Université de Paris **(Date: 07/19/2020)**

UFR Mathématiques

SP1301 Model Theory: Problem Set #2

Professor: Samaria Montenegro Juan Ignacio Padilla, B55272

Second problem set for the model theory course. These correspond to Chapter 5 of the course notes: models of arithmetic and incompleteness theorems.

Problem 1. Presburger Arithmetic

Consider $\mathcal{L}_{\text{Pres}} = \{0, 1, +, <, 1\} \cup \{\equiv_n, n \geq 1\}$, where $\equiv_n$ are binary relations. *Presburger arithmetic* is given by the $\mathcal{L}_{\text{Pres}}$-theory T_{Pres} consisting of:

- Axioms for an ordered commutative group.
- 1 is the least positive element.
- For all $n \geq 1$ the following axiom

$$\varphi_n := \forall x, y \left(x \equiv_n y \leftrightarrow \exists z \; x + \underbrace{z + z + \cdots + z}_{n\text{-times}} = y \right).$$

- For all $n \geq 1$ the following axiom

$$\psi_n := \forall x \left(\bigwedge_{i=0}^{n-1} x \equiv_n \underbrace{1 + 1 + \cdots + 1}_{i-\text{times}} \right).$$

(1) Prove that $\langle \mathbb{Z}, 0, 1, +, <, \equiv_n \rangle \models T_{\text{Pres}}$.

(2) Prove that T_{Pres} has quantifier elimination, and that it is complete.

(3) Deduce that T_{Pres} is decidable.

Solution: Part 1) is evident; it is clear that $\mathbb{Z}$ is an ordered group whose first positive element is 1, and where the congruence relations modulo n (for $n \geq 1$) satisfy the axioms φ_n and ψ_n. To prove part 2), we will show that every model of T_{Pres} contains $\mathbb{Z}$ as a substructure. Let us add $-$

to the language, since it is definable from the group axioms. Let $\mathcal{M} \models T_{\text{Pres}}$. Define

$$Z^+ := \{\underbrace{1+1+\cdots+1}_{n-\text{times}}, n \geq 1\}$$

$$Z^- := \{-z, z \in Z^+\}$$

$$Z := Z^- \cup \{0\} \cup Z^+.$$

and restrict $+, <$ and $\equiv_n$ to Z. Let us show that $Z \subseteq \mathcal{M}$.

By construction, Z is closed under $+,-$ and contains 0. This makes Z a commutative group. We also have that $<$ is the restriction of a total order on $\mathcal{M}$, which makes $<$ a total order on Z. Furthermore, if $a, b \in Z$ and $c \in Z^+$, since Z^+ only contains positive elements of $\mathcal{M}$, we have

$$Z \models a < b \to a + c < b + c.$$

It remains to show that if $\mathcal{M} \models x \equiv_n y$ then $Z \models x \equiv_n y$ for $n \geq 1$. Suppose there exists $\alpha \in \mathcal{M}$ such that $x + \alpha n = y$, with $x, y \in Z$; in fact, we may assume without loss of generality that $\alpha > 0$ (otherwise swap b with a). Then we have $\alpha n = y - x \in Z$. This implies that the set $K = \{z \in Z^+, \alpha \leq z\}$ is non-empty. Let k_0 be the first element of K (since $\langle Z^+, \leq\rangle \cong \langle \mathbb{N}, \leq\rangle$). Assume by contradiction that $\alpha \notin Z$. Then

$$Z \models k_0 - 1 < \alpha < k_0$$

$$\Rightarrow Z \models 0 < \alpha + 1 - k_0 < 1$$

which contradicts the axioms of T_{Pres}. Therefore we can deduce that $\alpha \in Z$ and that $Z \models x \equiv_n y$. Finally, it is clear that the map $\underbrace{1+1+\cdots+1}_{m-\text{times}} \mapsto m$ can be defined so that $Z \cong \mathbb{Z}$ (respecting all relations and functions). We have shown that $\mathbb{Z} \subseteq \mathcal{M}$. We will now prove 2), that T_{Pres} admits quantifier elimination.

Let $\mathcal{M}, \mathcal{N} \models T_{\text{Pres}}$. We know that $\mathbb{Z}$ is a substructure of both models. Let $\varphi(x, \bar{y})$ be a quantifier-free formula. We will show that the existence of $\bar{z} \in \mathbb{Z}^p$ and $m \in \mathcal{M}$ satisfying $\mathcal{M} \models \varphi[m, \bar{z}]$, implies the existence of $n \in \mathcal{N}$ such that $\mathcal{N} \models \varphi[n, \bar{z}]$. Since φ has no quantifiers, the following logical equivalence holds

$$\varphi(x, \bar{y}) \sim \bigvee_i \bigwedge_j \chi_{ij}(x, \bar{y})$$

with χ_{ij} atomic formulas (or negations thereof). In fact, if $\mathcal{M} \models \varphi[m, \bar{z}]$ then for some i, $\mathcal{M} \models \bigwedge_j \chi_{ij}[m, \bar{z}]$. Thanks to this, we may assume that φ is a conjunction of atomic formulas or their negations.

In $\mathcal{L}_{\text{Pres}}$, atomic formulas are equivalent [1] to one of the following forms: $p(\bar{x}) = 0$,
$p(\bar{x}) < 0, p(\bar{x}) \equiv_n 0$, where $p(\bar{x})$ is a polynomial **of degree 1** with coefficients in $\mathbb{Z}$. Therefore, we assume without loss of generality that

$$\varphi(x, \bar{y}) = \bigwedge_i (p_i(x, \bar{y}) = 0) \wedge \bigwedge_i (q_i(x, \bar{y}) < 0) \wedge \bigwedge_i (r_i(x, \bar{y}) \equiv_n 0)$$

Where p_i, q_i, r_i are degree 1 polynomials with coefficients in $\mathbb{Z}$.
If $\mathcal{M} \models p_i(m, \bar{z}) = 0$, then there exist $k, a_1, \dots, a_n \in \mathbb{Z}$ such that

$$km + a_1 z_1 + a_2 z_2 + \cdots + a_p z_p = 0$$

$$\Rightarrow km = -(a_1 z_1 + a_2 z_2 + \cdots + a_p z_p) := A \in \mathbb{Z}$$

By an argument analogous to one used earlier, we can show that $km \in \mathbb{Z} \Rightarrow m \in \mathbb{Z}$, so m would be the witness in $\mathcal{N}$ that we are looking for. Suppose then that φ has the form

$$\varphi(x, \bar{y}) = \bigwedge_i (q_i(x, \bar{y}) < 0) \wedge \bigwedge_i (r_i(x, \bar{y}) \equiv_n 0).$$

Then m is the solution of a system (with unknown x) of the type

$$\begin{cases} k_i x < A_i & \text{for finitely many } i \\ l_j x + B_j \equiv_{n_j} 0 & \text{for finitely many } j \end{cases}$$

where $k_i, A_i, l_j, B_j \in \mathbb{Z}$ and $n_j \geq 2$ for all i, j. We want to solve this system in $\mathcal{N}$. Note that the inequality $k_i x < A_i$ is equivalent to $x < h_i$, where h_i is the smallest integer such that $hk_i < A_i < h(k_i + 1)$. Moreover, we can summarize all inequalities into a single one by taking $h = \min_i\{h_i\}$. We need to solve in $\mathcal{N}$ the equivalent system

$$\begin{cases} x < h \\ l_j x + B_j \equiv_{n_j} 0 & \text{for finitely many } j \end{cases} \tag{0.1}$$

[1]Expressions of the type $p(x) \not\equiv_n 0$ can be replaced by one of the form $\bigvee_{i=1}^{n-1} p(x) + \underbrace{1 + 1 + \cdots + 1}_{i-\text{times}} \equiv_n 0$

Let $n = \prod_j n_j$, and choose $0 \leq j \leq n-1$ satisfying $\mathcal{M} \models m \equiv_n j$. By known properties of $\equiv_n$, j is a solution to the system of congruences. Finally, choose a representative $g < A$ of the equivalence class of j modulo n; this is possible since $(-\infty, A]$ contains, thanks to the axioms of T_{Pres}, at least one element congruent to each of $1, 2, \ldots, n-1$. Then we have $g < A$ and since $g \equiv_n j$ it follows that g is also a solution of the congruences, and therefore a solution of system (0.1). Since $g \in \mathcal{N}$, $\mathcal{N} \models \varphi(g, \bar{z})$. We conclude therefore that

$$\mathcal{M} \models \exists x \varphi[x, \bar{z}] \Rightarrow \mathcal{N} \models \exists x \varphi[x, \bar{z}]$$

which is equivalent to T_{Pres} having quantifier elimination. Since every model of T_{Pres} has $\mathbb{Z}$ as a substructure, given $\mathcal{M}, \mathcal{N}$ any two models of T_{Pres}, by what we have just shown, we will have $\mathcal{M} \equiv \mathcal{N}$. Since these are arbitrary models, we conclude that T_{Pres} is complete. Finally, to see 3), note that T_{Pres} is clearly recursive, and being complete, a theorem from the section tells us it is a decidable theory.

