Введение в математическую логику и теорию алгоритмов: Семинар № 3

Языки первого порядка, выразимость, невыразимость

(см. книгу: Верещагин, Шень «Языки и исчисления», §3.1, 3.2, 3.3)

Синтаксис. В любом языке I порядка есть неизменная часть (символы, используемые в каждом языке):

- *индивидные переменные* — их счетное число; обозначим их множество $\mathsf{Var} = \{x_0, x_1, x_2, \ldots\}$;
- булевы связки: $\neg$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$ (если хочется, то и $\perp$, $\top$);
- кванторы: $\forall$, $\exists$;
- вспомогательные символы: скобки «(» и «)» и запятая «,».

А также «переменная» часть — набор символов, присущий именно этому языку; он называется *сигнатурой* $\Sigma = (\mathsf{Pred}, \mathsf{Func}, \mathsf{Const})$ и состоит из трёх конечных или счётных (и попарно непересекающихся) множеств символов:

- *предикатные* символы — множество этих символов $\mathsf{Pred} \neq \varnothing$;
- *функциональные* символы — их множество Func может быть пустым;
- *константы* — множество констант Const тоже может быть пустым.

Каждому предикатному и каждому функциональному символу приписано натуральное число $\geqslant 1$, называемое его *валентностью* или *арностью* (от англ. *arity*), и означающее «количество аргументов, которое нужно давать этому символу». Валентность символа $P \in \mathsf{Pred}$ и $f \in \mathsf{Func}$ будем обозначать $\mathsf{ar}(P)$ и $\mathsf{ar}(f)$, соответственно.

Из этих символов строятся (по индукции) выражения двух «типов»:

Термы (множество всех термов будем обозначать Tm):

- каждая переменная $x \in \mathsf{Var}$ является термом: $x \in \mathsf{Tm}$;
- каждая константа $c \in \mathsf{Const}$ является термом: $c \in \mathsf{Tm}$;
- если $f \in \mathsf{Func}$ и $\mathsf{ar}(f) = n$ и если $t_1, \ldots, t_n \in \mathsf{Tm}$, то выражение $f(t_1, \ldots, t_n)$ является термом.

Формулы (множество всех формул будем обозначать Fm):

- если $P \in \mathsf{Pred}$ и $\mathsf{ar}(P) = n$ и если $t_1, \ldots, t_n \in \mathsf{Tm}$, то выражение $P(t_1, \ldots, t_n)$ — формула («атомарная»);
- если A — формула, то $\neg A$ — тоже формула;
- если A, B — формулы, то $(A \wedge B)$, $(A \vee B)$, $(A \to B)$, $(A \leftrightarrow B)$ — тоже формулы;
- если A — формула, $x \in \mathsf{Var}$ — переменная, то $\forall x\, A$ и $\exists x\, A$ — тоже формулы. В них A считается *областью действия* квантора $\forall$ или $\exists$ по переменной x, а все вхождения переменной x в формулу A называются *связанными* вхождениями.

Вхождение переменной x в формулу A называется *свободным*, если оно не находится в области действия никакого квантора по переменной x. Свободно входящие в формулу A переменные ещё называют её *параметрами*. Формула A называется *замкнутой* (или *предложением*), если в ней нет параметров.

Семантика. Задать *интерпретацию* $M = (D, *)$ языка I порядка сигнатуры Σ — это значит фиксировать непустое множество D (*носитель* интерпретации) и сопоставить символам из сигнатуры Σ следующие объекты:

- каждой константе $c \in \mathsf{Const}$ сопоставить произвольный *элемент* c^* множества D, то есть $c^* \in D$;
- каждому функциональному символу $f \in \mathsf{Func}$ валентности $\mathsf{ar}(f) = n$ сопоставить произвольную n-местную *функцию* f^* (иначе говоря, n-местную *операцию*) на множестве D, то есть $f^* \colon D^n \to D$;
- каждому предикатному символу $P \in \mathsf{Pred}$ валентность $\mathsf{ar}(P) = n$ сопоставить произвольный n-местный *предикат* P^* (иначе говоря, n-местное *отношение*) на множестве D, то есть[1] $P^* \subseteq D^n$.

