École polytechnique — X2022 — INF412 Fondements de l'informatique

Logique du premier ordre

(corrigé)

1 Le corps des réels

Le corps $\mathbb{R}$ des réels vérifie les propriétés suivantes :

1. c'est un groupe additif (on appelle 0 son neutre),
2. ...un anneau (on appelle 1 son neutre multiplicatif, on note 2 pour 1+1, etc.),
3. ...un corps,
4. ...muni d'une relation d'ordre total compatible avec les opérations arithmétiques,
5. tout élément positif est un carré,
6. tout polynôme de degré impair a une variable à au moins un zéro.

Question 1.1. *Proposez une signature et, sur le modèle des axiomes présentés en cours pour les propriétés 1 à 3, proposez 6 axiomes permettant d'exprimer la propriété 4. Proposez un axiome permettant d'exprimer la propriété 5.*

Solution : Pour la signature, on prend celle du cours à laquelle on ajoute une relation binaire $\leq$: la signature est donc $(\{0, 1\}, \{+, \times\}, \{=, \leq\})$. Les axiomes pour la relation d'ordre total sont

— $\leq$ est réflexive : $\forall x\ x \leq x$;
— $\leq$ est transitive : $\forall x \forall y \forall z\ x \leq y \wedge y \leq z \Rightarrow x \leq z$;
— $\leq$ est antisymétrique : $\forall x \forall y\ x \leq y \wedge y \leq x \Rightarrow x = y$;
— $\leq$ est totale : $\forall x \forall y\ x \leq y \vee y \leq x$;
— $\leq$ est compatible avec l'addition : $\forall x \forall x' \forall y\ x \leq x' \Rightarrow x + y \leq x' + y$;
— $\leq$ est compatible avec la multiplication : $\forall x \forall x' \forall y\ y \geq 0 \wedge x \leq x' \Rightarrow x \times y \leq x' \times y$.

Ensuite, tout élément positif est un carré s'exprime par l'axiome : $\forall x\ 0 \leq x \Rightarrow \exists y\ x = y \times y$.

□

Question 1.2. *Exprimez la propriété 6 par un ensemble d'axiomes (potentiellement infini).*

Solution : Pour chaque $n \in \mathbb{N}$ on prend l'axiome

$$\forall a_0, \ldots, a_{2n+1} \qquad a_{2n+1} \neq 0 \implies \exists x \sum_{i=0}^{2n+1} a_i x^i = 0$$

□

On obtient ainsi une axiomatisation des *corps réels clos*. Mais le corps des réels n'est pas le seul qui vérifie les axiomes que nous avons écrits ! On appelle *réels algébriques* l'ensemble des réels x tels qu'il existe un polynôme P à coefficients entiers tel que $P(x) = 0$. Nous admettrons qu'ils forment un sous-corps de $\mathbb{R}$ (ce n'est pas très difficile à prouver mais cela nous entraînerait hors sujet), dénombrable, et que ce sous-corps est un corps réel clos. Pour garantir d'avoir tous les réels et non seulement les algébriques, on voudrait compléter le système d'axiomes. L'un des axiomes classiques des réels indique le caractère complet pour la topologie (« les suites de Cauchy convergent ») et peut s'exprimer ainsi (les ensembles bornés supérieurement ont un supremum) :

$$\begin{aligned}\forall X \subseteq \mathbb{R}(X \neq \emptyset \wedge (\exists b \in \mathbb{R}, \forall x \in X, x \leq b) \Rightarrow \\ \exists t \in \mathbb{R}((\forall x \in X, x \leq t) \wedge (\forall b \in \mathbb{R},\ (\forall x \in X, x \leq b) \Rightarrow t \leq b))).\end{aligned} \quad (1)$$

Question 1.3. *Cette formule est-elle du premier ordre sur la signature* $(\{0,1\},\{+,\times\},\{=,\leq\})$ *?*

Solution : Elle ne l'est pas puisque la quantification $\forall X \subseteq \mathbb{R}$ porte sur un sous-ensemble et non pas sur un élément et qu'on utilise $\in$, qui n'est pas dans la signature. □

En réalité, une telle axiomatisation des réels est vouée à l'échec. Nous allons tout d'abord montrer ce résultat dans le cas où la signature est dénombrable.