Problem 2.

(1) Let $\Phi = \{\#\varphi, \varphi$ is a satisfiable $\mathcal{L}_{ar}$-sentence $\}$. Prove that Φ is not recursively enumerable.

(2) Let Φ_m be the set of codes of $\mathcal{L}_{ar}$-sentences satisfiable by some $\mathcal{L}_{ar}$-structure with domain $\{0, \dots, m-1\}$. Prove that Φ_m is primitive recursive.

(3) Let Φ_{fin} be the codes $\#\varphi$ of $\mathcal{L}_{ar}$-sentences satisfiable by some finite $\mathcal{L}_{ar}$-structure. Using the previous question and an appropriate encoding, prove that Φ_{fin} is recursively enumerable.

Solution: First we prove a). Suppose that Φ is recursively enumerable. By the representability theorem, there exists a Σ_1-formula τ that represents Φ. That is, $\mathsf{PA}_0 \models \tau(\#\varphi)$ if and only if there exists an $\mathcal{L}_{ar}$-structure $\mathcal{M}$ such that $\mathcal{M} \models \varphi$ (with φ a sentence). Let $\mathcal{M} \models \mathsf{PA}_0$.

- If $\mathcal{M} \models \varphi$, then by definition of τ, $\mathsf{PA}_0 \models \tau(\#\varphi) \Rightarrow \mathcal{M} \models \tau(\#\varphi)$.
- If $\mathcal{M} \models \neg\varphi$, then $\mathsf{PA}_0 \models \tau(\#\neg\varphi) \Rightarrow \mathcal{M} \models \tau(\#\neg\varphi)$.

We have just shown that there exists a formula with one free variable $\tau(x)$ that has the property

$$\mathcal{M} \models \varphi \iff \tau(\#\varphi),$$

this contradicts Tarski's theorem.

Before proving b) and c) we must work through some preliminaries. First we will give an effective enumeration of all finite $\mathcal{L}_{ar}$-structures. Let $m \geq 1$, and let $\mathcal{M}$ be an $\mathcal{L}_{ar}$-structure whose domain has m elements. We will encode the interpretations of the symbols of $\mathcal{L}_{ar}$: $+, \times, <, S$ (to be rigorous we should encode that $0^{\mathcal{M}} = 0$ but this does not alter the proof). For $n \geq 0$, define $\pi(n)$ as the $(n+1)$-th prime number and let $\alpha_n : \mathbb{N}^2 \to \mathbb{N}$ be a primitive recursive and invertible function. We encode as follows:

- $+ : M^2 \to M$ as follows: if $a, b, c \in M$ are such that $a + b = c$, then

$$\ulcorner + \urcorner = \prod_{a,b \in M} \pi(\alpha_2(a,b))^c.$$

- $\times : M^2 \to M$ as follows: if $a, b, c \in M$ are such that $a \times b = c$, then

$$\ulcorner \times \urcorner = \prod_{a,b \in M} \pi(\alpha_2(a,b))^c.$$

- $<\subseteq M^2$ as follows: if $a, b \in M$ are such that $a < b$, then

$$\lceil < \rceil = \prod_{a,b \in M} \pi(\alpha_2(a,b))^{\mathbb{1}_{a<b}}.$$

- $S : M \to M$ as follows: if $a, b \in M$ are such that $S(a) = b$, then

$$\lceil S \rceil = \prod_{a \in M} \pi(a)^b.$$

Finally we define

$$\lceil \mathcal{M} \rceil = \alpha_5(m, \lceil + \rceil, \lceil \times \rceil, \lceil < \rceil, \lceil S \rceil).$$

Let $\mathcal{M}$ be an $\mathcal{L}_{ar}$-structure with m elements; let us momentarily enrich the language to $\mathcal{L}_{ar}^*$, adding symbols for $1, 2, \ldots, m-1$. We will show by induction on φ that the set $\#\,\mathrm{Thm}(\mathcal{M}) = \{\#\varphi; \text{with } \varphi \text{ a sentence and } \mathcal{M} \models \varphi\}$ is primitive recursive.

- If φ is atomic, when interpreted in $\mathcal{M}$ it is equivalent to a formula of one of the following forms:
  - $a + b = c$.
  - $a \times b = c$.
  - $S(a) = b$.
  - $a < b$.

  For some $a, b, c \in M = \{0, 1, \ldots, m-1\}$.

  To check if $\mathcal{M} \models \varphi$, in the first case we must check if $\pi(\alpha_2(a,b))^c \mid \lceil + \rceil$. The other cases are similar. Moreover, all these operations are primitive recursive.
- The Boolean case is direct since primitive recursive functions are compatible with Boolean connectives.
- If $\varphi = \exists x \psi(x)$, with $\psi(x)$ a formula, we note that since

$$\mathcal{M} \models \exists x \varphi(x) \iff \mathcal{M} \models \bigvee_{k=0}^{m-1} \varphi(i),$$

  the result follows by induction hypothesis, since we can check in a primitive recursive way if $\mathcal{M} \models \varphi(k)$ for each $k = 0, 1 \ldots, m-1$.

Note: we can return to considering only sentences in the language $\mathcal{L}_{ar}$ by adding to the elements of $\mathrm{Thm}(\mathcal{M})$ the additional restriction of having no occurrence of $1, 2, \ldots, m-1$. The last thing we need for the proofs is to observe that since there are only finitely many $\mathcal{L}_{ar}$-structures with m elements, the set of their codes is primitive recursive; let us denote it $\mathcal{F}_m$.

Proof of b): We have

$$n \in \Phi_m \iff n = \#\varphi \text{ with } \varphi \text{ a sentence}, \exists z, z = \lceil \mathcal{M} \rceil \text{ with } \lceil \mathcal{M} \rceil \in \mathcal{F}_m / \text{ and also } n \in \#\,\mathrm{Thm}(\mathcal{M})\}.$$

As we have shown, all these sets are primitive recursive, so Φ_m is as well.

Proof of c): Let $\mathcal{F}$ be the set of codes of all finite $\mathcal{L}_{ar}$-structures. We have already given a recursive enumeration of this set. Then note that

$$\Phi_{fin} = \{(n,z), n = \#\varphi \text{ with } \varphi \text{ a sentence}, z = \lceil \mathcal{M} \rceil \text{ for } \lceil \mathcal{M} \rceil \in \mathcal{F}, n \in \#\,\mathrm{Thm}(\mathcal{M})\}.$$

Similar to b), we conclude that Φ_{fin} is recursively enumerable.

Problem 3. Let $\mathcal{L} = \{P, c\}$ where P is a unary predicate and c a constant symbol.

(1) Determine all countable $\mathcal{L}$-structures up to isomorphism.

(2) Deduce that two $\mathcal{L}$-structures $\mathcal{M}$ and $\mathcal{N}$ are elementarily equivalent when the following two conditions are satisfied

- $\mathcal{M} \models Pc$ if and only if $\mathcal{N} \models Pc$.
- $\mathcal{M} \models \exists^{\geq k} x Qx$ if and only if $\mathcal{N} \models \exists^{\geq k} x Qx$ for any $k \in \mathbb{N}$ and $Q \in \{P, \neg P\}$.

(3) Prove that an $\mathcal{L}$-sentence φ is universally valid if and only if $\mathcal{M} \models \varphi$ for any finite $\mathcal{L}$-structure. Deduce that the empty theory in $\mathcal{L}$ is decidable.

Solution:

In a countable $\mathcal{L}$-structure $\mathcal{M}$, the only things we can define are $c^{\mathcal{M}}$ and $P^{\mathcal{M}}$. In other words, the only way to distinguish elements of $\mathcal{M}$ is by checking whether it is c or whether P holds for that element. Whether $\mathcal{M} \models Pc$ is also key. We will show then that the isomorphism class of $\mathcal{M}$ depends only on the satisfiability of Pc and on the size of $P^{\mathcal{M}}$.

Lemma: Let $\mathcal{M} = \{m_0, m_1, \dots\}$ and $\mathcal{N} = \{n_0, n_1, \dots\}$, be countable $\mathcal{L}$-structures such that

- $\mathcal{M} \models Pc$ if and only if $\mathcal{N} \models Pc$.
- $\mathcal{M} \models \exists^{\geq k} x Qx$ if and only if $\mathcal{N} \models \exists^{\geq k} x Qx$ for any $k \in \mathbb{N}$ and $Q \in \{P, \neg P\}$.

Then $\mathcal{M} \cong \mathcal{N}$.

