École polytechnique — X2013 — INF412 Fondements de l'informatique

Logique du premier ordre

Sujet proposé par David Monniaux
(corrigé)

1 Le corps des réels

On s'intéresse ici à la structure $\mathbb{R} = \langle \mathbb{R}, +, \cdot, <, 0, 1 \rangle$, le corps ordonné des réels. La construction habituelle de $\mathbb{R}$ passe par un certain nombre d'axiomes qui caractérisent $\mathbb{R}$ à isomorphisme près. L'objectif de cet exercice est de montrer le résultat suivant.

Théorème 1. *Il n'existe pas d'ensemble d'axiomes du premier ordre, sur une signature dénombrable, caractérisant $\mathbb{R}$ à isomorphisme près.*

Pour prouver ce résultat, on fera appel au théorème de Löwenheim-Skolem, vu en cours.

Question 1.1. *Prouver le théorème 1 à l'aide du théorème de Löwenheim-Skolem.*

Solution : La signature est bien dénombrable, il existe donc un modèle dénombrable, qui ne peut donc être isomorphe à $\mathbb{R}$. □

Même avec une signature non-dénombrable, le résultat du théorème 1 persiste : on considère maintenant la structure $\langle \mathbb{R}, +, \cdot, <, r_{r \in \mathbb{R}} \rangle$ avec un symbole de constante r différent par nombre réel. Une des propriétés de $\mathbb{R}$ est son caractère *archimédien* :

$$\forall x \exists n, x < n,$$

où n est le terme $((1 + 1) + \cdots + 1)$ n fois.

Question 1.2. *Justifier pourquoi cette formule n'est pas du premier ordre sur la signature que l'on s'est fixée.*

Solution : Le quantificateur existentiel porte sur une variable n qui est contrainte à être un entier et non un élément quelconque du domaine $\mathbb{R}$. □

On introduit un nouveau symbole de constante c. Nous prendrons comme axiomes l'ensemble des formules du premier ordre vraies sur $\mathbb{R}$, et les formules $c > r$ pour tous les réels r.

Question 1.3. *Montrer que la théorie ainsi formée possède un modèle ${}^\star\mathbb{R}$. [Indication : utiliser le théorème de compacité.]*

Solution : Toute partie finie de cette théorie ne fait intervenir qu'un nombre fini de symboles de constantes r. Il suffit alors d'interpréter c comme 1 plus le plus grand de ces réels, et $\mathbb{R}$ fournit un modèle de cette partie. □

Question 1.4. *Conclure que ${}^\star\mathbb{R}$ est un modèle non-archimédien des formules du premier ordre vraies sur $\mathbb{R}$ qui n'est donc pas isomorphe à $\mathbb{R}$.*

Solution : Le raisonnement est le même que pour les entiers non-standards. Le modèle est bien un modèle des axiomes de corps ordonné, et il contient un élément qui est plus grand que tous les réels, donc que tout n. Il n'est donc pas archimédien et ne peut donc pas être isomorphe à $\mathbb{R}$. □

Question 1.5. *Proposez une construction explicite d'un tel corps.*

Solution : On peut prendre le corps des fractions rationnelles en une variable c, ordonnées par leur comportement asymptotique (c'est-à-dire que l'ordre est donné par le signe du premier coefficient non nul du développement asymptotique de la différence).

On peut aussi, plus algébriquement, prendre le corps des séries de Laurent formelles sur $\mathbb{R}$ avec X comme indéterminée, considérées comme des suites $(a_k)_{k\in\mathbb{Z}}$ de réels indexées par les entiers relatifs telles qu'il existe k_0 tel que $\forall k < k_0 \mid a_k = 0$ (l'addition est l'addition terme à terme, la multiplication est définie par $(a \cdot b)_k = \sum_{\alpha+\beta=k} a_\alpha b_\beta$, qui est en fait une somme finie). Il faut alors interpréter c par X^{-1}. □

La section suivante est longue, il est donc probable que nous n'arriverons pas au bout.

