Московский физико-технический институт
Факультет инноваций и высоких технологий
Математическая логика и теория алгоритмов, весна 2015
Выразимость в арифметике

Язык арифметики содержит один константный символ 0, один одноместный функциональный символ S и двухместные функциональные символы $+$ и $\cdot$. Единственным (двухместным) предикатным символом языка является равенство.

В стандартной интерпретации переменные принимают значения в множестве натуральных чисел $\mathbb{N}$, символ 0 интерпретируется как ноль, S как операция прибавления единицы, а $+$ и $\cdot$ как сложение и умножение соответственно.

Формула в языке арифметики с k свободными переменными задаёт некоторый предикат $P \subset \{0,1\}^k$. Если предикат можно выразить некоторой формулой в языке арифметики, то он называется *арифметичным.* Например, свойство (одноместный предикат) «x чётно» арифметично, т.к. его можно выразить формулой $\exists y(x = y + y)$. Функция $f\colon \mathbb{N}^k \to \mathbb{N}$ называется *арифметичной*, если арифметичен предикат $P_f\colon \mathbb{N}^{k+1} \to \{0,1\}$, где $P_f(\mathbf{x}, y) = 1 \Leftrightarrow f(\mathbf{x}) = y$.

1. Выразите в арифметике следующие предикаты и функции:

а) Свойство $x = c$ для любой константы c.
б) Отношение (двухместный предикат) $x > y$;
в) Отношение $x \,\vdots\, y$;
г) Функцию x/y (неполное частное от деления x на y);
д) Функцию $x \mod y$ (остаток от деления x на y);
е) Функции НОК(x, y), НОД(x, y);
ж) Свойство «x есть простое число»;
з) Трёхместный предикат «m/n есть рациональное приближение числа $\sqrt{2}$ с точностью $1/k$ »;
и) Свойство «x есть степень двойки»;
к) Свойство «x есть степень четверки».
л) Символ Лежандра (выразите 4 предиката: «$\left(\frac{a}{p}\right)$ не определён», «$\left(\frac{a}{p}\right) = 0$», «$\left(\frac{a}{p}\right) = 1$», «$\left(\frac{a}{p}\right) = -1$»).

2. *Выразимой нумерацией пар* натуральных чисел называется инъективная арифметичная функция $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

а) Докажите, что при любой выразимой нумерации пар функции $\mathrm{fst}(n)$ («первый элемент пары номер n») и $\mathrm{snd}(n)$ («второй элемент пары номер n»), не определённые, если n не является номером пары, также арифметичны.
б) Докажите, что при выразимой нумерации предикат «n является номером некоторой пары» арифметичен.

в) Придумайте взаимно однозначную выразимую нумерацию пар.

Для доказательства арифметичности многих предикатов используется мощный инструмент, называемый β-функцией Гёделя.

3. Докажите, что для любого n найдётся такое b, что числа $b+1, \ldots, nb+1$ попарно взаимно просты. Более того, b может быть сколь угодно большим.

4. Докажите, что для любого набора $(x_1 \ldots, x_n)$ найдутся числа a и b, такие что $a \equiv x_i \mod (bi+1)$ при всех i от 1 до n.

5. Докажите, что функция $\beta(a,b,i) = a \mod (bi+1)$ арифметична. (Т.е. четырёхместный предикат «$x = \beta(a,b,i)$» арифметичен.)

6. Выразите на языке формальной арифметики следующие предикаты:

а) Свойство «x есть степень шестёрки»;
б) Двухместный предикат $x = 2^y$;
в) Двухместный предикат «x есть n-ое по счёту простое число»;
г) Двухместный предикат $x = n!$;
д) Свойство «x есть совершенное число» (т.е. оно равно сумме всех своих делителей, крмое самого себя);
е) Двухместный предикат «m есть целая часть числа e^x».

Альтернативный способ доказательства арифметичности подобных предикатов — кодирование Смаллиана.

Введём следующее взаимно однозначное кодирование натуральных чисел последовательностями из нулей и единиц: имея число n, возьмём число $n+1$, запишем его в двоичной записи и вычеркнем первую единицу. Например: $5 \to 6 \to 110 \to 10$, $18 \to 19 \to 10011 \to 0011$. Обозначим код числа x через $\hat{x}$.

7. Упражнения:

а) Покажите, что кодирование действительно взаимно однозначное.
б) Найдите $\widehat{42}$, $\widehat{188}$, $\widehat{2015}$.
в) Кодами каких чисел являются строки 110, 101111, 010011000110010?

8. Покажите арифметичность следующих предикатов и функций. (В формулировках используются обозначения из теории формальных языков, но все они объясняются словами. Указание: нужно «переводить» утверждения с языка кодов на язык чисел).