Proof: We will exhibit the isomorphism. Define $\sigma : M \to N$ as follows: first, $\sigma(c^{\mathcal{M}}) = c^{\mathcal{N}}$. Since $\mathcal{M}$ and $\mathcal{N}$ are countable, we can find $\alpha, \beta \leq \omega$ such that

$$P^{\mathcal{M}} = \{m_{i_k}\}_{k \in \alpha \leq \omega} \quad , \quad \mathcal{M} \setminus P^{\mathcal{M}} = \{\hat{m}_{i_k}\}_{k \in \beta \leq \omega}.$$

By the second hypothesis, we have $|P^{\mathcal{N}}| = \alpha$ and $|\mathcal{N} \setminus P^{\mathcal{N}}| = \beta$. Then we can also enumerate

$$P^{\mathcal{N}} = \{n_{i_k}\}_{k \in \alpha \leq \omega} \quad , \quad \mathcal{N} \setminus P^{\mathcal{N}} = \{\hat{n}_{i_k}\}_{k \in \beta \leq \omega}.$$

Then take $m_{i_k} \mapsto n_{i_k}$ and $\hat{m}_{i_j} \mapsto \hat{n}_{i_j}$ for all $k \in \alpha$ and all $j \in \beta$. By construction, σ is a morphism of $\mathcal{L}$-structures, since it preserves P and c. Moreover, we have constructed it to be bijective, which allows us to see that $\mathcal{M} \cong \mathcal{N}$. This completes the proof of 1).

To prove 2) note that every $\mathcal{L}$-sentence φ is a consequence of a formula of the type

$$Pc \wedge \exists^{\geq k_1} x Px \wedge \exists^{\geq k_2} y \neg Py \tag{*}$$

or of the type

$$\neg Pc \wedge \exists^{\geq k_1} x Px \wedge \exists^{\geq k_2} y \neg Py \tag{**}$$

for some $k_1, k_2 \in \mathbb{N}$. To see this, we can assume the opposite. If φ is not a consequence of any formula of this type, we can find countable $\mathcal{L}$-structures $\mathcal{M}_1$, $\mathcal{M}_2$ that satisfy the hypotheses of the previous lemma, but also satisfy $\mathcal{M}_1 \models \varphi$ and $\mathcal{M}_2 \models \neg\varphi$. By the same lemma however we would have $M_1 \equiv M_2$, which is absurd. We can assume then without loss of generality that if φ is a sentence, then it has one of the forms (*) or (**); thanks to the hypotheses we can then conclude that $\mathcal{M} \models \varphi$ if and only if $\mathcal{N} \models \varphi$.

The $\Rightarrow$ direction of 3) is evident. Let us prove the converse direction: suppose that for all finite $\mathcal{M}$, $\mathcal{M} \models \varphi$. Let $\mathcal{M}'$ be an infinite $\mathcal{L}$-structure. We must show that $\mathcal{M}' \models \varphi$. Suppose without loss of generality that $\mathcal{M}' \models Pc$ (the opposite case would be handled analogously). We consider two cases:

- If $P^{\mathcal{M}'}$ is finite, we can find some finite $\mathcal{M}$ such that $|P^{\mathcal{M}'}| = |P^{\mathcal{M}}|$ and also $\mathcal{M} \models Pc$. Then by 2) we would have $\mathcal{M}' \equiv \mathcal{M}$ and by hypothesis we conclude that $\mathcal{M}' \models \varphi$.
- If $P^{\mathcal{M}'}$ is infinite, consider the following theory

$$T = \{\varphi, Pc\} \cup \{\bigwedge_{i \neq j} x_i \neq x_j\}_{i,j<\omega} \cup \{Px_i\}_{i<\omega}.$$

We know that T is finitely consistent, since for all n we can define a finite L-structure $\mathcal{M}_n$ where $|P^{\mathcal{M}_n}| = n$, $M_n \models Pc$ and $M_n \models \varphi$ (thanks to its finiteness). By the compactness theorem, there exists $\mathcal{N} \models T$. This implies that $P^{\mathcal{N}}$ is infinite, and since $N \models Pc$, by 2) we have $\mathcal{M}' \equiv \mathcal{N}$, and therefore $\mathcal{M} \models \varphi$. Finally, to see that in $\mathcal{L}$ the empty theory is decidable, note that $\mathrm{Thm}(\varnothing) = \{\varphi, \vdash_{\mathcal{L}} \varphi\}$. We know from the theory of the chapter that the set of universal truths is recursively enumerable. Finally, $\mathrm{Thm}(\varnothing)^C$ consists of those sentences φ whose negation is in Φ_{fin}, and we can adapt the proof of part 2) of Problem 3 to see that Φ_{fin} is recursively enumerable. The conclusion follows from the complement theorem.

Problem 4. The objective of this exercise is to prove that there exists a total recursive function that is not provably total Σ_1.

(1) Prove that there exists a partial recursive function $h \in \mathcal{F}_2^*$ with the following properties:

a) If $a = \#\varphi$ for a Σ_1-formula $\varphi(v_0, v_1)$ and if $n \in \mathbb{N}$ is such that there exists $m \in \mathbb{N}$ with $\mathsf{PA} \vdash \varphi(\underline{\mathsf{n}}, \underline{\mathsf{m}})$, then $\mathsf{PA} \vdash \varphi(\underline{\mathsf{n}}, \underline{\mathsf{h(a,n)}})$.

b) If $a = \#\varphi$ for a Σ_1-formula $\varphi(v_0, v_1)$ and if $n \in \mathbb{N}$ is such that there is no $m \in \mathbb{N}$ with $\mathsf{PA} \vdash \varphi(\underline{\mathsf{n}}, \underline{\mathsf{m}})$, then $(a, n) \notin \mathrm{dom}(h)$.

c) In any other case, $h(a, n) = 0$.

(2) Choose h as above, and define $g \in \mathcal{F}^3$ as follows

- If $a = \#\varphi$ for a Σ_1-formula $\varphi(v_0, v_1)$ and if $b = \#\#d$ for a formal proof d of $\forall v_0 \exists! v_1 \varphi(v_0, v_1)$ in PA, then $g(a, b, n) = h(a, n)$.
- In any other case, $g(a, b, n) = 0$.

Prove that g is total recursive, and that it is *universally provably total* Σ_1 in the following sense: a function $f \in \mathcal{F}_1$ is provably total Σ_1 if and only if there exist $a, b \in \mathbb{N}$ such that $f = \lambda n.g(a, b, n)$.

(3) Conclude.

Solution: Throughout the proof, we will use the following fact: if ϕ is a Σ_1-sentence, then $\mathsf{PA_0} \vdash \phi$ if and only if $\mathsf{PA} \vdash \phi$. This follows from a theorem in the notes that states that every Σ_1-sentence valid in $\mathbb{N}_{st}$ is indeed a theorem of $\mathsf{PA_0}$. First we prove 1). Given $a = \#\varphi$ and $n \in \mathbb{N}$ satisfying the hypotheses of 1a), we only need to show that $h(a, n)$ is recursive in this case. We can describe $h(a, n)$ as the first number m such that $\mathsf{PA} \vdash \varphi(\underline{\mathsf{n}}, \underline{\mathsf{m}})$. We can in fact represent the function h as follows

$$\mathsf{PA} \vdash \forall \mathsf{y} \Big((\varphi(\underline{\mathsf{n}}, \mathsf{y}) \wedge (\forall (\mathsf{z} < \mathsf{y}) \neg \varphi(\underline{\mathsf{n}}, \mathsf{z})) \leftrightarrow \mathsf{y} = \underline{\mathsf{h(a,n)}} \Big)$$

Since the formula on the left side of the $\leftrightarrow$ is Σ_1, we deduce that h is partial recursive. To prove 2), it is clear that g is a total function. Consider now the set $C \subseteq \mathbb{N}^2$ of ordered pairs satisfying that $a = \#\varphi$, for a Σ_1-formula $\varphi(v_0, v_1)$ and $b = \#\#d$ for a formal proof d of $\forall v_0 \exists! v_1 \varphi(v_0, v_1)$ in PA. The results studied in the section show that C is recursive. This implies that we can define g recursively as

$$g(a, b, n) = \begin{cases} h(a, n) & \text{if } (a, b) \in C \\ 0 & \text{if } (a, b) \notin C \end{cases}$$

Next, it is clear that for any a, b, the functions $\lambda n.g(a,b,n)$ are Σ_1-provably total, since in the non-trivial case where $(a,b) \in C$, the formula that describes g is precisely the one whose code is a. Now, if f is Σ_1-provably total, choose $\chi_f(x,y)$ a Σ_1-formula that represents f and such that $\mathsf{PA} \vdash \forall \mathsf{x} \exists ! \mathsf{y} \chi_\mathsf{f}(\mathsf{x},\mathsf{y})$. Let $n \in \mathbb{N}$, let $m = f(n)$. Then take $a = \#\chi_f(\underline{n}, \underline{m})$ and b as the code of the formal proof of $\forall x \exists ! y \chi_f(x,y)$ in PA. Note then that by definition of $g(a,b,n)$, m is the first natural number satisfying $\mathsf{PA} \vdash \chi_\mathsf{f}(\underline{\mathsf{n}}, \underline{\mathsf{m}})$. Since χ_f is Σ_1, this is equivalent to $\mathsf{PA_0} \vdash \chi_\mathsf{f}(\underline{\mathsf{n}}, \underline{\mathsf{m}})$, and since χ_f represents f, this is in turn equivalent to $\mathsf{PA_0} \vdash \underline{\mathsf{f(n)}} = \underline{\mathsf{m}}$. We conclude then that for all n, $\mathsf{PA_0} \vdash \underline{\mathsf{g(a,b,n)}} = \underline{\mathsf{f(n)}}$, which implies that $g(a,b,n) = f(n)$ since $\mathbb{N} \models \mathsf{PA_0}$. This proves that f is Σ_1-provably total if and only if there exist a, b such that $f(n) = \lambda n.g(a,b,n)$.