Question 1.4. *Montrer qu'il n'existe pas d'axiomatisation, par des formules du premier ordre sur une signature dénombrable, dont le seul modèle est le corps des réels. On pourra utiliser le théorème de Löwenheim-Skolem.*

Solution : Par le théorème de Löwenheim-Skolem, une telle axiomatisation devrait avoir un modèle dénombrable, et comme le corps des réels n'est pas dénombrable, elle doit donc avoir au moins deux modèles distincts ! □

Question 1.5. *Montrer que la conclusion du théorème de Löwenheim-Skolem est fausse si l'on ne suppose pas la signature dénombrable.*

Solution : Nous devons exhiber une théorie, dont la signature n'est pas dénombrable, qui n'admette pas de modèle dénombrable. On peut par exemple prendre la théorie qui admet une constante c_x pour tout réel $x \in \mathbb{R}$ et un axiome $\neg(c_x = c_y)$ pour tous réels distincts x et y (attention, sans ces axiomes, on pourrait par exemple avoir le modèle réduit à un élément, où toutes les constantes sont interprétées de la même façon). □

2 Corps archimédiens

L'une des propriétés qui caractérise le corps des réels est son caractère *archimédien* :

$$\forall x \exists n, n \in \mathbb{N} \wedge x < n,$$

Question 2.1. *Justifiez pourquoi cette formule n'est pas du premier ordre sur la signature que l'on s'est fixée.*

Solution : La sous-formule $n \in \mathbb{N}$ utilise les symboles $\in$ et $\mathbb{N}$ qui ne sont pas dans la signature. On peut bien sûr chercher à définir dans notre signature le fait d'être un entier. Mais c'est en fait impossible dans la syntaxe de la logique du premier ordre, et c'est ce que prouve la suite de l'exercice. □

On pourrait être tenté de définir un prédicat unaire (appelons-le `entier`), pour exprimer le fait qu'un réel est un entier. La formule précédente deviendrait donc

$$\forall x \exists n, \texttt{entier}(n) \wedge x < n,$$

ce qui est bien dans notre nouvelle signature.

Question 2.2. *Proposez des axiomes pour* `entier`*. Soit* $\mathfrak{M}_{\mathbb{R}}^{\mathbb{N}}$ *un modèle de cette théorie construit à partir de* $\mathfrak{M}_{\mathbb{R}}$ *qui interprète* `entier` *par* $E \subseteq \mathbb{R}$*, montrez que nécessairement* $E = \mathbb{N}$*.*

Solution : On ajoute les axiomes

$$\texttt{entier}(0), \qquad \forall x\ \texttt{entier}(x) \Rightarrow \texttt{entier}(x+1),$$

$$\forall x\ \texttt{entier}(x) \Rightarrow x = 0 \vee \exists y\ x = y + 1 \wedge \texttt{entier}(y),$$

$$\forall x\ [x < 0 \vee (0 < x \wedge x < 1)] \Rightarrow \neg\texttt{entier}(x).$$

On vérifie aisément que pour toute interprétation E de `entier`, on a $\mathbb{N} \subseteq E$ par induction par les deux premiers axiomes. On observe ensuite que $\{x \mid x < 0 \vee x \in (0,1)\} \cap E = \emptyset$ par le dernier axiome. Pour terminer la preuve il suffit de montrer que E ne contient aucun réel positif $x > 1$ qui n'est pas un entier, ce qui s'établit par récurrence sur la partie entière $\lfloor x \rfloor$ de x en employant le troisième axiome. $\square$

Question 2.3. *À votre avis, le corps des réels est-il le seul modèle ?*

Solution : L'argument précédent fondé sur le théorème de Löwenheim-Skolem fonctionne encore.

On peut aussi construire un modèle non-standard (voir la partie suivante). Pour tout modèle $\mathfrak{M}$, on a toujours que $\mathfrak{M} \models \texttt{entier}(n)$ pour tout $n \in \mathbb{N}$. Par ailleurs, pour tout $n \in \mathbb{N}$ on a $\mathfrak{M} \models \forall x\ n < x \wedge x < n+1 \Rightarrow \neg\texttt{entier}(x)$. Toutefois un modèle non-standard peut contenir des éléments x « non-standards » qui ne sont ni entiers, ni compris entre deux entiers (en effet cela revient à avoir la propriété d'être archimédien). Il existe donc des « entiers non-standards » et des « non-entiers non-standards ». $\square$

3 L'impossible caractérisation des réels au premier order

Nous allons maintenant montrer que, même avec une signature non-dénombrable, le résultat persiste. L'objectif de cet exercice est de montrer le résultat suivant :

Théorème. *Il n'existe pas d'ensemble d'axiomes du premier ordre caractérisant le corps des réels à isomorphisme près.*