Чтобы интерпретировать формулы и термы, нужно еще задать *оценку*, сопоставляющую индивидным переменным произвольные элементы из D; тем самым оценка — это произвольная функция $v \colon \mathsf{Var} \to D$.

Интерпретация (с оценкой) распространяется на все термы и формулы по индукции. Не будем повторять здесь определение, его можно найти в лекциях или учебнике. При этом каждый терм t оказывается обозначающим некоторый *элемент* множества D, а каждая формула A становится либо «истинной», либо «ложной» в данной интерпретации M с оценкой v. Если в формуле A нет свободных переменных (то есть она замкнута), то формула A оказывается либо «истинной», либо «ложной» в данной интерпретации M (оценка ей уже не нужна).

Пишем: $M \models A$, где A — замкнутая формула; $M \models A(a_1, \ldots, a_n)$, где $a_1, \ldots, a_n \in D$, если A имеет свободные переменные $x_1, \ldots, x_n$ и мы рассматриваем оценку переменных v, такую что $v(x_1) = a_1, \ldots, v(x_n) = a_n$.

Выразимость

Пусть дана сигнатура Σ и интерпретация $M = (D, *)$ сигнатуры Σ.

Определение. Говорят, что n-местное отношение $R \subseteq D^n$ *выразимо* в M формулой сигнатуры Σ, если существует формула $A(x_1, \ldots, x_n)$ сигнатуры Σ, имеющая n свободных переменных $x_1, \ldots, x_n$ и такая, что

$$(a_1, \ldots, a_n) \in R \quad \iff \quad M \models A(a_1, \ldots, a_n) \quad \text{для всех } a_1, \ldots, a_n \in D.$$

То есть формула A истинна в точности на тех n-наборах элементов из D, которые находятся в отношении R.

Задачи

1. Сигнатура (**генеалогическая**) Σ: одноместные предикатные символы $\mathsf{Мужчина}$, $\mathsf{Женщина}$, двуместные предикатные символы $\mathsf{Супруг}$, $\mathsf{Родитель}$; функциональных символов и констант нет. Рассмотрим интерпретацию M, где носитель — все люди, а предикатные символы имеют естественный смысл.

   Выразить в M формулой сигнатуры Σ следующие отношения:

   а) «человек x является дедушкой человека y»:
   $\mathsf{Мужчина}(x) \wedge \exists z\, (\mathsf{Родитель}(x, z) \wedge \mathsf{Родитель}(z, y))$;

   б) «человек x является сестрой человека y»:
   $\mathsf{Женщина}(x) \wedge \neg(x = y) \wedge \exists z\, (\mathsf{Родитель}(z, x) \wedge \mathsf{Родитель}(z, y))$;

   в) «человек x является бабушкой»:
   $\mathsf{Женщина}(x) \wedge \exists y \exists z\, (\mathsf{Родитель}(x, y) \wedge \mathsf{Родитель}(y, z))$;

[1] **Примечание:** некоторые авторы под n-местным *предикатом* (или *отношением*) подразумевают отображение $D^n \to \{0, 1\}$, понимая «0» как «ложь» и «1» как «истина». Подумайте, почему это равносильно нашему определению, то есть от одного определения можно легко переходить к другому и наоборот, а значит, на каком варианте остановиться — дело вкуса.

г) «человек x является предком человека y»:
выразить нельзя (подумайте, почему? за рамками семинара);

д) «все дети человека x — женского пола»:
$\forall y\,(\mathsf{Родитель}(x,y) \to \mathsf{Женщина}(y))$.