Finally, to conclude the existence of a total recursive function that is not Σ_1-provably total, consider by a diagonalization argument the function $d(n) = \lambda n.g(\beta_1^2(n), \beta_2^2(n), n) + 1$, which is clearly total recursive[2]. If this function were Σ_1-provably total, there would exist a, b such that $d(n) = g(a,b,n)$. Take in particular $n_0 = \beta^{-1}(a,b)$ and observe that

$$d(n_0) = g(a,b,n_0) + 1 = g(a,b,n_0)$$

which is impossible.

[2]Here we take β_1^2 and β_2^2 as the components of some primitive recursive bijection between $\mathbb{N}$ and $\mathbb{N}^2$.

Problem 5. End extensions in Peano arithmetic.

The objective of this exercise is to prove the following result:

Let $\mathcal{M}$ be a countable model of PA. Then there exists a proper elementary extension $\mathcal{M} \preccurlyeq \mathcal{N}$ where $\mathcal{N}$ is an end extension of $\mathcal{M}$, that is, for all $m \in M$ and all $n \in N \setminus M$, we have $\mathcal{N} \models m < n$.

(1) Let $\mathcal{M} \models \mathsf{PA}$. Prove that the *pigeonhole principle* holds in $\mathcal{M}$: for every $\mathcal{L}_{ar}(M)$-formula $\theta(v,z)$ and every $a \in M$, we have

$$\mathcal{M} \models p(a) := [\forall x(\exists z > x)(\exists v < a)\theta(v,z)] \to (\exists v < a)\forall x(\exists z > x)\theta(v,z)$$

(2) Let $\mathcal{M} \models \mathsf{PA}$. Let c be a new constant symbol, and let $\mathcal{L} = \mathcal{L}_{ar}(M) \cup \{c\}$. Consider now the $\mathcal{L}$-theory $T := D(\mathcal{M}) \cup \{c > m, m \in M\}$, where $D(\mathcal{M})$ is the complete diagram of $\mathcal{M}$.

- Verify that T is consistent.
- Let $a \in M$ and let $\theta(v,z)$ be an $\mathcal{L}$-formula such that $T \vdash \forall v(\theta(v,c) \to v < a)$ and such that $T \cup \{\exists v \theta(v,c)\}$ is consistent. Prove that there exists $m \in M$ with $m < a$ and such that $\mathcal{M} \models \forall x(\exists z > x)\theta(m,z)$.
- Let $a \in M$ be a nonstandard element. Consider the set of formulas

$$\pi_a(v) := \{v < a\} \cup \{v \neq m, m \in M\}.$$

  Prove that π_a is a non-isolated partial 1-type in T.

(3) Conclude.

Solution: 1). We can proceed by induction in $\mathcal{M}$. If $a = 0$, there is nothing to prove. Assume as hypothesis that $\mathcal{M} \models p(a)$. Assume that

$$\mathcal{M} \models [\forall x(\exists z > x)(\exists v < a+1)\theta(v,z)]$$

In view of the following equivalence

$$\begin{aligned}\mathcal{M} \models \forall x(\exists z > x)(\exists v < a+1)\theta(v,z) &\leftrightarrow \forall x(\exists z > x)(\exists v < a)\ \theta(v,z) \vee \theta(z+1)\\ &\leftrightarrow \forall(\exists v < a)x(\exists z > x)\ \theta(v,z) \vee \theta(z+1) \text{ by I.H}\\ &\leftrightarrow (\exists v < a+1)\forall x(\exists z > x)\theta(v,z)\end{aligned}$$

The proof is complete.

2) If T_0 is a finite part of $D(\mathcal{M}) \cup \{c > m\}_{m\in M}$, then there exists $m \in M$ such that $T_0 \subseteq D(\mathcal{M}) \cup \{c > m\}$. We can take $\mathcal{M}$ as a model of T_0, interpreting $c^{\mathcal{M}} = S(m)$ and all other symbols as their respective elements of $\mathcal{M}$. Since T_0 is arbitrary, we conclude by the compactness theorem that T is consistent.

Let $a \in M$ and let $\theta(v,z)$ be an $\mathcal{L}$-formula such that $T \vdash \forall v(\theta(v,c) \to v < a)$ and such that $T \cup \{\exists v\theta(v,c)\}$ is consistent. We want to prove that

$$\mathcal{M} \models (\exists m < a)\forall x(\exists z > x)\theta(m,z).$$

For this, by the pigeonhole principle it suffices to prove the same proposition with the $\forall x$ swapped with $(\exists m < a)$. Suppose by contradiction that this is not the case. That is

$$\mathcal{M} \models \exists x(\forall m < a)(\forall z > x)\neg\theta(m,z). \tag{*}$$

Let now $\mathcal{N} \models T \cup \{\exists v\theta(v,c)\}$. Since $\mathcal{M} \preccurlyeq \mathcal{N}_{\restriction\mathcal{L}}$,

$$\mathcal{N} \models \exists x(\forall m < a)(\forall z > x)\neg\theta(m,z).$$

We then have $x \in \mathcal{N}$ a witness for this last formula. Note that then $\mathcal{N} \models x \geq c$, since we know by our hypotheses that

$$\mathcal{N} \models \exists v < a\ \theta(v,c)$$

that is, in $\mathcal{N}$, for any $x < c$ we can find $m < a$ such that $\mathcal{N} \models \theta(m, c)$. Since $\mathcal{N} \models x \geq c$, a witness of formula (*) cannot belong to M. This contradicts our initial assumption, which concludes the proof.

To see that $\pi_a(v)$ is a partial 1-type, consider a finite part $\pi(v) \subset \{v < a\} \cup \{v \neq m_i\}_{i=1}^{k}$. Let $\mathcal{N} \models T$, then $\mathcal{N}$ realizes $\pi(v)$, since a being nonstandard, there are infinitely many elements in $\mathcal{N}$ less than a, and one of them must be different from the m_i. Suppose now by contradiction that $\pi_a(v)$ is isolated; in that case there exists an $\mathcal{L}-$formula $\varphi(v)$, or more precisely, an $\mathcal{L}_{ar}(\mathcal{M})-$formula $\theta(v, z)$ such that

$$T \vdash (\theta(v, c) \to v < a)$$

$$T \vdash (\theta(v, c) \to v \neq m) \text{ for each } m \in M$$

The first condition, together with the previous item, allows us to conclude that in $\mathcal{M}$, there exists $m < a$ such that

$$\mathcal{M} \models \forall x \exists z > x \; \theta(m, z).$$

Let us see that $T \cup \{\theta(m, c)\}$ is consistent. Any finite part of this theory has the form $T_0 \subseteq D(\mathcal{M}) \cup \{c > m_0\} \cup \{\theta(m, c)\}$, for some $m_0 \in M$. We can then take $\mathcal{M} \models T_0$, interpreting c as the witness of $\exists z > m_0 \; \theta(m, z)$; this proves consistency. Let $\mathcal{N} \models T \cup \{\theta(m, c)\}$; in particular we have $\mathcal{N} \models \theta(m, c) \to m \neq m$, which is absurd. We conclude that for all nonstandard $a \in M$, $\pi_a(v)$ is a non-isolated partial 1-type.

3) Since $\mathcal{M}$ is countable, $\mathcal{L}$ is also countable, and we can apply the omitting types theorem to find an $\mathcal{L}$-structure $\mathcal{M}'$ that omits $\pi_a(v)$ for all nonstandard $a \in M$. That is, for all $m' \in M'$ and for all nonstandard $a \in M$, $\mathcal{M}' \models m' \geq a$ or $m' \in M$. In particular, this implies that if $m' \in M' \setminus M$, for any $m \in M$ we have $\mathcal{M}' \models m' > m$. $\mathcal{M}'$ is an elementary end extension of $\mathcal{M}$.

Problem 6. Tennenbaum's Theorem

Let $\mathcal{M}$ be a nonstandard model of PA and let $\eta(x,y)$ be an $\mathcal{L}_{ar}$-formula. Denote $S_\eta(\mathcal{M})$ as the family of $A \subseteq \mathbb{N}$ for which there exists $a \in M$ such that

$$A = \{n \in \mathbb{N}, \mathcal{M} \models \eta(\underline{n}, a)\}.$$

Let $S(\mathcal{M})$ be the union of $S_\eta(\mathcal{M})$, where η ranges over all formulas with two free variables.

