Logique
TD n°8

Emilie Grienenberger
emilie.grienenberger@lsv.fr

March 31, 2021

In the following, we will use the result:

> Let ϕ be a quantifier-free formula. There is an equivalent formula of the form $\bigvee_{i\in I}\left(\bigwedge_{j\in J} L_{i,j}\right)$ where $L_{i,j}$ are literals. This form is called DNF (disjunctive normal forms).

Exercise 1 : Another theory of numbers

We work over signature $\mathcal{F} = \{\ 0(0)\ ,\ S(1)\ \}$, $\mathcal{P} = \{\ =(2)\ \}$ and define the theory of axioms the axioms of equality and:

$$\begin{array}{rll} & (F_1) & \forall x.\ S(x) \neq 0 \\ & (F_2) & \forall x, y.\ S(x) = S(y) \Rightarrow x = y \\ & (F_3) & \forall x.\ \exists y.\ x = 0 \vee x = S(y) \\ \text{For every } n > 0, & (C_n) & \forall x.\ S^n(x) \neq x \end{array}$$

Let $T' = \{\ F_1\ ,\ F_2\ ,\ F_3\ \}$ and $T = T' \cup \{\ C_n\ \}_{n>0}$.

1. Show that any model of T is infinite.

   In any model $\mathcal{M}$ of T, $S_\mathcal{M}$ is injective but not surjective, so $\mathcal{D}_\mathcal{M}$ is infinite.

2. Find a model of T of domain $\mathbb{Q}$.

   There is a bijection $\phi : \mathbb{N} \to \mathbb{Q}$. We define the model $\mathbb{Q}'$ with domain $\mathbb{Q}$, interpretations $0_{\mathbb{Q}'} = \phi(0)$ and $S_\mathbb{Q}(\phi(a)) = \phi(a+1)$.

3. Show that, for every n, $T' \nvdash C_n$. Conclude that T' and T are not equivalent.

   Let $\mathcal{M}$ be the structure of domain $\mathbb{N} \uplus \{\ \omega\ \}$ and interpretations $0_\mathcal{M} = 0$, $S_\mathcal{M}(n) = n+1$, and $S_\mathcal{M}(\omega) = \omega$. $\mathcal{M}$ is a model of T', but for any n, $\mathcal{M} \not\models C_n$. By correction, T' and T are not equivalent.

4. Let A be the set of boolean combinations of atomic formulas.

(a) Let F be a conjunction of literals containing x on only one side of equality. Give an algorithm transforming formula $\exists x.\ F$ into a formula G such that $T \vdash \exists x.\ F \Leftrightarrow G$.

Atomic formulas in F are of the form $S^j(x) = S^i(0)$, $S^j(x) = S^i(y)$ where $j \geq 0$ and $i \geq 0$.
For any p, any atomic formula of the form $S^j(x) = t$ where $t = S^i(0)$ or $t = S^i(y)$ is equivalent in theory T to atomic formula $S^{j+p}(x) = S^p(t)$ by the axioms of equality and the injectivity of S. As a consequence, there is a n and a conjunction of literals F' such that $T \vdash F' \Leftrightarrow F$ and all atomic formulas in F' are of the form $S^n(x) = S^j(y)$ or $S^n(x) = S^j(0)$.
Let z be a fresh variable and G the formula F' where every occurrence of $S^n(x)$ is replaced by z. We define $G' = z \neq 0 \wedge \cdots \wedge z \neq S^{n-1}(0) \wedge G$. Then $T \vdash \exists x. F' \Leftrightarrow \exists z. G'$ and there are two cases:

- If there is a literal of the form $z = S^j(t)$ in G' where $t = 0$ or $t = y$, then $T \vdash \exists x. F \Leftrightarrow G'\{z \to S^j(t)\}$.
- Else, G' is of the form $\bigwedge_{i \in I} \neg(z = S^{n_i}(t_i))$ where $t_i = 0$ or $t_i = y$ for a variable y. We have $T \vdash \exists x. F \Leftrightarrow \top$ as every model of T is infinite.

(b) Show that T admits quantifier elimination.

We use the same reasoning as in Exercise 1.

5. Show that T is complete.

Immediate by quantifier elimination and the form of closed quantifier-free formulas.

