

TD 8 – Théories décidables

Nicolas Dumange nicolas.dumange@ens-paris-saclay.fr
Théo Vignon theo.vignon@ens-paris-saclay.fr

Dans ce TD, on pourra utiliser le résultat suivant :

Définition — DNF

Soit φ une formule sans quantificateurs. Il existe une formule équivalente de la forme

$$\bigvee_{i \in I} \left(\bigwedge_{j \in J} L_{i,j} \right)$$

où $L_{i,j}$ sont des formules atomiques. Cette formule est appelée DNF de φ (forme normale disjonctive).

Exercice 1 — Une autre théorie des nombres

Dans cet exercice, on considère la signature suivante : $\mathcal{F} = \{0(0), S(1)\}$, $\mathcal{P} = \{=(2)\}$. On considère également l'ensemble d'axiomes suivant :

$$(F_1) \quad \forall x. S(x) \neq 0$$

$$(F_2) \quad \forall x, y. S(x) = S(y) \Rightarrow x = y$$

$$(F_3) \quad \forall x. \exists y. x = 0 \vee x = S(y)$$

$$\text{Pour tout } n > 0, (C_n) \quad \forall x. S^n(x) \neq x$$

On définit $T' = \{F_1 F_2 F_3\}$ et $T = T' \cup \{C_n\}_{n>0}$.

- Montrez que tout modèle de T est infini.
- Trouvez un modèle de T qui a pour domaine $\mathbb{Q}$
- Montrez que, pour tout n , $T' \not\models C_n$. Concluez que T' et T ne sont pas équivalents.
- Montrez que, pour tout n , $T' \cup \{C_k\}_{k<n} \not\models C_n$.
- Soit A l'ensemble des combinaisons booléennes de formules atomiques.
 - Soit F une conjonction de formules atomiques contenant x seulement d'un côté de l'égalité. Donnez un algorithme transformant la formule $\exists x.F$ en une formule sans quantificateurs G tel que $T \vdash \exists x.F \Leftrightarrow G$.
 - Montrez que l'on peut éliminer les quantifications dans T
- Montrez que T est complète.
 - Soit $T'' = \{F_1 F_2\} \cup \{\text{Ind}_{F,x} \mid F \text{ formule avec au moins une variable libre } x\}$ où $\text{Ind}_{F,x}$ est l'axiome d'induction sur la formule F et la variable x . Montrez que T et T'' sont équivalentes.

Exercice 2 — Théorie des ordres totaux denses sans extrémités

Nous travaillons sur le langage contenant les symboles de prédicat binaires $<$ et $=$.

Définition — Théorie des ordres totaux denses sans extrémités $\mathcal{T}_O$

La théorie $\mathcal{T}_O$ est définie par les axiomes de l'égalité et:

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

Les modèles de $\mathcal{T}_O$ sont les ensembles munis d'un ordre total dense sans extrémités.

1. Familiarisons-nous avec cette théorie:
 1. Montrez que ses modèles sont infinis.
 2. Donnez deux modèles non isomorphes de $\mathcal{T}_O$
 3. Montrez que $\mathcal{T}_O$ est cohérente.

Le but de cet exercice est de montrer que cette théorie est décidable, en montrant qu'elle satisfait l'élimination des quantificateurs. On veut donc montrer que, pour toute formule ψ de la forme $\exists x. \bigvee_{i=1}^n \bigwedge_{j=1}^m L_{i,j}$ de variables libres $x_1, \dots, x_k$ où $L_{i,j}$ est un atome, il existe une formule φ sans quantificateurs avec les mêmes variables libres telle que $\mathcal{T}_O \vdash \forall x_1, \dots, x_k. [\varphi \Leftrightarrow \psi]$.

2. Montrez que l'on peut se ramener au cas où ψ ne contient que des atomes de la forme : $x = x_i$, $x_i = x_j$, $x_i < x_j$, $x_i < x$, $x < x_i$.
3. Montrez qu'il suffit de montrer le résultat pour des formules de la forme $\exists x. \bigwedge_{j=1}^m K_j$ où K_j est de la forme $x = x_i$, $x_i = x_j$, $x_i < x_j$, $x_i < x$, or $x < x_i$.