(1) Let $\eta_0(x,y)$ be an $\mathcal{L}_{ar}$-formula such that for any pair of finite disjoint sets $A, B \subseteq \mathbb{N}$, the sentence

$$\exists x \left(\bigwedge_{i \in A} \eta_0(\underline{i}, x) \wedge \bigwedge_{j \in B} \neg\eta_0(\underline{j}, x) \right)$$

is provable in PA. Prove that $S_{\eta_0}(\mathcal{M}) = S(\mathcal{M})$.

(2) Prove that there exists a Σ_1-formula η_0 with two free variables such that for all $n \in \mathbb{N}$ the sentence

$$\eta_0(\underline{n}, x) \leftrightarrow \exists y(\underline{\pi(n)} \cdot y = x)$$

is provable in PA. Prove that $S_{\eta_0}(\mathcal{M}) = S(\mathcal{M})$. [3]

(3) Let $A, B \subseteq \mathbb{N}$ be two disjoint recursively enumerable sets.

a) The set of Δ_0-formulas is defined as the smallest set of $\mathcal{L}_{ar}$-formulas that contains the atomic formulas and is stable under $\wedge, \neg$ and under bounded quantification $(\exists x < t)$, $(\forall x < t)$, with t a term not depending on the variable x. Observe that there are Δ_0-formulas $\alpha(x,y)$ and $\beta(x,y)$ such that in $\mathbb{N}_{st}$, A is defined by $\exists y \alpha(x,y)$ and B by $\exists \beta(x,y)$.

b) Prove that for all $k \in \mathbb{N}$,

$$\mathcal{M} \models (\forall x, y, z < \underline{k}) \neg(\alpha(x,y) \wedge \beta(x,z)),$$

and that there exists nonstandard $\zeta \in M$ such that

$$\mathcal{M} \models (\forall x, y, z < \zeta) \neg(\alpha(x,y) \wedge \beta(x,z)).$$

[3] $\pi(n)$ denotes the $(n+1)$-th prime number.

c) Consider A, B infinite and recursively inseparable ($A \cap B = \varnothing$ and there is no recursive $C \subseteq \mathbb{N}$ such that $A \subseteq C$ and $C \cap B = \varnothing$). Deduce that $S(\mathcal{M})$ contains a non-recursive set.

(4) If M is countable and $h : \mathbb{N} \to M$ is a bijection, we can transport the $\mathcal{L}_{ar}$-structure $\mathcal{M}$ via h^{-1} to $\mathbb{N}$, defining $x +' y = h^{-1}(h(x) + h(y))$ and the other operations analogously. Suppose $\mathcal{M}$ is *recursive,* that is, there exists a bijection h as described, such that $+'$ and $\cdot'$ are recursive functions.

(a) For any fixed $c \in \mathbb{N}$, prove that the function $f \in \mathcal{F}^2$ given by

$$f(n,m) = \begin{cases} 1, & \text{if} \underbrace{m +' \cdots +' m}_{\pi(n)-\text{times}} = c \\ 0, & \text{in any other case} \end{cases}$$

is recursive.

(b) Deduce from this that $S(\mathcal{M})$ only contains recursive sets.

(5) Deduce Tennenbaum's theorem: *There are no nonstandard models of* PA *that are recursive.*

Solution: 1) It is only necessary to prove $S(\mathcal{M}) \subseteq S_{\eta_0}(\mathcal{M})$. Let $a \in M$, $\eta(x,y)$ be arbitrary and let $A = \{n \in \mathbb{N}, \mathcal{M} \models \eta(\underline{n}, a)\}$. We must prove that there exists $b \in M$ such that

$$A = \{n \in \mathbb{N}, \mathcal{M} \models \eta_0(\underline{n}, b)\}.$$

Let $n \in \mathbb{N}$. Take

$$A_n = \{k \leq n, \mathcal{M} \models \eta(\underline{k}, a)\}$$

$$B_n = \{k \leq n, \mathcal{M} \models \neg\eta(\underline{k}, a)\}$$

We know by hypothesis that

$$\mathsf{PA} \vdash \exists \mathsf{x} \left(\bigwedge_{\mathsf{i} \in \mathsf{A_n}} \eta_0(\underline{\mathsf{i}}, \mathsf{x}) \wedge \bigwedge_{\mathsf{j} \in \mathsf{B_n}} \neg\eta_0(\underline{\mathsf{j}}, \mathsf{x}) \right).$$

If we define the formula $\phi(x) = (\forall y \leq x)\eta_0(y,x) \leftrightarrow \eta(y,x)$, this proves in particular that $\mathcal{M} \models \phi(\underline{n})$ for any $n \in \mathbb{N}$. By the *overspill* lemma, there exists $b \in M$ (nonstandard) such that $\mathcal{M} \models \phi(b)$.

This implies that for all natural n,

$$\mathsf{PA} \vdash \eta(\underline{\mathsf{n}}, \mathsf{a}) \iff \eta_0(\underline{\mathsf{n}}, \mathsf{b})$$

which concludes the proof.

2) Note that the formula $\exists y(\underline{\pi(n)}y = x)$ expresses that "x is divisible by the n-th prime number". We need to first describe the $n-$th prime. Consider the function $f : \mathbb{N} \to \mathbb{N}$ that sends n to the number of primes strictly less than n (the π function from number theory). Note that since $f(0) = 0$ and $f(n+1) = f(n) + \mathbb{1}_{\text{prime}}$, f is a recursive function. Therefore, we can assert that $f(n) = k$ if and only if there exist $a, b \in \mathbb{N}$ such that $\beta(a, b, 0) = 0$, $\beta(a, b, n) = k$, and for each $0 < i < n$, $\beta(a, b, i+1) = \beta(a, b, i) + \mathbb{1}_{\text{prime}}$, where β is Gödel's beta function. In summary, we can represent f with a Σ_1-formula, and therefore we can also represent the following property

$$\phi(n, x) := f(x+1) = n \wedge f(x) + 1 = n$$

Note that $\mathcal{M} \models \phi(\underline{n}, x)$ if and only if x is the n-th prime number [4]. We can then define the formula we need as

$$\eta_0(n, x) = \exists y \exists z(yz = x \wedge \phi(\underline{n}, z)).$$

To see in this case that $S(\mathcal{M}) = S_{\eta_0}(\mathcal{M})$, take A, B finite and disjoint, and note that the formula

$$\exists x \left(\bigwedge_{i \in A} \eta_0(\underline{i}, x) \wedge \bigwedge_{j \in B} \neg\eta_0(\underline{j}, x) \right)$$

has as witness $x = \prod_{i \in A} \pi(i)$, which belongs to every model of PA. We see then that η_0 satisfies all hypotheses of 1).

3a) Since A is recursively enumerable, there exists a Σ_1-formula $\varphi(x)$ that describes it. We can assume without loss of generality that φ has the form $\exists x_1, x_2, \ldots x_k \tilde{\varphi}(x, x_1, \ldots, x_k)$, with $\tilde{\varphi}$ a Δ_0-formula. This is possible since φ is a Σ_1-formula, and removing the $\exists$ will leave a formula whose only quantifiers are of the type $\forall v < t$. Next, we can replace the block of existentials as follows,

$$\varphi \sim \exists y \tilde{\varphi}(x, \beta_1^k(x), \ldots, \beta_k^k(x)) =: \exists y \alpha(x, y),$$

[4]Strictly, $\pi(n)$ represents the $(n+1)$-th prime, but for convenience we have renumbered.

where β_i^k are the components of a primitive recursive bijection between $\mathbb{N}^k$ and $\mathbb{N}$. This procedure applies equally to B.

3b) Suppose by contradiction that for some k, there exist $x, y, z < k$ such that

$$\mathcal{M} \models \alpha(x, y) \wedge \beta(x, y),$$

this directly implies that $x \in A$ and $x \in B$, by item 3a). This is impossible since A and B are disjoint. The existence of the required ζ follows directly from the *overspill* lemma.