---

2 Théorème de complétude

Nous nous proposons ici de démontrer le théorème de complétude de la logique du premier ordre par construction d'un modèle de Herbrand. Le résultat final auquel nous arriverons est :

Théorème 2. *Tout système d'axiomes (formules closes) sur une signature au plus dénombrable soit permet d'obtenir une contradiction (une preuve de « faux »), soit admet des modèles, dont certains sont au plus dénombrables.*

En fait, nous prouverons même au passage la version du théorème de Löwenheim-Skolem utilisée dans la partie 1 et le théorème de compacité de la logique du premier ordre ! Bien entendu, l'utilisation de ces théorèmes est donc interdite dans cet exercice, mais on pourra faire appel à leur analogue du calcul propositionnel.

Quelques points de vocabulaire et de notations :

- Au plus dénombrable = fini ou dénombrable.
- Preuve de l'absurde : preuve de la formule « faux », notée $\bot$, qui a valeur de vérité 0 pour toute valuation.
- Nous notons $F[t/x]$ (resp. $\tau[t/x]$) la formule (resp. le terme) où la variable libre x est remplacée par le terme t, avec les précautions usuelles pour éviter les captures de variables (renommage des variables quantifiées).

Pour prouver que le système d'axiomes peut permettre d'obtenir une preuve de l'absurde, il faut spécifier un système de preuve. Sans le préciser complètement, nous supposerons qu'il vérifie les propriétés usuelles, dont :

Complétude Si $F_1, \dots, F_n, G$ sont des formules *propositionnelles* et que toute valuation des variables propositionnelles qui satisfait $F_1, \dots, F_n$ satisfait G, alors $F_1, \dots, F_n \vdash G$ (« le système de preuve permet de déduire G à partir de $F_1, \dots, F_n$ »).

Spécialisation De toute formule quantifiée universellement $\forall x\ F$ on peut déduire $F[t/x]$ où t est un terme quelconque.

Modus ponens Si $F_1, \dots, F_n \vdash G$ et $F_1, \dots, F_n, G \vdash H$, alors $F_1, \dots, F_n \vdash H$.

Pour fixer les idées, on pourra par exemple prendre le système de Frege-Hilbert, qui vérifie ces propriétés.

2.1 Lemmes sur des formules propositionnelles

Avant de nous attaquer à la logique du premier ordre, nous avons besoin de lemmes sur des formules propositionnelles.

Question 2.1. *Démontrez qu'un ensemble E fini de formules* propositionnelles *sur un ensemble fini de variables qui n'admet pas de modèle permet une preuve de l'absurde.*

Solution : C'est une application directe de la complétude du système de preuve. Cette propriété peut se récrire ainsi : si

$$\{v \text{ valuation} \mid v(F_1) = \cdots = v(F_n) = 1\} \subset \{v \text{ valuation} \mid v(G) = 1\}$$

alors $F_1, \ldots, F_n \vdash G$.

Dans cette question, E est l'ensemble des F_i et l'inclusion ci-dessus devient $\emptyset \subset \emptyset$ qui est vraie, d'où le résultat $E \vdash \bot$. □

Question 2.2. *Même question si E est infini.*

Solution : Le plus simple est d'utiliser le théorème de compacité du calcul propositionnel. Si E n'admet pas de modèle, c'est qu'une de ses parties finies n'en admet pas, et alors la question précédente conclut.

On peut aussi prouver le résultat directement. Soient $v_1, \ldots, v_n$ les variables propositionnelles. Chaque formule $\phi \in E$ se traduit en une fonction $[\![\phi]\!] : \{0,1\}^n \to \{0,1\}$; deux formules sont équivalentes si elles induisent la même fonction. La conjonction de toutes les formules de E est équivalente à la conjonction d'une formule par classe d'équivalence, qui sont en nombre fini $F_1 \wedge \cdots \wedge F_m$ (on utilise ici l'axiome du choix). Soit on a un modèle de $F_1, \ldots, F_m$, soit il n'y en a pas et donc tout modèle de ces formules satisfait la formule « faux ». Alors, par l'hypothèse de l'énoncé sur le système de preuve, on peut démontrer « faux » à partir de $\{F_1, \ldots, F_m\}$ et donc a fortiori à partir de E. □

Question 2.3. *Démontrez qu'un ensemble E (éventuellement infini) de formules propositionnelles sur un ensemble au plus dénombrable de variables soit est inconsistant (et alors il existe une preuve de l'absurde à partir de ces formules), soit admet un modèle.*

Indice : On ne s'occupera que du cas où l'ensemble de variables est dénombrable, le cas fini ayant été traité à la question précédente. On note E_n l'ensemble des formules de E ne portant que sur les variables $v_1, \ldots, v_n$.