6. Let T" $= \{ F_1 , F_2 \} \cup \{ Ind_{F,x} \mid F$ a formula with at least one free variable $\}$ where $Ind_{F,x}$ is the induction applied to formula F and variable x. Prove that T and T" are equivalent.

We have already proven F_3 by induction in a previous exercise sheet. Formulas C_n are provable by immediate induction. As a consequence, $T'' \vdash T$.

Conversely, let us prove that $Ind_{F,x}$ holds in T for any F. As T is complete, either $T \vdash Ind_{F,x}$ either $T \vdash \neg Ind_{F,x}$, but $\mathbb{N}$ is a model of T so the latter option is contradictory. As a consequence, $T \vdash Ind_{F,x}$.

7. Show that T has a model $\mathcal{M}$ of domain $\{0\} \times \mathbb{N} \cup \{1\} \times \mathbb{R}$. What can we conclude?

We define $0_{\mathcal{M}} = (0, 0)$ and $S_{\mathcal{M}}((i, x)) = (i, x + 1)$. We can conclude that a set containing $\mathbb{R}$ satisfies induction.

Exercise 2 : Presburger arithmetic

We study the first order theory of natural numbers and addition called Presburger arithmetic. More precisely, it is the first order theory over the language containing the binary predicate symbol $=$ and function symbols 0, S, and $+$ and of axioms every formula true over natural numbers, i.e. every formula Φ such that for every valuation $\sigma : \mathcal{X} \to \mathbb{N}$ we have $\mathbb{N}, \sigma \models \Phi$. In the following, two formulas ϕ_1, ϕ_2 are said to be equivalent if for any valuation σ, $\mathbb{N}, \sigma \models \phi_1$ iff $\mathbb{N}, \sigma \models \phi_2$.

1. Show that any formula can be transformed in polynomial time in an equivalent formula of atomic formulas of the form $x = 0$, $x = S(y)$ or $x + y = z$ (where x, y, z are variables) without any universal quantifiers. We say such a formula is *reduced*.

We remove the universal quantifiers using the equivalence: $\vdash \forall x.\ \phi \Leftrightarrow \neg(\exists x.\ \neg\phi)$. We inductively use the following transformation $|.|$ over atomic propositions:

$$\begin{array}{rcl} |x = y| & = & x + z = y \wedge z = 0 \\ |t_1 = x| & = & |x = t_1| \text{ (if } t_i \text{ is not a variable)} \\ |t_1 = S(t_2)| & = & |x = t_1| \wedge |y = t_2| \wedge |x = S(y)| \\ |t_1 = t_2 + t_3| & = & |z = t_1| \wedge |x = t_2| \wedge |y = t_3| \wedge x + y = z \end{array}$$

This transformation preserves equivalence using properties of equality in $\mathbb{N}$.

We encode natural numbers in base 2, little-endian convention (the heaviest byte is on the right). We define a decoding function $\nu : \{0,1\}^* \to \mathbb{N}$ by:

$$\nu(\epsilon) = 0 \qquad \nu(0w) = 2\nu(w) \qquad \nu(1w) = 1 + 2\nu(w)$$

This function is surjective but not injective. Let $\mathcal{V} \subseteq \mathcal{X}$ be a subset of variables. Valuations $\sigma : \mathcal{V} \to \mathbb{N}$ are coded by words on the alphabet $\Sigma_{\mathcal{V}} = \{0,1\}^{\mathcal{V}}$. If w is a word over $\Sigma_{\mathcal{V}}$, we define w_x the projection on its x^{th} component. The function ν can be extended to a function from $\Sigma_{\mathcal{V}}^*$ to valuations over $\mathcal{V}$ by:

$$\nu(w) = (x \mapsto \nu(w_x))_{x \in \mathcal{V}}$$

If Φ is a formula and $\mathcal{V}$ contains the free variables of Φ, we write $[\Phi]_{\mathcal{V}} = \{w \in \Sigma_{\mathcal{V}}^* \mid \mathbb{N}, \nu(w) \vDash \Phi\}$.

