

INF412 – PC notée

1 Machines de Turing sur entiers binaires

On considère des machines de Turing sur l'alphabet d'entrée $\Sigma = \{0, 1\}$ et l'alphabet de travail $\Gamma = \Sigma \cup \{B\}$, où B est le symbole de blanc. Le but de cet exercice est d'implémenter des machines de Turing travaillant sur des entiers binaires, codés comme des suites de 0 et de 1. Par exemple l'entier 6 sera codé par le mot 110 (entouré de blancs). On s'efforcera d'expliquer brièvement le fonctionnement des machines de Turing présentées.

Question 1. Construire un machine de Turing permettant de décider si un entier binaire est pair.

Question 2. Construire une machine de Turing qui, étant donné un entier binaire n en entrée, écrit $n - 1$ si $n \neq 0$, ou 0 si $n = 0$.

2 Monoïdes non commutatifs

Un *monoïde* $(M, \times, 1)$ est un ensemble M muni d'une fonction $\times : M^2 \rightarrow M$ (le produit) et d'un élément $1 \in M$ (l'élément neutre) tels que le produit soit associatif et admette 1 comme élément neutre. Par exemple, étant donné un ensemble X , on a le monoïde X^* des mots sur X dont le produit est donné par la concaténation et l'élément neutre par le mot vide.

Question 3. Proposer une signature et une théorie \mathcal{T} sur cette signature dont les modèles égalitaires soient les monoïdes.

Question 4. Montrer que la formule

$$\forall x.(x \times y = y \times x)$$

n'est pas prouvable dans la théorie \mathcal{T} .

3 Principe de Robinson

On rappelle qu'un *corps* $(C, 0, 1, +, \times)$ est un ensemble C muni de deux éléments distingués 0 et 1, et de deux fonctions $+$ et \times d'arité 2 tels que

1. l'addition est associative, commutative et admet 0 comme élément neutre,
2. tout élément admet un opposé,
3. la multiplication est associative et admet 1 comme élément neutre,
4. tout élément non nul est inversible,

5. la multiplication est distributive sur l'addition.

On supposera dans la suite donnée une théorie \mathcal{C} pour les corps (qu'on ne cherchera pas à expliciter). La *caractéristique* d'un corps est le plus petit entier $n \in \mathbb{N}$ tel que

$$\underbrace{1 + 1 + \dots + 1}_{n \text{ éléments}} = 0$$

s'il existe, ou bien 0 si un tel entier n'existe pas.

Question 5. Étant donné $n \in \mathbb{N}$, donner

- une théorie \mathcal{C}_n des « corps de caractéristique zéro ou au moins n »,
- une théorie \mathcal{Z} des « corps de caractéristique (exactement) zéro ».

Question 6. Soient \mathcal{T} et \mathcal{T}' deux théories sur la même signature telles que $\mathcal{T} \subseteq \mathcal{T}'$. Montrer que si \mathcal{T} est inconsistante alors \mathcal{T}' l'est aussi.

Question 7. Soit F une formule satisfaite pour tous les corps de caractéristique 0. Montrer qu'il existe $n \in \mathbb{N}$ tel que la théorie $\mathcal{C}_n \cup \{\neg F\}$ est inconsistante.

Question 8. Montrer le principe de Robinson : si une formule F est satisfaite pour tous les corps de caractéristique 0, alors il existe $n \in \mathbb{N}$ tel que F est satisfaite pour tous les corps de caractéristique k , avec $k \geq n$.

4 Modèles non dénombrables des entiers

Dans cette question, nous allons montrer que la théorie des entiers naturels admet un modèle non dénombrable.

Question 9. Considérons la signature Σ qui ne contient que deux constantes a et b (et pas de symboles de fonctions ni de relations). Montrer que la théorie vide (aucun axiome) sur cette signature admet un modèle à un seul élément.

Question 10. Considérons une signature Σ qui contient un symbole $=$. Comment peut-on s'assurer qu'il existe des modèles dans lesquels ce symbole est interprété par l'égalité (quitte à rajouter des axiomes) ?

Question 11. Donner une signature et une théorie sur cette signature de sorte que tout modèle de celle-ci ait au moins deux éléments.
Même question pour un modèle non dénombrable.