Supposons donc par l'absurde qu'il existe une telle axiomatisation du corps des réels ordonné, c'est-à-dire une signature $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$ avec $\{0,1\} \subseteq \mathcal{C}$, $\{+,\cdot\} \subseteq \mathcal{F}$ et $\{=,<\} \subseteq \mathcal{R}$, ainsi qu'un ensemble d'axiomes $\mathcal{A}$ sur Σ qui caractérise $\mathbb{R}$ à isomorphisme près. Plus précisément, $\mathbb{R}$ est l'ensemble de base d'une structure $\mathfrak{M}_{\mathbb{R}}$ sur Σ, qui interprète $0, 1, +, \cdot, =, <$ de manière standard et qui satisfait $\mathcal{A}$, et toute autre structure sur Σ qui satisfait $\mathcal{A}$ est isomorphe à $\mathfrak{M}_{\mathbb{R}}$.

Question 3.1. *Donnez une théorie $\mathcal{A}^+$ qui contienne $\mathcal{A}$ (on s'autorisera à étendre la signature, mais pas à utiliser* `entier`*) et dont les modèles sont des corps réels ordonnés qui ne sont pas archimédiens.*

Solution : On considère l'extension Σ^+ de Σ où l'on rajoute simplement une constante supplémentaire c, et on définit la théorie $\mathcal{A}^+$ comme $\mathcal{A} \cup \{\overline{n} < c \mid n \in \mathbb{N}\}$ où $\overline{n}$ est le terme $\underbrace{((1+1)+\cdots+1)}_{n \text{ fois}}$. $\square$

Question 3.2. *Montrez que $\mathcal{A}^+$ possède un modèle ${}^\star\mathfrak{M}_{\mathbb{R}}$. [Indication : utiliser le théorème de compacité, qui est vrai pour toute signature, dénombrable ou pas.]*

Solution : Toute partie finie de cette théorie ne fait intervenir qu'un nombre fini d'axiomes de la forme $\overline{n} < c$. Il suffit alors de choisir un réel r_∞ plus grand que tous les entiers n correspondants, et l'extension de $\mathfrak{M}_{\mathbb{R}}$ qui interprète c par r_∞ fournit un modèle de cette partie. Ainsi, pour chaque partie finie de la théorie, on trouve un modèle dont le domaine est $\mathbb{R}$, et ceci prouve l'existence d'un modèle de $\mathcal{A}^+$, sans rien dire sur son domaine. $\square$

Question 3.3. *Déduisez-en le Théorème.*

Solution : Le raisonnement est le même que pour les entiers non-standards. Le modèle ${}^\star\mathfrak{M}_{\mathbb{R}}$ est un modèle de $\mathcal{A}^+$, et donc en particulier de $\mathcal{A}$. Il contient un élément qui est plus grand que tous les entiers. Il n'est donc pas archimédien et ne peut donc pas être isomorphe à $\mathbb{R}$: un tel isomorphisme doit envoyer c sur un réel, qui est dominé par un entier, en contradiction avec les relations d'ordre que l'isomorphisme doit transporter. □

Question 3.4. *Proposez une construction explicite d'un corps réel ordonné, qui contienne $\mathbb{R}$ et qui ne soit pas archimédien. [Précision : on n'impose pas que ce corps soit clos, comme l'est $\mathbb{R}$.]*

Solution : Comme on veut que ce corps ne soit pas archimédien, on est amené à supposer l'existence d'un élément c du modèle qui est plus grand que tous les entiers. On veut de plus que ce modèle contienne $\mathbb{R}$ et soit clos par les opérations d'addition, multiplication, division, etc., ce qui suggère de considérer le corps $\mathbb{R}(c)$ des fractions rationnelles à coefficients réels, en une variable c. Pour la relation d'ordre, on utilise le comportement asymptotique des fractions. Plus précisément, si $f \in \mathbb{R}(c)$, alors il existe deux polynômes P et Q avec Q unitaire tels que $f = P/Q$, $P = p_0 c^k + p_1 c^{k-1} + \cdots + p_k$ avec $p_0 \neq 0$ sauf si $f = P = 0$. On dira alors que $f \geq 0$ lorsque $p_0 \geq 0$. Il est facile de voir que la relation ainsi définie vérifie les axiomes des relations d'ordre, et est compatible avec les opérations de corps. Muni de cet ordre, le corps $\mathbb{R}(c)$ n'est pas archimédien, puisque pour tout $n \in \mathbb{N}$, le polynôme $c - n = (c - n)/1$ est plus grand que 0 puisque son coefficient de tête est 1. □