On considère donc par la suite une formule ψ de la forme décrite en question 3.

4. Traitez le cas où ψ contient une formule de la forme $x = x_i$.
5. Dans le cas contraire, montrez que ψ est équivalente à une formule de la forme $K_1 \wedge \exists x. K_2$ telle que:
 - $K_1 = \bigwedge_r K_r$ de variables libres $x_1, \dots, x_k$,
 - K_2 est de la forme

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

où I et J sont des sous-ensembles de $\{1, \dots, n\}$.

6. Montrez que si $I \cap J \neq \emptyset$ alors ψ est équivalente à $\perp$.
7. Montrez que si $I \cap J = \emptyset$ alors ψ est équivalente à une formule sans quantificateurs.
8. Concluez que $\mathcal{T}_O$ est complète, et décidable.

Exercice 3 — Arithmétique de Presburger

On étudie une théorie sur les entiers naturels et l'addition appelée l'arithmétique de **Presburger**. Plus précisément, c'est une théorie sur le langage contenant le symbole de prédicat binaire $=$, les symboles de fonctions $0, S$ et $+$ et a pour axiomes toutes les formules vraies pour les entiers naturels, i.e. toute formule Φ tel que pour toute valuation $\sigma : \mathcal{X} \Rightarrow \mathbb{N}$, on a que $\mathbb{N}, \sigma \models \Phi$. Dans la suite on dit que deux formules φ_1, φ_2 sont équivalentes si pour toute valuation σ , $\mathbb{N}, \sigma \models \varphi_1$ si, et seulement si, $\mathbb{N}, \sigma \models \varphi_2$.

1. Montrez que toute formule peut être transformée en une formule équivalente de formules atomiques de la forme $x = 0$, $x = S(y)$ ou $x + y = z$ (où x, y, z sont des variables) sans aucune quantification universelle. On dit qu'une telle formule est **réduite**.

On encode les entiers naturels en base deux, avec le bit de poids fort sur la droite. On définit une fonction de décodage $\nu : \{0, 1\}^* \rightarrow \mathbb{N}$ par:

$$\nu(\varepsilon) = 0 \quad \nu(0w) = 2\nu(w) \quad \nu(1w) = 1 + 2\nu(w)$$

Cette fonction est surjective mais pas injective. Soit $\mathcal{V} \subseteq \mathcal{X}$ un sous-ensemble de variables. Les valuations $\sigma : \mathcal{V} \rightarrow \mathbb{N}$ sont encodées par des mots sur l'alphabet $\Sigma_{\mathcal{V}} = \{0, 1\}^{\mathcal{V}}$. Si w est un mot sur $\Sigma_{\mathcal{V}}$, on définit w_x comme étant la projection sur son $x^{\text{ème}}$ élément. La fonction ν peut être étendue comme une fonction de $\Sigma_{\mathcal{V}}^*$ vers les valuations sur $\mathcal{V}$ par:

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

Si Φ est une formule et $\mathcal{V}$ contient les variables libres de Φ , on écrit $[\Phi]_{\mathcal{V}} = \{w \in \Sigma_{\mathcal{V}}^* \mid \mathbb{N}, \nu(w) \models \Phi\}$.

2. Montrez que une formule Φ est satisfaite par $\mathbb{N}$ si, et seulement si, $[\Phi]_{\text{fv}(\Phi)} = \Sigma_{\text{fv}(\Phi)}^*$ où $\text{fv}(\Phi)$ est l'ensemble des variables libres de Φ .
3. Montrez que pour toute formule réduite Φ , il existe un automate fini A_{Φ} sur l'alphabet $\Sigma_{\text{fv}(\Phi)}$ qui reconnaît le langage $[\Phi]_{\text{fv}(\Phi)}$.
4. Montrez que l'arithmétique de **Presburger** est décidable. Quelle est la complexité de cette procédure?