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 $\times : M^2 \to M$ (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.

Démonstration. On propose un signature avec
- symboles de constantes : 1
- symboles de fonctions : $\times$ (d'arité 2)
- symboles de relation : $=$ (d'arité 2)

Les axiomes sont
- $\forall x.1 \times x = x$
- $\forall x.x \times 1 = x$
- $\forall x.\forall y.\forall z.(x \times y) \times z = x \times (y \times z)$ □

Question 4. Montrer que la formule

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

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

Démonstration. Par le théorème de complétude, si la formule est prouvable alors elle est vérifiée dans tout modèle. Or, ce n'est pas le cas pour le monoïde X^* qui n'est pas commutatif dès que X a au moins deux éléments (on a $ab \neq ba$). □

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

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

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 ».

Démonstration. On note F_n la formule $\neg([n] = 0)$, où $[n]$ est une notation pour $1 + \ldots + 1$ (on additionne n copies de 1). On a alors
— $\mathcal{C}_n = \mathcal{T} \cup \{F_k \mid 0 \leq k < n\}$
— $\mathcal{Z} = \mathcal{T} \cup \{F_k \mid k \in \mathbb{N}\}$ □

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.

Démonstration. Si $\mathcal{T}$ est inconsistante, il n'existe pas de modèle dans laquelle toute ses formules sont satisfaites. Donc il n'existe pas non plus de modèle dans lequel toutes les formules de $\mathcal{T}'$ soient satisfaites, sinon celui-ci serait aussi un modèle de $\mathcal{T}$. □

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.

Démonstration. La contraposée du théorème de compacité dit qu'une théorie inconsistante admet un sous-ensemble fini de formules qui soit aussi inconsistant. Comme F est satisfaite pour tous les corps de caractéristique 0, $\mathcal{Z} \cup \{\neg F\}$ est inconsistante (sinon on aurait un modèle, qui est un corps de caractéristique 0, qui ne satisfait pas F). Il admet un sous-ensemble fini $\mathcal{T} \subseteq \mathcal{Z}$ inconsistant. Celui-ci ne contient qu'un nombre fini de formules F_k dont en notant n le max de ces indices plus 1 on a $\mathcal{T} \subseteq \mathcal{C}_n \cup \{\neg F\}$. Et $\mathcal{C}_n \cup \{\neg F\}$ est inconsistant par la question précédente. □

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 $k \geq n$.

Démonstration. On note n l'entier associé à F par la question précédente. Un corps K de caractéristique au moins n est un modèle de $\mathcal{C}_n$, et n'est pas un modèle de $\mathcal{C}_n \cup \neg F$ (qui n'est pas satisfiable par la question précédente). Donc K ne satisfait pas $\neg F$, donc K satisfait F. □

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.

Démonstration. Notons $\{*\}$ l'ensemble à un élément. La fonction qui interprète a et b par $*$ convient puisqu'il n'y a pas d'axiome à vérifier. □

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) ?

Démonstration. Par un théorème du cours (Proposition 6.1), si l'on ajoute les axiomes exprimant la réflexivité, la symétrie et la transitivité de l'égalité, ainsi que le fait qu'elle est une congruence vis-à-vis de tout symbole de fonction ou de relation, la théorie résultante admet un modèle si et seulement si elle admet un modèle égalitaire. □

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.

Démonstration. Construisons ces théories.

- On considère la signature $\Sigma = (\{a, b\}, \emptyset, \{=\})$ avec les axiomes de l'égalité ainsi que $\neg(a = b)$. Le modèle, qui peut être supposé égalitaire, a au moins deux éléments puisque les interprétations de a et b sont différentes par l'axiome.
- On prend comme signature $\Sigma = (\{c_x \mid x \in \mathbb{R}\}, \emptyset, \{=\})$. Les axiomes sont ceux de l'égalité ainsi que les formules de la forme $\neg(c_x = c_y)$ pour $x, y \in \mathbb{R}$ avec $x \neq y$. On a au moins autant d'éléments dans le modèle que dans $\mathbb{R}$ (on a une injection de $\mathbb{R}$ dans le modèle) donc celui-ci n'est pas 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 $\mathrm{Th}(\mathbb{N})$ 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 $\mathrm{Th}(\mathbb{N})$ admet un modèle non dénombrable.