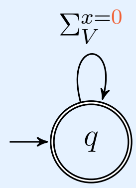
2. Show that a formula Φ is satisfied by $\mathbb{N}$ iff $[\Phi]_{fv(\Phi)} = \Sigma_{fv(\Phi)}^*$ where $fv(\Phi)$ is the set of the free variables of Φ.

$$\begin{array}{rcl} \mathbb{N} \text{ satisfies } \Phi & \Leftrightarrow & \text{for every valuation } \sigma, \mathbb{N}, \sigma \models \phi \\ & \Leftrightarrow & \text{for every word } w \in \Sigma_{fv(\Phi)}^*, \mathbb{N}, \nu(w) \models \Phi \\ & & \text{(as } \nu \text{ is surjective)} \\ & \Leftrightarrow & [\Phi]_{fv(\Phi)} = \Sigma_{fv(\Phi)}^* \end{array}$$

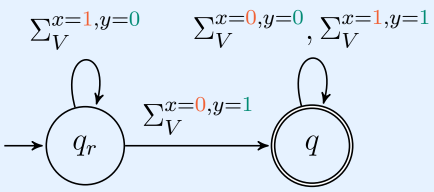
3. Show that for any reduced formula Φ, there exists a finite automaton A_Φ over alphabet $\Sigma_{fv(\Phi)}$ of language $[\Phi]_{fv(\Phi)}$.

We proceed by induction on ϕ, using a set V such that $fv(\phi) \subseteq V$:

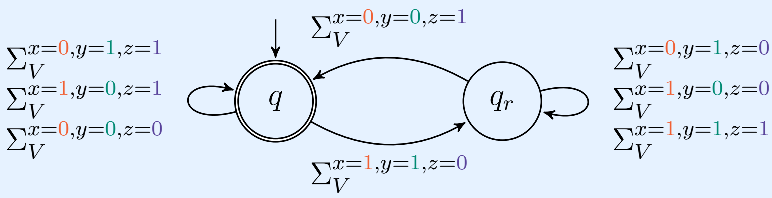
If $\phi = (x = 0)$, we build the automaton:



If $\phi = (x = S(y))$, we build the automaton:



If $\phi = (x + y = z)$, we build the automaton:



Boolean operations: rational languages are closed by conjunction, disjunction, complement, projection.

Existential quantifier $\exists x.\ \phi$: projection on $\Sigma_{V\setminus\{x\}}$ of every transition. Add as terminal every state which is the start of a path labelled by 0^* and reaching an accepting state, to account for the noninjectivity of ν.

4. Show that Presburger arithmetic is decidable. What is the complexity of this procedure?

Let Φ be a closed formula.

We transform Φ to Ψ by the transformation in Question 1. in polynomial time, and we build a corresponding automaton A_Ψ in exponential time (we use the complement construction which requires determinization).

We can decide the universality of automaton A_Ψ (exponential), so we can decide Presburger arithmetic.

Exercise 3 : Theory of total dense orders without borders

We work over the language containing the binary predicate symbols $<$ and $=$.

The theory $\mathcal{T}_O$ is defined with the axioms of equality and:

$$\begin{array}{lrl} (O_1) & \forall x \forall y. & \neg(x < y \wedge y < x) \\ (O_2) & \forall x \forall y \forall z. & x < y \wedge y < z \Rightarrow x < z \\ (O_3) & \forall x \forall y. & x < y \vee x = y \vee y < x \\ (O_4) & \forall x \forall y \exists z. & x < y \Rightarrow x < z \wedge z < y \\ (O_5) & \forall x \exists y. & x < y \\ (O_6) & \forall x \exists y. & y < x \end{array}$$

Models of $\mathcal{T}_O$ are sets with a total, dense order without borders.

1. Let us familiarize ourselves with this theory:
   (a) Show that models of $\mathcal{T}_O$ are infinite.

   Let $\mathcal{M}$ be a model of $\mathcal{T}_0$. We build an infinite sequence:

   - $\mathcal{D}_\mathcal{M} \neq \emptyset$, so there is $x_0 \in \mathcal{D}_\mathcal{M}$.
   - By (O_5), there is $x_{n+1} > x_n$, and $\neg(x_n = x_{n+1})$ by antisymmetry and transitivity.

   (b) Give two models of $\mathcal{T}_O$ that are not isomorphic.

   $\mathbb{Q}$ and $\mathbb{R}$.

   (c) Show that $\mathcal{T}_O$ is consistent.

   $\mathcal{T}_O$ has a model, so is consistent by correction.