3c) First consider $k \in \mathbb{N}$. Let $i < k$ be arbitrary and observe that $i \in A$ if and only if there exists $a_i \in M$ such that $\mathcal{M} \models \alpha(\underline{i}, a_i)$, which implies by item 1) that there exists $y_i \in M$ such that $\mathcal{M} \models \eta_0(\underline{i}, y_i)$, or in other words, $\mathcal{M} \models \pi(i)|y(i)$. We can repeat this to find $z_0, z_1, \ldots, z_k$ satisfying $i \in B \Rightarrow \pi(i)|z(i)$. Note first that for all i, $y_i \neq z_i$, since if they coincided, we would again have $A \cap B \neq \varnothing$. Take $y = y_0 \ldots y_k$; then we have shown that for all $k \in \mathbb{N}$, there exists $y \in M$ such that

$$\mathcal{M} \models \exists y(\forall i < k)((i \in A \to \pi(i)|y) \wedge (i \in B \to \pi(i) \nmid y)).$$

By the *overspill* lemma, there exists nonstandard $\zeta \in M$ such that

$$\mathcal{M} \models \exists \zeta(\forall i < \zeta)((i \in A \to \pi(i)|\zeta) \wedge (i \in B \to \pi(i) \nmid \zeta)).$$

That is, there exists $\zeta \in M$ whose prime divisors are indexed by some set that contains A and is disjoint from B. Let then

$$\begin{aligned} C &:= \{n \in \mathbb{N}, \mathcal{M} \models \underline{\pi(n)}|\zeta\} \\ &= \{n \in \mathbb{N}, \mathcal{M} \models \eta_0(\underline{n}, \zeta)\} \in S_{\eta_0}(\mathcal{M}) = S(\mathcal{M}). \end{aligned}$$

Since $A \subseteq C$ and $C \cap B = \varnothing$, by the inseparability hypothesis, we conclude that $C \in S(\mathcal{M})$ is not recursive.

4a) Assuming that $+'$ is recursive, we can define the summation operation $g(n,m) = \underbrace{m +' \cdots +' m}_{n-\text{times}}$ recursively as

$$g(n,0) = 0$$

$$g(n,m+1) = g(n,m) +' m$$

It is then easy to describe the function f with recursive conditions. Observe that

$$f(n,m) = \begin{cases} 1 & \text{if } g(\pi(n),m) = c \\ 0 & \text{if not.} \end{cases}$$

Since $\pi(n)$ is primitive recursive, this proves what we wanted.

4b) Let $A \in S(\mathcal{M})$. We know from what we have been proving that there exists $a \in M$ such that the elements of A are the indices of the prime divisors of a (indexing with the usual order of $\mathbb{N}$). In other words, $n \in A$ if and only if there exists $y \in M$ such that $\mathcal{M} \models \underbrace{y + \cdots + y}_{\pi(n)-\text{times}} = a$. Let $x = h^{-1}(y)$; we can translate this condition to $\mathbb{N}$ via h. We are looking then for $x \in \mathbb{N}$ such that $\mathcal{M} \models \underbrace{h(x) + \cdots + h(x)}_{\pi(n)-\text{times}} = a$. Applying h^{-1}, we can see then that $n \in A$ if and only if there exists $x \in \mathbb{N}$ such that

$$\mathbb{N} \models \underbrace{x +' \cdots +' x}_{\pi(n)-\text{times}} = h^{-1}(a)$$

and finally, taking h^{-1} as the c from the previous item, we see that $a \in A \iff \mathbb{N} \models \exists x f(n,x) = 1$. Finding a recursive way to determine if such an x exists or not will therefore be equivalent to proving that A is recursive.

We know that the division algorithm is valid in PA, therefore it is equally valid in $\mathcal{M}$. Since $\pi(n)$ is standard, there are finitely many elements in $\mathcal{M}$ less than $\pi(n)$, and all are standard (of the form $1 + \cdots + 1$). Dividing a by $\pi(n)$, we know with certainty that there exists $q \in M$ (unique) such that the disjunction of the following formulas is true in $\mathcal{M}$.

$$a = \underbrace{q + \cdots + q}_{\pi(n)-\text{times}}$$

$$a = \underbrace{q + \cdots + q}_{\pi(n)-\text{times}} + 1$$

$$\vdots$$

$$a = \underbrace{q + \cdots + q}_{\pi(n)-\text{times}} + \underbrace{1 + \cdots + 1}_{(\pi(n)-1)-\text{times}}$$

Note that this is an exclusive disjunction. Translating via h^{-1}, denoting $\tilde{q} = h^{-1}(q)$ and $\tilde{1} = h^{-1}(1)$, we know that in $\mathbb{N}$ there exists $\tilde{q}$ such that only one of the following equalities holds.

$$h^{-1}(a) = \underbrace{\tilde{q} +' \cdots +' \tilde{q}}_{\pi(n)-\text{times}}$$

$$h^{-1}(a) = \underbrace{\tilde{q} +' \cdots +' \tilde{q}}_{\pi(n)-\text{times}} +' \tilde{1}$$

$$\vdots$$

$$h^{-1}(a) = \underbrace{\tilde{q} +' \cdots +' \tilde{q}}_{\pi(n)-\text{times}} +' \underbrace{\tilde{1} +' \cdots +' \tilde{1}}_{(\pi(n)-1)-\text{times}}$$

Since we are assuming that $+'$ is recursive, the procedure of checking the truth of each of these (finitely many) equalities is recursive. Finally, noting that the first of these is equivalent to $f(n, q) = 1$, we conclude that to recursively determine if $\exists x f(n, x)$, it suffices to check which of the equalities is true. If the first one is, then $n \in A$; otherwise, $n \notin A$. Since A was taken arbitrarily, we conclude that every element of $S(\mathcal{M})$ is recursive.

5) To conclude, simply observe that the conclusion of 4b) contradicts that of 3c). This implies that the hypothesis of 4b) cannot be possible. In other words, the existence of a recursive and nonstandard model of PA is not possible. Describe a Turing machine that computes the sum $\lambda xy.x + y$.

Solution: We define a machine $\mathcal{M}$ that has 4 tapes, B_1, B_2, B_3 and B_4. It receives the *input* on the first two tapes, and outputs the result on B_3. The machine works as follows:

(1) Copy the number indicated on B_1 to B_3, and return the head to the beginning.

(2)
- If the number on B_2 is the same as on B_4, then proceed to clear tape B_4 and finish here.
- If not, then add a $|$ to the first empty space on tape B_4, and then repeat this action for tape B_3. Next, repeat step 2.

More formally, the machine $\mathcal{M}$ has 5 states, in addition to q_i, q_f (initial and final). The transition function is given somewhat informally as follows (symbols marked by $\times$ mean it could be either $|$ or b):

$$(q_i, \$, \$, \$, \$) \mapsto (q_i, \$, \$, \$, \$, +1)$$

$$(q_i, |, \times, b, \times) \mapsto (q_i, |, \times, |, \times, +1)$$

$$(q_i, b, \times, b, \times) \mapsto (q_|, b, \times, b, \times, \text{return to start})$$

$$(q_|, \$, \$, \$, \$) \mapsto (q_2, \$, \$, \$, \$, +1)$$

$$(q_2, \times, b, \times, b) \mapsto \text{END}$$

$$(q_2, \times, |, \times, |) \mapsto (q_2, \times, |, \times, |, +1)$$

$$(q_2, \times, |, \times, b) \mapsto (q_3, \times, |, \times, |, \text{return to start})$$

$$(q_3, \$, \$, \$, \$) \mapsto (q_4, \$, \$, \$, \$, +1)$$

$$(q_4, \times, \times, |, \times) \mapsto (q_4, \times, \times, |, \times, +1)$$

$$(q_4, \times, \times, b, \times) \mapsto (q_5, \times, \times, |, \times, \text{return to start})$$

$$(q_5, \$, \$, \$, \$) \mapsto (q_2, \$, \$, \$, \$, +1)$$

Problem 2. Let p, q be primes. We say that q is *p-Mersenne* if for some $n \in \mathbb{N}$,

$$q = \frac{p^n - 1}{p - 1}.$$

Show that the set

$$\{n \in \mathbb{N}, \exists p \text{ such that } n \text{ is } p\text{-Mersenne}\}$$

is primitive recursive.

Solution: Note that if there exists m such that $n = \frac{p^m-1}{p-1}$, then $n = 1 + p + p^2 + \cdots + p^{m-1} \geq p$. Furthermore,

$$p^m - 1 = n(p - 1)$$

$$\Rightarrow \quad m \leq p^m \leq np + 1$$

We can then say that n is p-Mersenne if and only if n is prime and

$$(\exists p \leq n)(\exists m \leq Np + 1)\left(p \text{ is prime } \wedge n = \sum_{k=0}^{m-1} p^k\right)$$

Problem 3. We define the function $\mathrm{fib} \in \mathcal{F}_1$ by

$$\mathrm{fib}(0) = 0$$

$$\mathrm{fib}(1) = 1$$

$$\mathrm{fib}(n + 2) = \mathrm{fib}(n + 1) + \mathrm{fib}(n)$$

Prove that $\mathrm{fib}(n)$ is a recursive function.

Solution: Consider the function $f : \mathbb{N} \to \mathbb{N}^2$, given by

$$f(0) = (0, 1)$$

$$f(n + 1) = \left(P_2^2 f(n), P_1^2 f(n) + P_2^2 f(n)\right)$$

It is clear that f is primitive recursive, and it is also easy to see that $\mathrm{fib}(n) = P_1^2 f(n)$.