On construit un arbre binaire A des choix successifs de $v_1, v_2, \ldots$, dont chaque nœud de profondeur p est donc associé à un chemin d'accès correspondant aux choix de $v_1, \ldots, v_{p-1}$, la profondeur de la racine étant de 1 (et son chemin d'accès est donc le mot vide) :

- les nœuds internes sont étiquetés par v_k où k est la profondeur dans l'arbre, et leurs arêtes sortantes sont étiquetées par 0 et 1 (signifiant respectivement que le sous-arbre sur lequel l'arête pointe décrit le cas où $v_k = 0$ ou $v_k = 1$) ;
- on met une feuille STOP à la position étiquetée par le chemin d'accès $b_1, \ldots, b_n$ dès que l'ensemble de formules $E_n[b_1, \ldots, b_n/v_1, \ldots, v_n]$ devient inconsistant.

Toute branche de l'arbre est donc soit infinie, soit terminée par une feuille STOP. Nous vous rappelons d'ailleurs le lemme de Koenig : un arbre binaire est infini si et seulement si il a une branche infinie.

Solution : La solution par compacité de la question précédente répond aussi à celle-ci.

Sinon, l'indice suggère de procéder comme suit. Soit A est fini, soit il a une branche infinie, d'après le lemme de Koenig. Si A est fini, cela veut dire qu'à une certaine profondeur p, on a obtenu des feuilles STOP dans toutes les branches, donc que E_p n'a pas de solution quelles que

soient les valeurs de $v_1, \ldots, v_p$, autrement dit que E_p est inconsistant. On conclut par la question précédente.

Si A est infini, alors il a (au moins) une branche infinie, étiquetée par les choix $b_1, b_2, \ldots$. Montrons que $\mathcal{M} : v_1 \mapsto b_1, v_2 \mapsto b_2, \ldots$ est un modèle de E. Si ce n'est pas un modèle, c'est qu'il y a une formule $\phi \in E$ telle que $\mathcal{M} \not\models \phi$. Cette formule ϕ ne met en jeu qu'un nombre fini de variables propositionnelles, donc elle appartient à un certain E_p ; mais alors, on aurait dû couper cette branche à une profondeur au plus p — contradiction, donc $\mathcal{M} \models E$. □

2.2 Retour au premier ordre

Nous considérons un système d'axiomes sur une signature comportant un ensemble au plus dénombrable de symboles de fonctions et un ensemble au plus dénombrable de relations. On rappelle que toute formule est équivalente à une formule en forme prénexe (voir le poly §5.4.2).

Question 2.4. *Montrez qu'on peut se ramener au cas d'un système d'axiomes de la forme $\forall x_1 \ldots \forall x_n\ F$ où F est sans quantificateurs, quitte à rajouter des symboles de fonction.*

Solution : On met les axiomes sous forme prénexe (on déplace les quantificateurs en tête de formule, quitte à renommer des variables) et on skolémise : on transforme chaque variable existentiellement quantifiée en une fonction des variables introduites par des quantificateurs universels précédant le quantificateur existentiel.

Par exemple : $\forall x \forall \alpha \exists \eta\ (|x - y| < \eta \Rightarrow |f(x) - f(y)| < \alpha)$ se traduit en $\forall x \forall \alpha\ (|x - y| < \eta(x, \alpha) \Rightarrow |f(x) - f(y)| < \alpha)$. □

On considère souvent des théories « égalitaires », comprenant une relation d'égalité dont on impose que l'interprétation soit l'égalité dans les modèles. Ceci va nous gêner.