The goal of this exercise is to prove that this theory is decidable, by proving it satisfies the elimination of quantifiers. We want to show that for every formula ψ of the form $\exists x. \bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} L_{i,j}$ of free variables $x_1, \ldots, x_n$ where L_i is a literal, there exists a quantifier-free formula ϕ of free variables in $x_1, \ldots, x_n$ such that $\mathcal{T}_O \vdash \forall x_1, \ldots, x_n. [\phi \Leftrightarrow \psi]$.

2. Show that we can consider that ψ contains only literals of the form $x = x_i$, $x_i = x_j$, $x_i < x_j$, $x_i < x$, $x < x_i$.

We have:

$$\begin{array}{lcl} \mathcal{T}_O & \vdash & (x = x) \Leftrightarrow \top \\ \mathcal{T}_O & \vdash & (x < x) \Leftrightarrow \bot \\ \mathcal{T}_O & \vdash & \neg(x = x) \Leftrightarrow \bot \\ \mathcal{T}_O & \vdash & \neg(x < x) \Leftrightarrow \top \\ \mathcal{T}_O & \vdash & (x_i = x) \Leftrightarrow (x = x_i) \\ \mathcal{T}_O & \vdash & \neg(t_1 = t_2) \Leftrightarrow t_1 < t_2 \vee t_2 < t_1 \\ \mathcal{T}_O & \vdash & \neg(t_1 < t_2) \Leftrightarrow t_1 = t_2 \vee t_2 < t_1 \end{array}$$

We distribute the created disjunctions to stay in DNF.

3. Show that proving the result on formulas of the form $\exists x.\ \bigwedge_{j=1}^{m} K_j$ where K_j is of the form $x = x_i$, $x_i = x_j$, $x_i < x_j$, $x_i < x$, or $x < x_i$ is enough to conclude.
Hint: use the equivalence $\vdash \exists x.\ [\phi_1 \vee \phi_2] \Leftrightarrow (\exists x.\ \phi_1) \vee (\exists x.\ \phi_2)$.

Using this equivalence we have that:

$$\exists x.\ \bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} L_{i,j} \quad \Leftrightarrow \quad \bigvee_{i=1}^{n} \exists x.\ \bigwedge_{j=1}^{m} L_{i,j}$$

If we find a quantifier-free equivalent to each $\exists x.\ \bigwedge_{j=1}^{m} L_{i,j}$, we can conclude.

We will consider that ψ is of the form described in Question 3. in the following.

4. Show that if ψ contains a literal of the form $x = x_i$, we can conclude.

By the axioms of equality or the substitution lemma:

$$\mathcal{T}_O \ \vdash \ \forall x_1, \dots, x_n.\ [\psi \Leftrightarrow \psi'\{x \to x_i\}]$$

5. Else, show that ψ is equivalent to a formula of the form $K_1 \wedge \exists x.\ K_2$ where:
   - $K_1 = \bigwedge_r K_r$ of free variables in $x_1, \dots, x_n$,
   - K_2 is of the form

   $$\bigwedge_{i \in I} x_i < x \quad \wedge \quad \bigwedge_{j \in J} x < x_j$$

   where I and J are subsets of $\{\ 1\ , \ \dots\ , \ n\ \}$.

We use the equivalence $\vdash \exists x.\ (\phi_1 \vee \phi_2) \Leftrightarrow (\exists x.\ \phi_1) \vee \phi_2$, which holds when $x \notin fv(\phi_2)$, and the associativity/commutativity of conjunction.

6. Show that if $I \cap J \neq \emptyset$ then ψ is equivalent to $\bot$.

In this case $\psi = \exists x.\ [(x_i < x) \wedge (x < x_i) \wedge \psi']$, and by antisymmetry (O_1) ψ is equivalent to $\exists x.\ \bot \wedge \psi'$ which is equivalent to $\bot$.

7. Show that if $I \cap J = \emptyset$ then ψ is also equivalent to a quantifier-free formula.

There are two cases:

- Either $I = \emptyset$, and by (O_5), $\mathcal{T}_O \vdash \psi \Leftrightarrow \top$.
- Either $I \neq \emptyset$ and $J \neq \emptyset$, and by (O_4):

$$\mathcal{T}_O \ \vdash \ \psi \Leftrightarrow \bigwedge_{(i,j) \in I \times J} x_i < x_j$$

8. Conclude that $\mathcal{T}_O$ is complete, and decidable.