Considérons la signature Σ suivante avec comme

- constantes : $\{c_n \mid n \in \mathbb{N}\}$ (c'est-à-dire qu'on a une constante c_n par entier n),
- symboles de fonctions : $+$ et \times (d'arité 2),
- symboles de relation : $=$ (d'arité 2).

Les termes de cette signature peuvent être interprétés dans le modèle \mathcal{N} avec \mathbb{N} comme ensemble sous-jacent, dans lequel c_n est interprété par n , $+$ par l'addition, \times par la multiplication et $=$ par l'égalité. On note $\text{Th}(\mathbb{N})$ l'ensemble des formules du premier ordre qui sont valides dans ce modèle.

Question 12. En considérant une signature avec un nombre non dénombrable de constantes, montrer que la théorie $\text{Th}(\mathbb{N})$ admet un modèle non dénombrable.

5 Modèles de Kripke

On considère ici les formules de la logique propositionnelle construites à partir d'un ensemble $\text{Var} = \{X, Y, \dots\}$ de variables et des connecteurs \wedge, \vee et \neg . Par une preuve, on entendra ici une preuve dans le système de Frege-Hilbert, dont nous rappelons les axiomes :

$$X \Rightarrow (Y \Rightarrow X) \quad (1)$$

$$(X \Rightarrow (Y \Rightarrow Z)) \Rightarrow ((X \Rightarrow Y) \Rightarrow (X \Rightarrow Z)) \quad (2)$$

$$X \Rightarrow \neg\neg X \quad (3)$$

$$\neg\neg X \Rightarrow X \quad (4)$$

$$(X \Rightarrow Y) \Rightarrow (\neg Y \Rightarrow \neg X) \quad (5)$$

$$X \Rightarrow (Y \Rightarrow (X \wedge Y)) \quad (6)$$

$$(X \wedge Y) \Rightarrow X \quad (7)$$

$$(X \wedge Y) \Rightarrow Y \quad (8)$$

$$X \Rightarrow (X \vee Y) \quad (9)$$

$$Y \Rightarrow (X \vee Y) \quad (10)$$

$$(X \vee Y) \Rightarrow ((X \Rightarrow Z) \Rightarrow ((Y \Rightarrow Z) \Rightarrow Z)) \quad (11)$$

Question 13. Donner une preuve de la formule $\neg X \wedge \neg Y$ dans la théorie $\mathcal{T} = \{\neg(X \vee Y)\}$.

On admettra dans la suite que ce système permet de prouver la formule $X \vee \neg X$, appelée *tiers exclus*. L'objectif de cet exercice est de montrer que si l'on retire le quatrième axiome

$$\neg\neg X \Rightarrow X \quad (4)$$

alors le tiers exclus $X \vee \neg X$ n'est plus prouvable. Une preuve est dite *constructive* si elle n'utilise pas l'axiome ci-dessus et on notera $\mathcal{T} \vdash_c F$ pour dire que F est prouvable de façon constructive dans une théorie \mathcal{T} . La preuve se fera à l'aide d'une famille particulière de modèles (qui sont différents des modèles vus dans ce cours), et ne nécessite pas de théorèmes avancés du cours (complétude, compacité, etc.).

Un *modèle de Kripke* est un triplet $K = (|K|, \leq, \Vdash)$ où

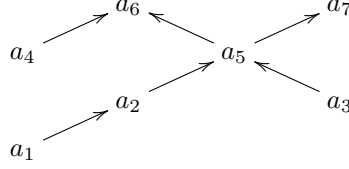
1. $|K|$ est un ensemble,
2. \leq est une relation réflexive et transitive sur $|K|$: pour tous $x, y, z \in |K|$,
 - $x \leq x$ et
 - si $x \leq y$ et $y \leq z$ alors $x \leq z$,
3. $\Vdash \subseteq |K| \times \text{Var}$ est une relation telle que pour tous $a, b \in |K|$ tels que $a \leq b$ et toute variable $X \in \text{Var}$, si $a \Vdash X$ alors $b \Vdash X$.