2. Сигнатура (**арифметическая**) Σ: двуместный предикатный символ $=$; двуместные функциональные символы $+$ и $\times$; констант нет. «Стандартная» интерпретация: носитель — множество натуральных чисел $\mathbb{N} = \{0, 1, 2, \ldots\}$, символам $+$ и $\times$ сопоставлены операции сложения и умножения натуральных чисел. Выразимые (в этой интерпретации формулами этой сигнатуры) отношения называют *арифметическими*. Выразите следующие отношения:

   а) $x \leqslant y$; $x < y$; $x = 0$; $x = 1$; $x = n$ (для каждого фикс. числа $n \in \mathbb{N}$);

   б) x чётное; x делится на 3, на 4, на n (для фикс. числа $n \in \mathbb{N}$);

   в) x делится на y; x простое; $x = \text{НОД}(y, z)$; $x = \text{НОК}(y, z)$;

   г) Сформулируйте *проблему Гольдбаха*. То есть напишите замкнутую арифметическую формулу, утверждающую, что каждое четное число, большее двух, раскладывается в сумму двух простых.

   д) x есть некоторая степень двойки: $x \in \{1, 2, 4, 8, \ldots\}$, некоторая степень простого числа p и т.д.

Невыразимость

Пусть дана сигнатура $\Sigma = (\mathsf{Pred}, \mathsf{Func}, \mathsf{Const})$ и некоторая интерпретация $M = (D, *)$ этой сигнатуры.

Говорят, что функция $h\colon D \to D$ *сохраняет* отношение (например, двуместное) $R \subseteq D \times D$, если для любых двух элементов $a, b \in D$ имеет место эквивалентность: $(a, b) \in R \Leftrightarrow (h(a), h(b)) \in R$.

Говорят, что функция $h\colon D \to D$ *сохраняет* операцию (например, двуместную) $f\colon D \times D \to D$, если для любых трех элементов $a, b, c \in D$ имеет место: $f(a, b) = c \Rightarrow f(h(a), h(b)) = h(c) \in R$. Это же можно записать короче: если для любых двух элементов $a, b \in D$ имеет место равенство: $h(f(a, b)) = f(h(a), h(b))$.

Напомним, что каждой константе $c \in \mathsf{Const}$ в интерпретации M сопоставлен некоторый элемент $c^* \in D$. Говорят, что функция $h\colon D \to D$ *сохраняет* константу c, если она оставляет на месте элемент c^*, т.е. $h(c^*) = c^*$.

Определение. *Автоморфизм* (то есть изоморфизм на себя) интерпретации M — это биекция $h\colon D \to D$, сохраняющая все отношения, операции и константы из данной сигнатуры.

Примеры: изоморфизм группы $(G, \circ)$ на себя; изоморфизм упорядоченного множества $(D, <)$ на себя.

Теорема. *Автоморфизм сохраняет каждое выразимое отношение.*

$\Rightarrow$ Способ доказать *невыразимость* отношения: предъявить автоморфизм, ***не*** сохраняющий это отношение.

Задачи

3. В $(\mathbb{Z}, <)$ выразимы ли: $x = y$, $x + 1 = y$, $x + y = z$? (да, да, нет)

   Решение. Трёхместное отношение $x + y = z$ не выразимо, поскольку имеется автоморфизм $h\colon \mathbb{Z} \to \mathbb{Z}$, а именно $h(n) = n + 1$ (очевидно, сохраняющий отношение $<$ на целых числах, а потому действительно являющийся автоморфизмом), который ***не*** сохраняет данное отношение. Действительно, тройка $(3, 4, 7)$ принадлежит рассматриваемому отношению, ибо $3 + 4 = 7$; однако тройка $(h(3), h(4), h(7))$, то есть $(4, 5, 8)$, не принадлежит рассматриваемому отношению, ибо $4 + 5 \neq 8$.

