Введение в математическую логику и теорию алгоритмов

Семинар № 4: Языки первого порядка

(все недостающие детали — в книге: Верещагин, Шень «Языки и исчисления», §3.4, 4.1)

Выразимость в арифметике (продолжение)

Чтобы выразить $x = 2^z$ в структуре $(\mathbb{N}, +, \times, =)$, было бы желательно уметь говорить о конечных *последовательностях* натуральных чисел, ибо тогда мы могли бы написать так:

«существует последовательность $c_0, \ldots, c_z$, такая что $c_0 = 1$, $c_z = x$ и
каждый следующий член вдвое больше предыдущего: $\forall i < z\ c_{i+1} = 2 \cdot c_i$».

В этом нам поможет следующая функция.

Определение. *Бета-функция Гёделя* — это функция $\beta\colon \mathbb{N}\times\mathbb{N}\times\mathbb{N} \to \mathbb{N}$ со следующим свойством: для любого $n \geqslant 0$ и любой последовательности натуральных чисел $c_0, \ldots, c_n \in \mathbb{N}$ существуют числа[1] $a, b \in \mathbb{N}$, такие что

$$\beta(a, b, 0) = c_0,\ \ \ldots,\ \ \beta(a, b, n) = c_n.$$

Ответ: годится $\beta(a, b, i) :=$ «остаток от деления a на $b(i+1)+1$».
Почему? См.: Верещагин, Шень «Вычислимые функции» (2012), §10.3, Леммы 1 и 2.

Лемма. *График бета-функции Гёделя выразим в арифметическом языке.*

То есть существует арифметическая формула $B(x, y, z, u)$, выражающая отношение $\beta(x, y, z) = u$.
Это очевидно, ведь отношение «r есть остаток от деления p на q» легко выразить.

Задачи

1. Используя бета-функцию Гёделя, выразите в арифметическом языке отношения $x = 2^z$, $x = y^z$.

   Указание: если бы в языке мы могли писать ***терм*** $\beta(a, b, i)$, то отношение $x = 2^z$ мы бы выразили так:

   $$\exists a\, \exists b\, \big[\, \beta(a, b, 0) = 1 \ \wedge\ \beta(a, b, z) = x \ \wedge\ \forall i\, (i < z \to \beta(a, b, i+1) = 2 \cdot \beta(a, b, i))\, \big].$$

   Кроме того, в этой «формуле» используются константы 0, 1, 2, которых в языке нет (но они выразимы!). Перепишите данную «формулу», используя формулу $B(x, y, z, u)$, выражающую β-функцию Гёделя.

2. Используя бета-функцию Гёделя, запишите в арифметическом языке утверждения:

   а) ***малую теорему Ферма***: *если p — простое число и a — любое число, то $a^p - a$ делится на p.*

   б) ***великую теорему Ферма***: *не существует таких $n \geqslant 3$ и $x, y, z \geqslant 1$, что $x^n + y^n = z^n$.*

---

[1] То, что конечную последовательность приходится кодировать *двумя* числами a, b, не принципиально, а лишь следствие конкретной конструкции. Можно было бы и одним числом: $\gamma(d, i) = c_i$. Ведь пары чисел легко кодируются одним числом и наоборот (см. домашнюю задачу) и тогда «$\gamma(d, i) = c_i$» мы выражаем так: «d есть код некоторой пары чисел (a, b) и имеет место $\beta(a, b, i) = c_i$».

Выполнимые и общезначимые формулы первого порядка

По аналогии с логикой высказываний, вводятся следующие понятия (только вместо «оценки переменных» говорим про «интерпретации»). Напомним, что *замкнутая формула* — это формула, в которой нет свободных переменных (то есть в ней все переменные связаны кванторами).

- Замкнутая формула A называется *общезначимой*, если она истинна во всех интерпретациях: $\forall M\ M \models A$.
- Замкнутая формула A называется *выполнимой*, если она истинна в некоторой интерпретации: $\exists M\ M \models A$.
- Две замкнутые формулы A и B называются *равносильными* (или *эквивалентными*), если в каждой интерпретации M имеем: $M \models A$ тогда и только тогда, когда $M \models B$. Пишем: $A \equiv B$.

Для формул со свободными переменными можно дать те же определения, но вместо «интерпретации» нужно говорить «интерпретация M с оценкой переменных v». Например, две (незамкнутые) формулы $Q(x) \wedge R(x,y)$ и $R(x,y) \wedge Q(x)$ равносильны, обе они — выполнимы, но не общезначимы.

К эквивалентностям, имевшимся в логике высказываний, в логике предикатов добавляются следующие.

