HOMEWORK 8

1. In the lecture we proved by induction on the complexity of formulae that if $\varphi(x_1, \ldots, x_\ell)$ is a Σ_1-formula, $a_1, \ldots, a_\ell \in \mathbb{N}$ and

$$\mathfrak{N} \models \varphi[a_1, \ldots, a_\ell]$$

then

$$A \vdash \varphi(\dot{\mathsf{S}}^{a_1}(\dot{0}), \ldots, \dot{\mathsf{S}}^{a_\ell}(\dot{0})).$$

The proof by induction on complexity of formulae is important because this proof can be formalized in Peano Arithmetic, which is crucial for the proof of the Second Gödel's Incompleteness Theorem. However, if we only want to prove the First Gödel's Incompleteness Theorem in set theory as a metatheory, we don't need to formalize the arguments in Peano Arithmetic. In this case the above result on Σ_1-formulae has a fast proof using Gödel's Completeness Theorem.

Assume $\mathfrak{M} \models A$.

(a) Show that $\mathfrak{N}$ is isomorphic to an initial segment of $\mathfrak{M}$.

(b) Show that if $\varphi(x_1, \ldots, x_\ell)$ is an arbitrary Σ_1-formula, $a_1, \ldots, a_\ell \in \mathbb{N}$ and $\mathfrak{N} \models \varphi[a_1, \ldots, a_\ell]$ then $\mathfrak{M} \models \varphi[a_1, \ldots, a_\ell]$.

(c) Use Gödel's Completeness Theorem to conclude that the above theorem holds.

Hint. Regarding (a), go over the formulae from the lecture which we showed to be provable in A. One of them implies (a). Regarding (b), this is an induction on complexity of formulae, but an easy and fast one.

2. Prove that every partial recursive function is Σ_1.

This is an induction on complexity of the building schema of partial recursive functions. Basic fuctions are easily seen to be Σ_0. The induction step uses several intermediate steps which are described below.

(a) Prove that if $R(y_1, \ldots, y_\ell)$ is a Σ_1-relation and $f_i(x_1, \ldots, x_k)$ are partial Σ_1-functions for $i \in \{1, \ldots, \ell\}$ then the relation $R'(x_1, \ldots, x_k)$ is also Σ_1. Recall that R' is defined as follows:

$$R'(x_1, \ldots, x_k)$$

if and only if $\langle x_1 \ldots x_k \rangle \in \mathrm{dom}(f_i)$ for all $i \in \{1, \ldots, \ell\}$, and letting $y_i = f_i(x_1 \ldots x_k)$, we have $R(y_1, \ldots, y_\ell)$.

(b) Prove that if $R(y_1, \dots, y_\ell)$ is a Π_1-relation and $f_i(x_1, \dots, x_k)$ are partial Σ_1-functions for $i \in \{1, \dots, \ell\}$ then the relation $R'(x_1, \dots, x_k)$ is also Π_1 where R' is as in (a).

(c) Use (a) to prove the following. If $g(y_1, \dots, y_\ell)$ is a partial Σ_1-function and $f_i(x_1, \dots, x_k)$ are partial Σ_1-functions for $i \in \{1, \dots, \ell\}$ then the composition $g(f_1(x_1, \dots, x_k), \dots, f_\ell(x_1, \dots, x_k))$ is also a partial Σ_1-function.

The above shows how to do the induction step in the case of composition. Now follows a list of steps that will give the induction step for the primitive recursion.

(d) Let $R(z, x_1, \dots, x_\ell)$ be a Σ_1-relation. Show that the relation R' defined by

$$R'(y, x_1, \dots, x_\ell) \iff (\forall z < y) R(z, x_1, \dots, x_\ell)$$

is also a Σ_1-relation.

For each $z < y$, the fact that $R(z, x_1, \dots, x_\ell)$ holds is witnessed by some u which witnesses an existential quantifier. You have to work with all $z < y$ as well as with corresponding witnesses u for each such z.

(e) Show that the function $\mathrm{op}(x, y)$ defined by

$$\mathrm{op}(x, y) = \frac{1}{2}(x + y)(x + y + 1) + x$$

is a primitive recursive bijection between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$. In this one particular case I do not require that you give a rigorous proof of bijectivity; instead, I am satisfied if you explain informally (possibly using a picture) how the function op acts.

The function op is a tool for coding ordered pairs of numbers by numbers. We will also need to compute the corresponding projections. We define functions

$$\begin{aligned} \mathrm{l}(z) &= \text{the unique } x \text{ such that } z = \mathrm{op}(x, y) \text{ for some } y. \\ \mathrm{r}(z) &= \text{the unique } y \text{ such that } z = \mathrm{op}(x, y) \text{ for some } x. \end{aligned}$$

Thus, $\mathrm{l}(z)$ is the left coordinate of the ordered pair coded by z, and $\mathrm{r}(z)$ is the right one. Use (d) to prove that the functions l and r are primitive recursive.