Problem 4. Kalmár's elementary functions:

E (the set of Kalmár's elementary functions) is defined as the smallest subset of $\mathcal{F}$ satisfying

- E contains the functions $C_0^0, P_i^n, \mathbb{1}_=$ for all $i, n \in \mathbb{N}$.

- if $g \in \mathcal{F}_k \cap E$, and $f_1, f_2, \ldots, f_k \in \mathcal{F}_n \cap E$, then $g(f_1, f_2, \ldots, f_k) \in E$.
- If $f \in F_{n+1} \cap E$, then bounded sums and products are in E, that is

$$\sum_{i=0}^{x} f(x_1, \ldots, x_n, i) \in E \quad , \quad \prod_{i=0}^{x} f(x_1, \ldots, x_n, i) \in E.$$

(1) Prove that C_k^n is elementary for all $k, n \in \mathbb{N}$.

Solution: Note that $C_1^0 = \mathbb{1}_=(C_0^0, C_0^0)$, then we can see that

$$C_k^0 = \sum_{i=0}^{k} C_1^0$$

and finally we see that $C_k^n(\bar{x}) = P_1^{n+1}(C_k^0, \bar{x})$.

(2) We say that $A \subseteq N^n$ is *elementary* if $\mathbb{1}_A \in E$. Prove that $\{0\}$ is elementary, and that the set of elementary parts of $\mathbb{N}$ is closed under Boolean operations.

Solution: We can define the recursive subtraction $\lambda x.1 - x$ within E by means of

$$1 - x = \mathbb{1}_=(0, x).$$

It is clear that $\mathbb{1}_{\{0\}}(x) = \mathbb{1}_=(x, C_0^0)$ is elementary. Suppose now that $A, B \subseteq \mathbb{N}$ are elementary, then

$$\mathbb{1}_{A \cap B} = \mathbb{1}_A \mathbb{1}_B$$

$$\mathbb{1}_{A^c} = 1 - \mathbb{1}_A$$

(3) Prove that $\exp(x, y) = \lambda xy.x^y$ is elementary.

Solution:

$$x^y = \prod_{i=0}^{y-1} x$$

which is recursive by axiom.

(4) Define $T \in \mathcal{F}_2$ as

$$T(m, 0) = m$$

$$T(m, n+1) = \exp(2, T(m, n))$$

Define also $T_n = \lambda x.T(x, n)$

(a) Prove that T is primitive recursive.

Solution: T is the primitive recursion between the functions $g(x) = P_1^1(x) = x$ and $h(x, y, z) = \exp(2, z)$.

(b) Prove that for all n, T_n is strictly increasing and that for fixed m, $T(m, n)$ is strictly increasing in n.

Solution: By induction, note that $T_0 = id$ is strictly increasing. Suppose now that T_n is strictly increasing. Let $m_1 < m_2$, then

$$\begin{aligned} T_{n+1}(m_1) &= 2^{T_n(m_1)} \\ &< 2^{T_n(m_2)} \text{ (IH)} \\ &= T_{n+1}(m_2) \end{aligned}$$

which proves what we wanted.

Suppose now that m is fixed, and note that for all n

$$T_{n+1}(m) = 2^{T_n(m)} > T_n(m)$$

so, for all $k > 0$,

$$T_n(m) < T_{n+1}(m) < \cdots < T_{n+k}(m).$$

This proves that T is strictly increasing in n as well.

(c) Prove that every elementary function is dominated by some T_n.

Solution: Note that $T_1(m) = 2^m$, and that

- $C_k^n \leq T_1(m)$, except for finitely many m's. This is clear since we already know that T_1 is strictly increasing and the left side is constant.
- $P_i^n(\bar{x}) \leq 2^{\max \bar{x}}$. This is clear.
- $\sum_{k=0}^n x_k \leq n \max_k x_k < 2^{\max_k x_k}$ except for finitely many tuples. This is because in general, $nt < 2^t$ for t sufficiently large.
- $\prod_{k=0}^n x_k \leq (\max_k x_k)^n < 2^{\max_k x_k}$ except for finitely many tuples. This is because, in general, $t^n < 2^t$ for t sufficiently large.

Suppose now that $g \in E \cap \mathcal{F}_n$, and that $f_1, \ldots, f_n \in E \cap \mathcal{F}_m$. If there exist $n, n_1, \ldots, n_m$ such that (except for finitely many tuples $\bar{y} \in \mathbb{N}^n$ and $\bar{x} \in \mathbb{N}^m$)

$$g(\bar{y}) \leq T_n(\max \bar{y})$$

$$f_i(\bar{x}) \leq T_{n_i}(\max \bar{x}) \quad \text{for } i = 1, \ldots, n$$

Then, except for finitely many tuples, we have

$$\begin{aligned}
g(f_1(\bar{x}), \ldots, f_n(\bar{x})) &\leq T_n(\max \{f_1(\bar{x}), \ldots, f_n(\bar{x})\}) \\
&\leq T_n\left(\max \{T_{n_1}(\max \bar{x}), \ldots, T_{n_m}(\max \bar{x})\}\right) \\
&\leq T_n(T_N(\max \bar{x})), \qquad \text{where } N = \max \{n_1, \ldots, n_m\} \\
* &\leq T_{N+n+1}(\max \bar{x})
\end{aligned}$$

which proves what we wanted. To prove the last inequality, we proceed by induction; note that

$$T_0(T_N(m)) = T_N(m)$$

which confirms the base case. Assuming inequality $(*)$ for n, we see that

$$\begin{aligned}
T_{n+1}(T_N(m)) &= \exp(2, T_n(T_N(m))) \\
&\leq \exp(2, T_{n+N+1}(m)) \text{ (IH)} \\
&= T_{n+N+2}(m)
\end{aligned}$$

We have thus proved that all basic functions are dominated by some T_n, as are their sums, products, and compositions. Therefore, every Kalmár elementary function is dominated by some T_n.

(d) Prove that T is not elementary.

Solution: Suppose that T is elementary, then $\lambda n.T_n(n)$ is elementary, which implies that there exist M and N such that if $n \geq N$

$$T_n(n) \leq T_M(m)$$

This is impossible for $n > \max\{N, M\}$. Therefore we deduce that T cannot be an elementary function.

Problem 5.

(1) Let $f \in \mathcal{F}_1$ be an increasing recursive function. Prove that $\mathrm{Im}(f)$ is recursive.

Solution: Note that

$$y \in \mathrm{Im}(f) \iff (\exists x \leq y)(f(x) = y).$$

We can assert that $x \leq y$ since f is increasing.

(2) Prove that every infinite recursive $X \subseteq \mathbb{N}$ is the image of a unary recursive function.

Solution: Let $X \subseteq \mathbb{N}$ be infinite and recursive. Define $f : \mathbb{N} \to \mathbb{N}$ given by

$$f(0) = \mu m(m \in X)$$
$$f(n+1) = \mu m(m \in X \wedge m > f(n))$$

f is recursive and strictly increasing by definition. Clearly $\mathrm{Im}\, f = X$.

(3) Prove that every infinite and recursively enumerable X contains an infinite recursive set.

Solution: Let $X \subseteq \mathbb{N}$ be infinite and recursively enumerable. Then there exists $f : \mathbb{N} \to \mathbb{N}$ total recursive such that $X = \mathrm{Im}\, f$. Then define $g : \mathbb{N} \to \mathbb{N}$ given by

$$g(0) = f(0)$$
$$g(n+1) = \mu x(x \in X \wedge x > f(n))$$

Observe that g is recursive and strictly increasing, so $\mathrm{Im}\, g$ is recursive (by the previous point). Note also that $\mathrm{Im}\, g \subseteq \mathrm{Im}\, f$.

Problem 6. Construction of a primitive bijection whose inverse is not primitive recursive.

(1) Prove that the set of bijective recursions on $\mathbb{N}$ forms a group.

Solution: Let $S = \{f : \mathbb{N} \to \mathbb{N}, f \text{ is bijective}\}$. It is clear that if $f, g \in$, then $f \circ g \in S$, by axioms of recursion. Moreover, it is also clear that the identity is in S, and is the neutral element. Finally, note that if $f \in S$, then

$$f^{-1}(y) = \mu x(f(x) = y)$$

which shows that $f^{-1} \in S$.

(2) Prove that for every Turing machine $\mathcal{M}$ that computes a total function, the graph of the time function $T_{\mathcal{M}}$ is primitive recursive.

Solution: Note that if $\bar{x} \in \mathbb{N}^n$, then

$$(\bar{x}, t) \in G(T_{\mathcal{M}}) \iff ((i, t, \bar{x}) \in B^n) \wedge (\forall z \leq t)((i, z, \bar{x}) \notin B^n)$$

where $G(T_{\mathcal{M}})$ is the graph of $T_{\mathcal{M}}$ and B^n is the set of 3-tuples $(i, t, \bar{x})$ where the machine with index i and *input* $\bar{x}$ is in a final state at time t, with a valid *output* configuration (i.e., one that represents a number on the output tape).