Démonstration. On considère la signature Σ' obtenue à partir de Σ en rajoutant des symboles de constantes d_x indexées par $x \in \mathbb{R}$. On considère la théorie $\mathcal{T}$ obtenue à partir de $\mathrm{Th}(\mathbb{N})$ en ajoutant $\neg(d_x = d_y)$ pour $x, y \in \mathbb{R}$ avec $x \neq y$.

Montrons que la théorie $\mathcal{T}$ est finiment satisfiable. Soit $\mathcal{T}' \subseteq \mathcal{T}$ un sous-ensemble fini. Les formules de $\mathcal{T}'$ font intervenir un nombre fini de c_n (indexées par $n \in C \subseteq \mathbb{N}$) et un nombre fini de d_x (indexées par $x \in D \subseteq \mathbb{R}$). Pour $n \in C$ on interprète c_n par n, et pour $x \in D$ on interprète d_x par un entier quelconque qui ne soit pas dans C de sorte que les interprétations de deux constantes distinctes soient distinctes (ce que l'on peut faire car C et D sont finis). Une formule de $\mathcal{T}'$ est soit une formule de $\mathrm{Th}(\mathbb{N})$ qui est satisfaite car $\mathcal{N}$ est un modèle de $\mathrm{Th}(\mathbb{N})$, soit $\neg(x = y)$ qui est satisfaite par construction. Donc on a un modèle de $\mathcal{T}'$. Par compacité $\mathcal{T}$ est satisfiable, et ce modèle contient un nombre non-dénombrable d'éléments par un raisonnement analogue à la question précédente. □

5 Modèles de Kripke

On considère ici les formules de la logique propositionnelle construites à partir d'un ensemble $\mathrm{Var} = \{X, Y, \ldots\}$ 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 :

$$X \Rightarrow (Y \Rightarrow X) \tag{1}$$
$$(X \Rightarrow (Y \Rightarrow Z)) \Rightarrow ((X \Rightarrow Y) \Rightarrow (X \Rightarrow Z)) \tag{2}$$
$$X \Rightarrow \neg\neg X \tag{3}$$
$$\neg\neg X \Rightarrow X \tag{4}$$
$$(X \Rightarrow Y) \Rightarrow (\neg Y \Rightarrow \neg X) \tag{5}$$
$$X \Rightarrow (Y \Rightarrow (X \wedge Y)) \tag{6}$$
$$(X \wedge Y) \Rightarrow X \tag{7}$$
$$(X \wedge Y) \Rightarrow Y \tag{8}$$
$$X \Rightarrow (X \vee Y) \tag{9}$$
$$Y \Rightarrow (X \vee Y) \tag{10}$$
$$(X \vee Y) \Rightarrow ((X \Rightarrow Z) \Rightarrow ((Y \Rightarrow Z) \Rightarrow Z)) \tag{11}$$

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

Démonstration. On a :

$\neg(X \vee Y)$	
$X \Rightarrow X \vee Y$	axiome (8)
$\neg(X \vee Y) \Rightarrow \neg X$	coupure avec (5)
$\neg X$	coupure avec l'axiome de $\mathcal{T}$
$Y \Rightarrow X \vee Y$	axiome (9)
$\neg(X \vee Y) \Rightarrow \neg Y$	coupure avec (5)
$\neg Y$	coupure avec l'axiome de $\mathcal{T}$
$\neg Y \Rightarrow \neg X \wedge \neg Y$	coupure avec (6)
$\neg X \wedge \neg Y$	coupure

□

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

$$\neg\neg X \Rightarrow X \tag{4}$$

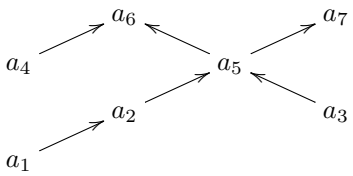
alors le tiers exclus $X \vee \neg X$ n'est plus prouvable. Une preuve est dite *constructive* si elle n'utilise pas l'axiome ci-dessus et on notera $\mathcal{T} \vdash_{\mathrm{c}} F$ pour dire que F est prouvable de façon constructive dans une théorie $\mathcal{T}$. La preuve se fera à l'aide d'une 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. $\Vdash \subseteq |K| \times \mathrm{Var}$ est une relation telle que pour tous $a, b \in |K|$ tels que $a \leq b$ et toute variable $X \in \mathrm{Var}$, 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 $a \Vdash F$.