(f) Prove the Chinese Remainder Theorem: Assume $d_1, \ldots, d_\ell > 1$ are numbers that are relatively prime and $a_1, \ldots, a_\ell$ are such that $a_i < d_i$ for all $i \in \{1, \ldots, \ell\}$. (Two numbers d, d' are relatively prime just in case that their only common divisor is 1.) Show that there is a unique number $c < d = d_1 \cdot d_2 \cdot \cdots \cdot d_\ell$ such that $a_i = \mathrm{rm}(c, d_i)$ for all $i \in \{1, \ldots, \ell\}$; here $\mathrm{rm}(c, d_i)$ is the remainder of division of c by d_i.

There is a fast proof of this theorem which has a set-theoretic flavor: First show that the map

$$c \mapsto \langle \mathrm{rm}(c, d_1), \ldots, \mathrm{rm}(c, d_\ell) \rangle$$

is an injection from $\{0, \ldots, d-1\}$ into the Cartesian product

$$\prod_{i=1}^{\ell} \{0, \ldots, d_i - 1\}.$$

Then try to finish the proof on your own.

(g) Prove that for every ℓ and a there are numbers $d_1, \ldots, d_\ell > a$ that are relatively prime. Try $d_i = (i-1) \cdot s! + 1$ for $i \in \{1, \ldots, s\}$ where $s > \max\{l, a\}$.

As a consequence of the above, if $\langle a_1, \ldots, a_\ell \rangle$ is a sequence of natural numbers, we can find a number b such that $1 \cdot b + 1, 2 \cdot b + 1, \ldots, \ell \cdot b + 1$ are relatively prime, and by the Chinese Remainder Theorem, we can find a unique number c such that $a_i = \mathrm{rm}(c, i \cdot b + 1)$. This way the ordered pair $\langle b, c \rangle$ codes the sequence $\langle a_1, \ldots, a_\ell \rangle$. Then $\mathrm{op}(b, c)$ is a single natural number that codes this sequence. It is important that this coding is sufficiently simple.

(h) Show that the function rm is Σ_0.

(i) We define functions $\beta(x, y, z)$ and $\delta(x, y)$ as follows.

$$\begin{aligned} \beta(x, y, z) &= \mathrm{rm}(y, z \cdot x + 1) \\ \delta(u, v) &= \beta(\mathrm{r}(u), \mathrm{l}(u), v) \end{aligned}$$

Show that the functions β and δ are Σ_0. The function β is called Gödel's β-function.

By the remarks preceding (h) and (i), if we let $a = \mathrm{op}(b, c)$ we obtain $a_i = \delta(a, i)$ for all $i \in \{1, \ldots, \ell\}$. Now we can approach primitive recursion.

(j) Let $f(x_1, \ldots, x_\ell)$ and $h(u, v, x_1, \ell, x_\ell)$ be partial Σ_1-functions. The partial function $g(y, x_1, \ldots, x_\ell)$ is defined from f and h using primitive recursion, that is:

$$\begin{aligned} g(0, x_1, \ldots, x_\ell) &\simeq f(x_1, \ldots, x_\ell) \\ g(y+1, x_1, \ldots, x_\ell) &\simeq h(g(y, x_1, \ldots, x_\ell), y, x_1, \ldots, x_\ell). \end{aligned}$$

Show that g is a partial Σ_1-function.

Verify that g is defined as follows:

$$z \simeq g(y, x_1, \ldots, x_\ell)$$

if and only if there is a number a such that the following three clauses hold:

– $\delta(a, 0) = f(x_1, \ldots, x_\ell)$,
– $(\forall i < y)(\delta(a, i+1) = h(\delta(a, i), i, x_1, \ldots, x_\ell))$,
– $z = \delta(a, y)$.

Then show, using (a) – (i) that this statement can be expressed using a Σ_1-formula.

Finally we proceed to the μ-operator.

(k) Let $f(z, x_1, \ldots, x_\ell)$ be a partial Σ_1-function and $g(x_1, \ldots, x_\ell)$ be defined from f using the μ-operator, i.e.

$$y \simeq g(x_1, \ldots, x_\ell)$$

if and only if for all $z \leq y$ the value $f(z, x_1, \ldots, x_\ell)$ is defined,

$$f(y, x_1, \ldots, x_\ell) = 0$$

and

if $z < y$ then $f(z, x_1, \ldots, x_\ell)$ is distinct from 0.

Again, using (a) – (i) show that this definition can be expressed using a Σ_1-formula.

3. Show that Robinson Arithmetic A does not prove that $\dot{<}$ denotes a strict linear ordering. In particular, show that A does not prove that $\dot{<}$ denotes a binary relation that is (a) irreflexive and (b) transitive.

Hint. Regarding (a), consider the ordinal ω^ω with the standard successor operation, ordinal addition and multiplication. Extend the ordering $\in$ on ω^ω so that it will violate irreflexivity, but still satisfy the axioms of A. Regarding (b), consider the model of A that is a result of placing a finite "cycle" on top of the standard model $\mathfrak{N}$.