(3) Prove that $f \in \mathcal{F}_n$ is primitive recursive if and only if its graph is primitive recursive and f is bounded above by some primitive recursive function.

Solution: Suppose that f is primitive recursive, then its graph satisfies

$$\mathbb{1}_{G(f)}(\bar{x}, y) = \mathbb{1}_{=}(f(\bar{x}, y)$$

which makes $G(f)$ primitive recursive. Moreover, we know that there exist $n, k \in \mathbb{N}$ such that, except for finitely many tuples $\bar{x}$,

$$f(\bar{x}) \leq \xi_n^k(\max \bar{x}),$$

where ξ_n^k is the Ackermann function evaluated at n and composed with itself k-times. Then we can define N as the maximum value that $f(\bar{x})$ takes on the tuples that do not satisfy the above inequality, and conclude that

$$f(\bar{x}) \leq \max\{N, \xi_n^k(\max \bar{x})\}.$$

Suppose now that $G(f)$ is primitive and that there exists a primitive recursive function g such that for all $\bar{x}$

$$f(\bar{x}) \leq g(\bar{x}).$$

We can then characterize f in a primitive recursive way as follows:

$$f(\bar{x}) = (\mu y \leq f(\bar{x})((\bar{x}, y) \in G(f)).$$

(4) Let $g \in \mathcal{F}_1$ be strictly increasing. Prove that the graph of g is primitive recursive if and only if $\operatorname{Im} g$ is primitive recursive.

Solution: If we first assume that $G(g)$ is primitive recursive, then we can characterize $\operatorname{Im} g$ as

$$y \in \operatorname{Im} g \iff (\exists x \leq y)((x, y) \in G(f)).$$

If we now assume that the image of g is a primitive recursive set, then

$$(x, y) \in G(g) \iff (x, y) \in (P_1^2)^{-1}[\operatorname{Im} y],$$

since the property of being primitive recursive is preserved under preimage of a primitive recursive function.

(5) Let $f \in \mathcal{F}_1$ be recursive but not primitive recursive, and let $\mathcal{M}$ be a Turing machine that computes f.

(a) Let $g_0 \in \mathcal{F}_1$ be defined by

$$g_0(x) = \max\{T_{\mathcal{M}}(y), y \leq x\} + 2x.$$

Prove that g_0 is recursive, but not primitive recursive. Prove also that its graph and image are both primitive recursive.

Solution: Note that g_0 is strictly increasing and recursive (since $T_{\mathcal{M}}$ is). Note that (Kleene normal form)

$$f(x) = (\mu y \leq T_{\mathcal{M}})((i, y, T_{\mathcal{M}}(\bar{x})x) \in C^p).$$

If $g_0(x)$ were primitive recursive, since by definition $g_0(x) > T_{\mathcal{M}}$, we would have the same expression for $f(x)$ but with primitive recursive time,

$$f(x) = (\mu y \leq g_0(x))((i, y, T_{\mathcal{M}}(\bar{x}), \bar{x}) \in C^p).$$

This would imply that f is primitive recursive, a contradiction.

(b) Let $g_1 \in \mathcal{F}_1$ be some strictly increasing function such that $\operatorname{Im} g_1 = \mathbb{N} \setminus \operatorname{Im} g_0$. Consider the function $h \in \mathcal{F}_1$ given by

$$h(2x) = g_0(x)$$
$$h(2x+1) = g_1(x)$$

Prove that h is a recursive bijection that is not primitive recursive. Prove that h^{-1} is primitive recursive.

Solution:

Injectivity: Let $x, y \in \mathbb{N}$. If $x \not\equiv y \pmod 2$, by definition, it is not possible that $h(x) = h(y)$ since h $\operatorname{Im} g_0 \cap \operatorname{Im} g_1 =$. If x and y have the same parity, and if w.l.o.g $x < y$, we have $h(x) < h(y)$, since both g_0 and g_1 are strictly increasing.

Surjectivity: Note that

$$\operatorname{Im} h = \operatorname{Im} g_0 \cup \operatorname{Im} g_1 = \mathbb{N}.$$

Recursivity: We know that g_0 is recursive and that $\operatorname{Im} g_0$ is primitive recursive, so $\operatorname{Im} g_1 = \mathbb{N} \setminus \operatorname{Im} g_0$ is also primitive recursive, which implies, by point 4), that $G(g_1)$ is primitive recursive. Now observe that

$$g_1(x) = \mu y((x, y) \in G(g_1)),$$

which implies that g_1 is recursive. We conclude that h is recursive by definition by cases.

h **is not primitive recursive:** Suppose by contradiction that it is, then by 3), there exists a primitive recursive function p such that for all x

$$h(x) \leq p(x)$$
$$\Rightarrow h(2x) \leq p(2x), \text{ in particular}$$
$$\Rightarrow g_0(x) \leq p(2x)$$

That is, g_0 is bounded by a primitive recursive function, and since $G(g_0)$ is primitive recursive, we conclude by 3) that g_0 is primitive recursive, a contradiction to the previous item.

h^{-1} **is primitive recursive:** We can prove this by describing h explicitly,

$$h^{-1}(y) = \begin{cases} 2((\mu x \leq y)((x, y) \in G(g_0))) \text{ if } x \in \operatorname{Im} g_0 \\ \\ 2((\mu x \leq y)((x, y) \in G(g_1))) + 1 \text{ if } x \in \operatorname{Im} g_1 \end{cases}$$

Problem 7: Existence of recursively enumerable sets that are recursively inseparable.

Note: Recall that φ_i^p denotes the i-th recursive function of p variables.

(1) Given $k \in \mathbb{N}$, denote by Z_k the set of all $n \in \mathbb{N}$ such that $n \in \operatorname{dom}(\varphi_n^1)$ and $\varphi_n^1(n) = k$. Prove that Z_k is recursively enumerable for all k.

Solution: Note that the function $g(n) = \lambda n.\varphi_n^1(n)$ is partial recursive, so $Z_k = g^{-1}[\{k\}]$ is recursive. Moreover, since

$$Z_k^c = \{n \in \mathbb{N}, \varphi_n^1(n) \neq k\} = g^{-1}[\{k\}^c],$$

we see that its complement is recursive. We conclude then that Z_k is recursively enumerable.

(2) Deduce that there exist disjoint recursively enumerable sets $A, B \subseteq \mathbb{N}$ such that there is no recursive C satisfying $A \subseteq C$ and $C \cap B = \varnothing$.

Solution: Take $A = Z_2$ and $B = Z_1 \cup Z_0$. Suppose that such C exists, then by universal properties, for some index i,

$$\mathbb{1}_C = \varphi_i^1,$$

note that this necessarily makes φ_i^1 total. Now observe that

- If $i \in C$, then $\mathbb{1}_C(i) = 1 = \varphi_i^1(i)$.
- If $i \notin C$, then $\mathbb{1}_C(i) = 0 = \varphi_i^1(i)$.

In both cases, we would have $i \in B$, which is a contradiction to the definition of C.

(3) Prove that there exists a unary partial recursive function that cannot be extended to a total recursive function.

Solution: Let $D = \cup_k Z_k = \operatorname{dom}(\lambda x.\varphi_x(x))$. Define the function $g : D \to \mathbb{N}$ given by $g(d) = \varphi_d(d) + 1$. Suppose by contradiction that there exists $\tilde{g} : \mathbb{N} \to \mathbb{N}$, total recursive, that extends g. Let then j be such that for all x,

$$\tilde{g}(x) = \varphi_j^1(x).$$

We have that, in particular:

- If $j \notin D$, then $\varphi_j^1(j)$ is not defined! This contradicts the fact that $\tilde{g}$ is total.
- If $j \in D$, then $\tilde{g}(j) = \varphi_j^1(j)$, but since $\tilde{g}$ extends g, we also have $\tilde{g}(j) = g(j) = \varphi_j^1(j)+1$. This is impossible.

We conclude then that g cannot be extended.

Problem 8. Prove that there exist primitive recursive functions $s_1, s_2 \in \mathcal{F}_1$ such that if φ_i^2 is bijective, the two components of its inverse can be expressed as $\varphi_{s_1(i)}^1$, $\varphi_{s_2(i)}^1$.

Solution: Suppose that $\varphi_i^2(x,y) = n$. We will prove the fact for the first coordinate, while the second coordinate is handled analogously. Let $g_1(i,n)$ be the first coordinate of the inverse of φ_i^1. We know from a previous exercise that g_1 is recursive, so we can choose $j \in \mathbb{N}$ such that

$$g(i,n) = \varphi_j^2(i,n).$$

It is important to note that j depends on neither i nor n. Applying the *smn* theorem, we see that there exists $s_1^1 \in \mathcal{F}_2$ primitive recursive such that

$$g(i,n) = \varphi_{s_1^1(j,i)}^1(n).$$

Since j does not depend on any other variable, we can simply take $s_1(i) := s_1^1(j,i)$.