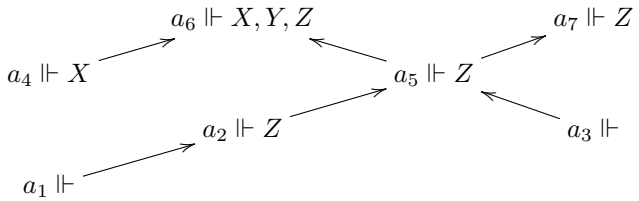
Question 14. On considère le modèle de Kripke suivant :



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

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

autrement dit, les variables forcés en chaque point sont



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

$$X \vee Y \qquad\qquad \neg X \qquad\qquad X \Rightarrow Y$$

Démonstration. Éléments forçant les formules :

$$\begin{aligned} X \vee Y &= \{a_4, a_6\} \\ \neg X &= \{a_7\} \\ X \Rightarrow Y &= \{a_1, a_2, a_3, a_5, a_6, a_7\} \end{aligned}$$

□

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 $b \Vdash F$.

Démonstration. Par induction sur 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 $|K|$.

Démonstration.

- Soit $a \in |K|$. On a, pour tout $b \geq a$ tel que $b \Vdash X \wedge Y$, $b \Vdash X$. Donc $a \Vdash X \wedge Y \Rightarrow X$.
- Soit $a \in |K|$. On a les équivalences suivantes :
  - $a \Vdash X \Rightarrow (Y \Rightarrow X)$
  - pour tout $b \geq a$, $b \Vdash X$ implique $b \Vdash Y \Rightarrow X$
  - pour tout $b \geq a$, $b \Vdash X$ implique pour tout $c \geq b$, $c \Vdash Y$ implique $c \vdash X$

  la dernière est vraie car $c \geq b$ et $b \Vdash X$ donc $c \Vdash X$ par la question précédente.
- Soit $a \in |K|$. On a les équivalences suivantes :
  - $a \Vdash \neg\neg X$
  - pour tout $b \geq a$, $b \nVdash \neg X$
  - pour tout $b \geq a$, non (pour tout $c \geq b$, $c \nVdash X$)
  - pour tout $b \geq a$, il existe $c \geq b$ tel que $c \Vdash X$

  Montrons $a \Vdash X \Rightarrow \neg\neg X$. Soit $b \geq a$ tel que $b \Vdash X$ alors $b \Vdash X$ et $b \geq b$ donc il $b \vdash \neg\neg X$. □

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 $\mathcal{T} \Vdash F$.

Démonstration. Par hypothèse, les axiomes sont vérifiés. Il ne reste plus qu'à montrer que si $a \Vdash F \Rightarrow G$ et $a \Vdash F$ alors $a \Vdash G$ (modus ponens), ce qui est vrai par définition de l'interprétation de l'implication. □

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 $a \leq b$.

Démonstration. Pour montrer que $X \vee \neg X$ n'est pas dérivable, il suffit de montrer qu'il existe un modèle tel que l'on n'ait pas $\Vdash X \vee \neg X$. Prenons K avec $|K| = \{a, b\}$, $a \leq b$, et $b \Vdash X$:

$$\begin{array}{c} b \Vdash \{X\} \\ \uparrow \\ a \Vdash \emptyset \end{array}$$

On a $a \Vdash \neg\neg X$ (puisque pour $a' \geq a$ il existe $b \geq a'$ avec $b \Vdash X$), mais $a \nVdash X$, donc $a \nVdash \neg\neg X \Rightarrow X$. De plus $a \nVdash X$ et $a \nVdash \neg X$ donc $a \nVdash X \vee \neg X$. □

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.