Universität Siegen
Lehrstuhl Theoretische Informatik
Markus Lohrey

Exercise 5

Task 1
Let $(\mathbb{Z}, +, \cdot)$ be a structure, where

- $\mathbb{Z}$ denotes the universe of the structure,
- $+$ denotes a binary function symbol interpreted as the addition of integers, and
- $\cdot$ denotes a binary function symbol interpreted as the multiplication of integers.

Show that $\mathrm{Th}(\mathbb{Z}, +, \cdot)$ is undecidable.
Hint: Apply Lagrange's four-square theorem:

Theorem 1 (Lagrange's four-square theorem)
Every natural number can be represented as the sum of four integer squares, that is, for every $x \in \mathbb{N}$, there are integers $x_1, x_2, x_3, x_4 \in \mathbb{Z}$, such that $x = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

Solution:
Note that Lagrange's four-square theorem does not hold for negative integers. Let F be a formula such that $(\mathbb{N}, +, \cdot)$ is suitable for F. We transform F into a formula F', such that $(\mathbb{Z}, +, \cdot)$ is suitable for F', and such that $F \in \mathrm{Th}(\mathbb{N}, +, \cdot)$ if and only if $F' \in \mathrm{Th}(\mathbb{Z}, +, \cdot)$. We define

$$\mathrm{natural}(x) := \exists y_1 \exists y_2 \exists y_3 \exists y_4 (x = y_1 \cdot y_1 + y_2 \cdot y_2 + y_3 \cdot y_3 + y_4 \cdot y_4).$$

In order to obtain F', we replace every occurrence of a subformula $\exists x_i G$ by

$$\exists x_i \, (G \wedge \mathrm{natural}(x_i))$$

and every occurrence of a subformula $\forall x_i G$ by

$$\forall x_i \, (\mathrm{natural}(x_i) \rightarrow G) \, .$$

This yields a formula F', such that $(\mathbb{Z}, +, \cdot)$ is suitable for F' and such that $F \in \mathrm{Th}(\mathbb{N}, +, \cdot)$ if and only if $F' \in \mathrm{Th}(\mathbb{Z}, +, \cdot)$. By Gödel's Theorem, $\mathrm{Th}(\mathbb{N}, +, \cdot)$ is undecidable. Thus, $\mathrm{Th}(\mathbb{Z}, +, \cdot)$ is undecidable as well.

Task 2
Consider the structure $(\mathbb{N}, +, \cdot, s, 0)$. Use Gödel's β-function in order to formalize the following statements in predicate logic:

(a) $x^y = z$ (use free variables x, y and z),

(b) Fermat's Last Theorem,

(c) Collatz conjecture.

Solution:
We give the main ideas:

(a) We express $x^y = z$ as: There is a sequence $(a_1, \ldots, a_y, a_{y+1})$ with $a_1 = 1$, $a_{i+1} = a_i \cdot x$ for $1 \leq i \leq y$ and $a_{y+1} = z$. This holds if there are $t, p \in \mathbb{N}$ with $\beta(t, p, 1) = 1$, $\beta(t, p, i+1) = \beta(t, p, i) \cdot x$ for every $1 \leq i \leq y$ and $\beta(t, p, y+1) = z$.

(b) Fermat's Last Theorem states the following: For all natural numbers $a, b, c \geq 1$ and $n \geq 3$ we have $a^n + b^n \neq c^n$. We already know how to formalize $x^y = z$. From Exercise 2, Task 2, we know how to formalize the numbers 1 and 2 and the relations $\geq$ and $>$ in $(\mathbb{N}, +, \cdot, s, 0)$. We can thus formalize: If $a, b, c \geq 1$ and $n > 2$ and $a^n = a'$, $b^n = b'$ and $c^n = c'$, then $a' + b' \neq c'$.

(c) Let $f\colon \mathbb{N} \to \mathbb{N}$ be defined as $f(2n) = n$ and $f(2n+1) = 3(2n+1) + 1$. Let C_n be the sequence $(n, f(n), f(f(n)), \ldots)$. We write $C_n[i]$ for the ith element of the sequence. The Collatz conjecture is the following question: Is there for every n an integer j, such that $C_n[j] = 1$? The function f can be formalized by distinguishing between odd and even numbers and by defining the numbers 2 and 3 (Exercise 2, Task 2). Using the β-function, we can formalize the Collatz conjecture as follows: For every $n \in \mathbb{N}$ there are $t, p \in \mathbb{N}$, such that $\beta(t, p, 1) = n$, $\beta(t, p, i+1) = f(\beta(t, p, i))$ and there is $j \in \mathbb{N}$ such that $\beta(t, p, j) = 1$.