Question 2.5. *Montrez qu'on peut remplacer dans la théorie $\mathcal{T}$ la relation d'égalité par une relation binaire supplémentaire $\sim$, des axiomes faisant de $\sim$ une relation d'équivalence, et des axiomes supplémentaires, obtenant ainsi une nouvelle théorie $\mathcal{T}'$, de façon à ce que tout modèle de $\mathcal{T}$ soit un modèle de $\mathcal{T}'$ et que tout modèle de $\mathcal{T}'$ puisse être transformé en un modèle de $\mathcal{T}$.*

Solution : On introduit une relation $\sim$, des axiomes de réflexivité, transitivité, et symétrie, et des axiomes de congruence par rapport à toutes les autres relations et symboles de fonction, c'est-à-dire que pour chaque symbole n-aire de fonction f dans la signature, on introduit l'axiome

$$\forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n\ x_1 \sim y_1 \wedge \cdots \wedge x_n \sim y_n \implies f(x_1, \ldots, x_n) \sim f(y_1, \ldots, y_n) \qquad (1)$$

et pour chaque relation n-aire P

$$\forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n\ x_1 \sim y_1 \wedge \cdots \wedge x_n \sim y_n \implies (P(x_1, \ldots, x_n) \Leftrightarrow P(y_1, \ldots, y_n)). \qquad (2)$$

Pour tout modèle de ce nouveau système, on obtient un modèle de l'ancien système en quotientant par l'interprétation de $\sim$ (c'est-à-dire en considérant les classes d'équivalence) ; réciproquement tout modèle de l'ancien système est un modèle du nouveau en interprétant $\sim$ par l'égalité.

□

Nous en arrivons à prouver le théorème de complétude pour la signature Σ et les axiomes $\mathcal{A}$ obtenus après les transformations des questions 2.4 et 2.5.

Question 2.6. *Prouvez, en utilisant les résultats des questions précédentes, que soit l'ensemble d'axiomes $\mathcal{A}$ produit une preuve de l'absurde, soit il admet un modèle $\mathcal{M}$, dit de Herbrand, dont l'ensemble de base est l'ensemble $T = \{t_1, t_2, \ldots\}$ (au plus dénombrable) des termes construits sur la signature Σ, les symboles de fonction étant interprétés comme eux-mêmes.*

Par exemple, si la signature Σ comporte un symbole de fonction unaire S, un symbole de constante O et un symbole de fonction binaire P, alors $P(S(O), S(S(O)))$ est un terme, et on impose que l'interprétation de O dans le modèle soit le terme O, que l'interprétation de S dans le modèle soit la fonction qui à un terme x associe le terme $S(x)$, et que l'interprétation de P dans le modèle soit la fonction qui à deux termes x, y associe le terme $P(x, y)$.

Solution : Il s'agit de se ramener aux résultats sur les formules propositionnelles. La question 2.4 a permi de se débarasser des quantificateurs existentiels, et il reste à faire de même pour les quantificateurs universels. Pour cela, on instancie chaque axiome de $\mathcal{A}$ par toutes les combinaisons d'éléments de T. Par exemple, un axiome $\forall x \forall y\ P$ (P sans quantificateurs) sera remplacé par $P[x \mapsto t_1, y \mapsto t_2]$ (remplacement de x par t_1 et de y par t_2 dans P) pour tous termes t_1 et t_2 (remarquons qu'un axiome est donc en général remplacé par une infinité dénombrable d'axiomes). On obtient ainsi un système d'axiomes $\mathcal{A}'$, à nouveau dénombrable.

Dans le système d'axiomes $\mathcal{A}'$ résultant, il n'y a plus de quantificateurs, et les formules atomiques sont de la forme $P(t_1, \ldots, t_k)$ où P est une relation k-aire et $t_1, \ldots, t_k$ sont des termes. On peut considérer que chacune de ces formules atomiques est une variable propositionnelle. On a donc construit un ensemble dénombrable de formules propositionnelles sur un ensemble dénombrable de variables. Trouver un modèle de $\mathcal{A}'$, c'est donc trouver des valeurs booléennes pour ces variables propositionnelles qui satisfont les axiomes.

On peut donc appliquer la question 2.3 : soit $\mathcal{A}'$ admet un modèle (qui correspond immédiatement à un modèle de $\mathcal{A}$), soit il n'en admet pas et on a une preuve de l'absurde à partir des axiomes de $\mathcal{A}'$. Or, chaque axiome de $\mathcal{A}'$ se déduit d'un axiome de $\mathcal{A}$ par spécialisation ; donc par modus ponens on peut déduire l'absurde à partir des axiomes de $\mathcal{A}$. □