а) $\hat{x} \in \{0\}^*$ ($\hat{x}$ состоит из одних нулей);
б) $|\hat{x}| = |\hat{y}|$ ($\hat{x}$ и $\hat{y}$ одной длины);
в) $|\hat{x}| \leqslant |\hat{y}|$ ($\hat{x}$ не длиннее $\hat{y}$);
г) $\hat{x}\hat{y}$ (*конкатенация* слов $\hat{x}$ и $\hat{y}$, т.е. слово, полученное приписыванием $\hat{y}$ справа к слову $\hat{x}$);
д) $\hat{x} \sqsubset \hat{y}$ ($\hat{x}$ есть начало $\hat{y}$);
е) $\hat{x} \sqsupset \hat{y}$ ($\hat{x}$ есть конец $\hat{y}$);

ж) $\hat{x}$ — подслово $\hat{y}$.

9. Докажите, что существует трёхместный предикат, обладающий следующими двумя свойствами: во-первых, для любых a и b множество $S_{ab} = \{x\colon S(x,a,b) = 1\}$ конечно. Во-вторых, для любого конечного множества M найдутся такие a и b, что $S_{ab} = M$. (Указание: в старых изданиях книги «Языки и исчисления» предлагался такой предикат: axa есть подслово b, тогда множество $M = \{x_1, \ldots, x_m\}$ совпадает с S_{ab} для $a = 10\ldots01$ и $b = ax_1ax_2a\ldots ax_ma$. Такой предикат не годится, однако его нетрудно исправить так, чтобы он подошёл.)

10. Докажите арифметичность следующих предикатов и функций при помощи кодирования Смаллиана:

а) Функции $f(k) = 2^k$ (Указание: используйте выразимую нумерацию пар. Выразите такое свойство: график функции $f(t) = 2^t$ проходит через точку (k, x));
б) Функции $f(k) = \varphi_k$ (k-ое по счёту число Фибоначчи);
в) Функции $f(k) = C_k$ (k-ое по счёту число Каталана);
г) Двухместного предиката «x и y есть дружественные числа» (дружественными называются различные числа, каждое из которых равняется сумме делителей другого, например $284 = 1+2+4+5+10+11+20+22+44+55+110$, $220 = 1+2+4+71+142$);
д) Символа Якоби (выразите 4 предиката: «$\left(\frac{a}{p}\right)$ не определён», «$\left(\frac{a}{p}\right) = 0$», «$\left(\frac{a}{p}\right) = 1$», «$\left(\frac{a}{p}\right) = -1$»).

11. Докажите арифметичность следующих строковых функций:

а) $\mathrm{Pref}(x, n)$ — начало $\hat{x}$ длины n;
б) $\mathrm{SubstrPosition}(x, n, k)$ — подслово $\hat{x}$ длины n, начиная с k-ой позиции;
в) $\mathrm{SuffContext}(x, y)$ — конец слова $\hat{x}$, начиная с первого вхождения слова $\hat{y}$;
г) $\mathrm{SubstrContext}(x, y, n)$ — подслово длины n слова $\hat{x}$, начиная с первого вхождения слова $\hat{y}$;
д) $\mathrm{Replace}(x, y, z)$ — результат замены первого вхождения слова $\hat{y}$ в слово $\hat{x}$ на слово $\hat{z}$;

12. Докажите арифметичность следующих функций и предикатов, связанных с вычислениями на машине Тьюринга:

а) $\mathrm{Step}(q, T)$ — следующая конфигурация при вычислении на машине $\hat{T}$ после конфигурации $\hat{q}$;
б) $\mathrm{Accept}(x, T)$ — машина $\hat{T}$ принимает вход $\hat{x}$;
в) $\mathrm{Rejept}(x, T)$ — машина $\hat{T}$ отвергает вход $\hat{x}$;

13. *(Ориентированным) графом* называется пара (V, E), где V — конечное множество вершин, $E \subset V \times V$ — множество рёбер (т.е. упорядоченных пар вершин). *Неориентированным графом* называется граф, в котором $\forall v\ (v, v) \notin E$ (т.е. нет петель) и $\forall v, w\ (v, w) \in E \Leftrightarrow (w, v) \in E$ (т.е. каждое ребро если проведено, то в обе стороны).

а) Придумайте, как занумеровать все графы натуральными числами. (Указание: если специфицировать число вершин n, то можно считать, что это числа $0, 1, \ldots, n-1$. Соответственно, рёбра суть пары таких чисел.)

Выразите в этой нумерации следующие предикаты:

б) «граф G неориентированный»;
в) «граф G связен» (любые две вершины можно соединить путём, ориентация рёбер неважна);
г) «граф G сильно связен» (любые две вершины в любом порядке можно соединить ориентированным путём);
д) «в графе G нет ориентированных циклов»;
е) «граф G является деревом»;
ж) «граф G можно раскрасить в три цвета» (т.е. покрасить каждую вершину в один из трёх цветов, так чтобы никакие две вершины одного цвета не были соединены ребром);
з) Двухместный предикат «граф G можно покрасить в k цветов»;
и) Двухместный предикат «диаметр графа G равен d» (диаметр — максимальное расстояние между вершинами, расстояние между вершинами — длина кратчайшего пути между ними).