Основные эквивалентности

Двойственность кванторов:

$$\neg\exists x\, A(x) \equiv \forall x\, \neg A(x)$$
$$\neg\forall x\, A(x) \equiv \exists x\, \neg A(x)$$

Переименование связанной переменной (y — новая переменная):

$$\forall x\, A(x) \equiv \forall y\, A(y)$$
$$\exists x\, A(x) \equiv \exists y\, A(y)$$

Фиктивный квантор (переменная x не свободна в формуле A):

$$\forall x\, A \equiv A$$
$$\exists x\, A \equiv A$$

Вынесение кванторов (переменная x не свободна в формуле B):

$$\forall x\, A(x) \wedge B \equiv \forall x\, (A(x) \wedge B)$$
$$\forall x\, A(x) \vee B \equiv \forall x\, (A(x) \vee B)$$
$$\exists x\, A(x) \wedge B \equiv \exists x\, (A(x) \wedge B)$$
$$\exists x\, A(x) \vee B \equiv \exists x\, (A(x) \vee B)$$

Сокращение кванторов:

$$\forall x\, A(x) \wedge \forall x\, B(x) \equiv \forall x\, (A(x) \wedge B(x))$$
$$\exists x\, A(x) \vee \exists x\, B(x) \equiv \exists x\, (A(x) \vee B(x))$$

Задачи (письменное задание — не здесь, а далее в рамке!)

3. Являются ли следующие формулы выполнимыми? общезначимыми?

   а) $\exists x\, R(x,x)$;
   б) $\forall x\, P(x) \ \rightarrow\ \exists x\, P(x)$;
   в) $\forall x\, \exists y\, R(x,y) \ \rightarrow\ \exists y\, \forall x\, R(x,y)$;
   г) $\forall x\, \exists y\, R(x,y) \ \leftarrow\ \exists y\, \forall x\, R(x,y)$.

4. Уметь доказывать основные равносильности (рассматриваем произвольную интерпретацию $M = (D, *)$ и рассуждаем об ее элементах).

5. Почему эквивалентностей «вынесения кванторов» — 4, а «сокращения кванторов» — только 2? Докажите, что недостающие два «закона» сокращения кванторов не являются общезначимыми.

6. Используя основные эквивалентности, сформулируйте закон «вынесения кванторов за импликацию» (здесь переменная x не входит свободно в формулу B):

   а) $B \rightarrow \forall x\, A(x) \ \equiv\ \ldots$
   б) $B \rightarrow \exists x\, A(x) \ \equiv\ \ldots$
   в) $\forall x\, A(x) \rightarrow B \ \equiv\ \ldots$
   г) $\exists x\, A(x) \rightarrow B \ \equiv\ \ldots$

7. Докажите, что следующая формула выполнима, но лишь в бесконечных интерпретациях:

$$\neg\exists x\, R(x,x) \ \wedge\ \forall x\, \exists y\, R(x,y) \ \wedge\ \forall x\, \forall y\, \forall z\, (R(x,y) \wedge R(y,z) \rightarrow R(x,z)).$$

Письменное домашнее задание

Решения следующих задач нужно сдать на отдельном листочке на ближайшем семинаре 11 / 13 ноября 2019 г.

1. Дана формула: $\neg\big((\neg p \lor r) \to (p \land \neg q)\big)$.

   а) Приведите ее к СДНФ, используя ***основные эквивалентности***.

   б) Постройте для этой формулы таблицу истинности.

   в) Постройте СДНФ по данной таблице истинности.

   Убедитесь, что ответы в пунктах (а) и (в) совпали.

2. Выразимы ли в структуре $(\mathbb{Z}, a + b = c)$ отношения:
   а) «x — четное»; **б)** «x делится на 3»; **в)** «остаток от деления x на 3 равен 1».

   Если выразимо — предъявите формулу, в которой участвует *трёхместный* предикатный символ $S(a, b, c)$, означающий, что $a+b = c$; если не выразимо — предъявите автоморфизм, не сохраняющий данное отношение.

3. Используя бета-функцию Гёделя, выразите в $(\mathbb{N}, +, \times, =)$ отношения (выберите лишь ОДИН пункт):
   а) $y = x!$,
   б) y есть x-ый член последовательности Фибоначчи,
   в) y есть x-ое по порядку простое число.

4. Проверьте, является ли данная формула выполнимой? общезначимой?

$$\forall x\,(P(x) \lor Q(x)) \;\to\; \forall x\, P(x) \lor \exists x\, Q(x).$$

   Ответ обоснуйте:
   для выполнимости — приведите выполняющую интерпретацию;
   для общезначимости — проведите доказательство, что формула истинна в каждой интерпретации;
   для необщезначимости — приведите контрмодель.