общезначимости для класса Π_0 и для класса Π_1 достаточно тривиальны – общезначимость формулы этих классов фактически равносильна тавтологичности некоторой формулы ИВ.

Для класса Σ_1 есть теорема. Теорема Эрбрана: формула $\psi = \exists x_1 \dots \exists x_n A$ общезначима тогда и только тогда, когда существует конечный набор подстановок термов вместо $x_1, \dots, x_n$ такой, что дизъюнкция

$$A(t_1^1/x_1, \dots, t_n^1/x_n) \vee \dots \vee A(t_s^1/x_1, \dots, t_n^s/x_n)$$

общезначима (здесь для примера s подстановок).

Теорема Сколема позволяет свести вопрос об общезначимости любой формулы к вопросу о выполнимости формулы класса Π_1 или, что то же самое, к вопросу об общезначимости формулы класса Σ_1. К сожалению, теорема Эрбрана отвечает на последний вопрос только неконструктивно. Никакого способа указать требуемый набор подстановок не вводится, а в общем случае определить существование такого набора невозможно.

2.1: Построить вывод формул в исчислении предикатов или пояснить, почему такой вывод невозможен

a) $\forall x \forall y A \to \forall y \forall x A$

b) $\forall x (A \to B) \to (\forall x A \to \forall x B)$

c) $(\forall x A \to \forall x B) \to \forall x (A \to B)$

d) $\forall x (A \to B) \to (\exists x A \to \exists x B)$

2.2: Пусть задана интерпретация: E – бинарный предикат, отвечающий предикату равенства. В качестве носителя возьмём множество натуральных чисел. Оценить формулу $\forall x E(x, y)$ при заданной оценке переменных $x = 1$, $y = 1$.

2.3: Приведите пример формулы, которая в одной интерпретации задаёт предикат $x < y$, а в другой $x > y$.

2.4: Существует ли такая формула A со свободными переменными x, y, что формула $\forall x \exists y A$ общезначима, а формула $\exists x \forall y A$ невыполнима?

2.5: Проверьте истинность следующих утверждений.

a) Если переменная x входит свободно в формулу A, то, заменив в формуле A все вхождения переменной x на y, мы получим эквивалентную формулу.

b) Если переменная y не входит в формулу A, то, заменив в формуле A все связанные вхождения переменной x на y, мы получим эквивалентную формулу.

c) Если переменная x не имеет свободных вхождений в формулу A, то, заменив в формуле A все вхождения переменной x на y, мы получим эквивалентную формулу.

d) Если переменная y не входит в формулу A, то, заменив в формуле A все свободные вхождения переменной x на y, мы получим эквивалентную формулу.

2.6: Существует ли замкнутая формула Φ, истинная в некоторой конечной интерпретации (носитель есть конечное множество), но ложная во всякой бесконечной интерпретации?

2.7: Существует ли замкнутая формула Φ, истинная в некоторой бесконечной интерпретации, но ложная во всякой конечной интерпретации?

2.8: Напишите предварённые нормальные формы, равносильные формулам:

$\overline{\forall x B(x) \to \forall x A(x)} \to \exists x A(x)$

$\exists x \forall y A(x, y) \lor \overline{\forall x \exists y B(x, y)}$

Проведите сколемизацию получившихся формул.

2.9: Пусть ψ имеет вид

$$\forall y \left(\forall y A(x, y) \to \forall x A(y, x)\right) \to \forall x \left(\forall y A(y, x) \to \forall x A(x, y)\right)$$

1) Может ли ψ выражать в некоторой интерпретации на целых числах бинарный предикат $xy = 0$?

2) Может ли ψ выражать в некоторой интерпретации на вещественных числах бинарный пре-

дикат $x < y$?

3) Может ли ψ выражать в некоторой интерпретации на вещественных числах бинарный предикат $x + y = 0$?

4) Может ли ψ выражать в некоторой интерпретации на натуральных числах (включая нуль) бинарный предикат $\forall y\, x|y \vee \forall x\, x|y$?

5) Какие бинарные предикаты может выражать ψ на целых числах?

2.10: Дана формула логики первого порядка в сигнатуре $\sigma = (P(\cdot,\cdot), Q(\cdot))$.

$$\forall x (P(x, y) \to Q(x)) \wedge Q(y)$$

Пусть носителем интерпретации является $\mathbb{N}$, $P(x, y)$ интерпретируется как “x делит y”, $Q(x)$ интерпретируется как ”x является полным квадратом”. На каких из следующих оценок формула в данной интерпретации истинна?

$x = 5, y = 1,$

$x = 1, y = 1,$

$x = 9, y = 32,$

$x = 4, y = 16.$