4. В $(\mathbb{Z}, a+b=c)$ выразимы ли: $x=0$, $x=y$, $x<y$? (да, да, нет)

Решение. Поясним условие. В задаче имеется в виду, что в рассматриваемой сигнатуре есть *трёхместный* предикатный символ S, которому на множестве $\mathbb{Z}$ сопоставлено следующее трехместное отношение S^*: тройка целых чисел (a, b, c) лежит в S^* тогда и только тогда, когда $a+b=c$.

Отношение $x=0$ выражается формулой с одной свободной переменной x, а именно: $S(x, x, x)$.

Отношение $x=y$ выразите самостоятельно.

Отношение $x<y$ не выразимо, так как оно ***не*** сохраняется при следующем автоморфизме: $h(n)=-n$.

5. В $(\mathbb{N}^+, a \vdots b)$ выразимы ли: $x=y$, $x=1$, $x=3$? (да, да, нет)

Здесь $\mathbb{N}^+=\{1,2,3,\ldots\}$; отношение $a \vdots b$ означает $\exists c\,(a=b\cdot c)$.

Указание: рассмотрите автоморфизм, «меняющий местами» простые числа 2 и 3 в разложении чисел.

Домашнее задание

6. Выразите в генеалогической сигнатуре (см. задачу 1) следующие *двуместные* отношения: *братья, двоюродные братья, родная тётя, племянница, тёща, зять, шурин, деверь.*

7. Сигнатура: $=$, $\in$, $\perp$ (двуместные предикатные символы); функциональных символов и констант нет. Интерпретация: носитель — все точки и прямые на плоскости; в ней сопоставлено: символу $=$ — совпадение объектов, символу $\in$ — «точка лежит на прямой», символу $\perp$ — «две прямые перпендикулярны». Выразить:

а) «x — точка», «x — прямая»;
б) «прямые x и y параллельны»;
в) «x, y, z — вершины невырожденного треугольника»;
г) утверждение: «Высоты треугольника пересекаются в одной точке»;
д) «точки x, y, z, u — последовательные вершины параллелограмма»;
е) «точка z делит отрезок x, y пополам».

8. Рассмотрим арифметическую сигнатуру, в которой вместо двуместных *функциональных* символов $+, \times$ имеются трехместные *предикатные* символы Sum и Prod. Интерпретируем их на множестве натуральных чисел $\mathbb{N}$ стандартным образом: для всех чисел $m, n, k \in \mathbb{N}$
$\mathsf{Sum}(m, n, k)$ истинно $\Longleftrightarrow m+n=k$;
$\mathsf{Prod}(m, n, k)$ истинно $\Longleftrightarrow m\cdot n=k$.
Выразите отношения из задачи 2 формулами такой сигнатуры.

9. Перенумеруем пары натуральных чисел «змейкой»:
$(0,0),\quad (0,1), (1,0),\quad (0,2), (1,1), (2,0),\quad (0,3), (1,2), (2,1), (3,0), \ldots$
Выразите в арифметическом языке $(\mathbb{N}; +, \times; =)$ трехместное отношение «z есть номер пары (x, y)».

10. Выразимы ли следующие отношения? Если да, напишите формулу. Если нет, предъявите автоморфизм.

а) В структуре $(\mathbb{N}, a \vdots b)$ отношение «x — простое число».
б) В структуре $(\mathbb{N}, a+b=c)$ отношения $x<y$, $x=0$, $x=1$, $x=2$.
в) В структуре $(\mathbb{Z}, a+1=b)$ отношение $x=0$.
г) В структуре $(\mathbb{Z}, a+2=b)$ отношение $x+1=y$.
д) В структуре $(\mathbb{Z}, |a-b|=1)$ отношение $x+1=y$.
е) В структуре $(\mathbb{R}, |a-b|=1)$ отношения $x=y$, $|x-y|=2$, $|x-y|=3$.

11. Выразимо ли в арифметическом языке отношение $x=2^y$? $x=z^y$?