On étend la relation \Vdash à toutes les formules par induction par

- $a \Vdash F \wedge G$ ssi $a \Vdash F$ et $a \Vdash G$,
- $a \Vdash F \vee G$ ssi $a \Vdash F$ ou $a \Vdash G$,
- $a \Vdash F \Rightarrow G$ ssi pour tout $b \in |K|$ tel que $a \leq b$ et $b \Vdash F$ on a $b \Vdash G$,
- $a \Vdash \neg F$ ssi pour tout $b \in |K|$ tel que $a \leq b$ on a $b \not\Vdash F$ (c'est-à-dire qu'on n'a pas $b \Vdash F$).

On dit que a *force* F lorsque $a \Vdash F$.

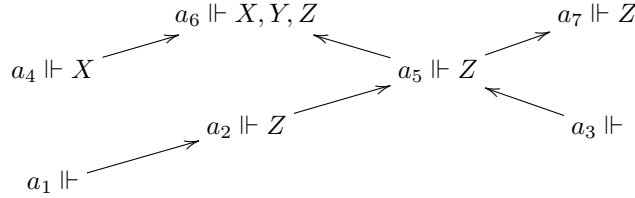
Question 14. On considère le modèle de Kripke suivant :



(on a $a_i \leq a_j$ lorsqu'il existe un chemin de a_i à a_j) avec

$$a_4 \Vdash X \quad a_6 \Vdash X \quad a_6 \Vdash Y \quad a_2 \Vdash Z \quad a_5 \Vdash Z \quad a_6 \Vdash Z \quad a_7 \Vdash Z$$

autrement dit, les variables forcées en chaque point sont



Par quels a_i les trois formules suivantes sont-elles forcées ?

$$X \vee Y \quad \neg X \quad X \Rightarrow Y$$

Dans la suite on supposera fixé un modèle de Kripke K .

Question 15. Montrer que si F est une formule, et $a, b \in |K|$ sont tels que $a \Vdash F$ et $a \leq b$, alors $b \Vdash F$.

Question 16. Étant donné un modèle de Kripke K , montrer que les axiomes (7), (1) et (3) sont forcés par tous les éléments de $|K|$.

Dans la suite, on admettra que tous les axiomes de (1) à (11), excepté (4), sont forcés par tous les éléments d'un modèle de Kripke quelconque. Étant données un théorie \mathcal{T} et une formule F , on notera $\mathcal{T} \Vdash F$ lorsque, pour tout $a \in |K|$, si a force toutes les formules de \mathcal{T} alors a force F .

Question 17. Étant donnée une théorie \mathcal{T} , montrer que $\mathcal{T} \vdash_c F$ alors $\mathcal{T} \Vdash F$.

Question 18. Montrer que les formules $\neg\neg X \Rightarrow X$ (l'axiome (4)) ainsi que $X \vee \neg X$ (le tiers exclus) ne sont pas constructivement prouvables dans la théorie vide. On pourra considérer un modèle de Kripke K avec deux éléments $|K| = \{a, b\}$ tels que $a \leq b$.

Une petite explication sur la constructivité en logique (inutile pour faire le sujet).
Le fait que l'on puisse prouver $X \vee \neg X$ dans le système complet, et donc $F \vee \neg F$ pour toute formule F , permet en pratique de faire des raisonnements qui ne permettent pas de construire des témoins pour les quantifications existentielles : il se peut que l'on prouve $\exists x F$ sans pour autant que l'on sache exhiber un terme t et une preuve de $F[t/x]$. Par exemple, on peut montrer qu'il existe deux irrationnels a et b tels que a^b soit rationnel de la façon suivante.

1. On sait que $\sqrt{2}$ est irrationnel.

2. Le réel $c = \sqrt{2}^{\sqrt{2}}$ est soit rationnel, soit irrationnel.
3. Si c est rationnel alors $a = \sqrt{2}$ et $b = \sqrt{2}$ permettent de conclure.
4. Si c est irrationnel alors $a = \sqrt{2}^{\sqrt{2}}$ et $b = \sqrt{2}$ permet de conclure, car dans ce cas $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$.

Dans ce raisonnement, on a utilisé le tiers exclus à l'étape 2. Il n'est pas *constructif*, car il ne permet pas d'exhiber des témoins pour a et b : on sait qu'il en existe mais on ne peut pas les calculer explicitement.