École polytechnique — X2011 — INF423 Fondements de l'informatique

Logique, modèles, calculs: PC notée

L'énoncé est intentionnellement trop long, ceci afin de pouvoir noter en barème débordant et de ne pas trop pénaliser ceux qui bloqueraient sur une question. Les parties sont indépendantes et pourront être traitées dans n'importe quel ordre. Il est possible d'admettre le résultat d'une question pour traiter les questions suivantes.

Nous attacherons de l'importance à la **clarté** de la rédaction et vous saurons gré d'**écrire lisiblement**. Les raisonnements mathématiques du corrigé des parties 1 et 3 peuvent s'exprimer synthétiquement en quelques lignes : il est probable que vous faites fausse route si vous cherchez quelque chose de compliqué.

1 Preuves et décidabilité

Question 1.1. *Supposons que nous sommes sur un langage et un système d'axiomes complet (toute formule close est soit prouvable, soit de contraire prouvable), avec un ensemble d'axiomes décidable (décider si une formule close est un axiome est un problème décidable ; autrement dit il y a une machine de Turing qui, si on lui met en entrée un texte sur un alphabet de symboles mathématiques, termine toujours, et accepte si et seulement si le texte est l'écriture d'une formule close qui est un axiome de ce système). Montrez qu'il existe une fonction calculable qui, au vu d'une formule close T, répond elle est démontrable ou de contraire démontrable.*

Question 1.2. *Étendez au cas où l'ensemble des axiomes est récursivement énumérable (autrement dit il y a une machine de Turing qui, si on lui met en entrée un texte sur un alphabet de symboles mathématiques, peut terminer* ou ne pas terminer*, et accepte si et seulement si le texte est l'écriture d'une formule close qui est un axiome de ce système).*

Nous fixons la signature à celle de l'arithmétique de Peano (0, successeur noté S, $+$, $-$, $\times$, $\leq$ usuels, avec les notations usuelles telles que $<$). Si n est un entier naturel, nous notons $\overline{n}$ le terme $\underbrace{S \dots S}_{n \text{ fois}} 0$; pour tout modèle de l'arithmétique, on appellera l'interprétation de ce terme « entier standard n ».

Une formule est dite Σ_1^0 si elle commence par des quantificateurs existentiels, puis se poursuit par une formule Σ_0^0. Une formule Σ_0^0 commence éventuellement par des quantificateurs bornés $\forall k < e\ F$ ou $\exists k < e\ F$ où e est une expression arithmétique en les variables libres ou introduites par les quantificateurs précédents, et se poursuit par une formule sans quantificateurs. Un quantificateur borné $\forall k < e\ F$ (F est une formule) est une notation pour $\forall k\ (k < e \Rightarrow F)$. Ainsi, $\exists n \forall a < n \forall b < n\ n \neq ab$ est une formule Σ_1^0 (qui veut dire « il existe un nombre premier »), mais $\exists n \forall a \forall b\ (n \neq ab \vee a = 1 \vee b = 1)$ (qui veut dire la même chose) n'est pas Σ_1^0.

Question 1.3. *Montrez que quel que soit le modèle $\mathcal{M}$ de l'arithmétique tel que $\mathcal{M} \models x < y$, si y a même interprétation que $\overline{n}$, alors les seules interprétations possibles de x sont celles des entiers naturels standards $m < n$.*

(Nous ne demandons pas de détailler les raisonnements arithmétiques simples : autrement dit, vous pouvez dire sans le justifier à l'aide des axiomes de Peano que, quel que soit le modèle $\mathcal{M}$ considéré, $\mathcal{M} \models \forall x \forall y\ x < y \Rightarrow x + 1 < y + 2$ ou autre formule évidente du même genre.)

Question 1.4. *Montrez que l'interprétation d'une formule Σ_0^0 close est la même dans tout modèle.*

Question 1.5. *Soit F une formule Σ_1^0 close, de la forme $\exists x_1 \dots \exists x_n\ B$, où tous les quantificateurs de B sont bornés (les variables libres de B sont donc incluses dans les $x_1, \dots, x_n$). Supposons F indécidable (c'est-à-dire qu'il existe au moins un modèle où F est vraie et un modèle où F est fausse).*

Montrez que B est alors toujours fausse si on remplace toutes ses variables libres par des entier naturels standards.

On admettra qu'il existe une formule H de l'arithmétique de Peano, à un « trou » noté x, de classe Σ_1^0, telle que $H[\overline{n}/x]$ (H dans laquelle on a remplacé x par $\underbrace{S \dots S}_{n \text{ fois}} 0$) est vraie dans le modèle standard $\mathbb{N}$ si et seulement si la machine de Turing numéro x termine sur l'entrée x.

Question 1.6. *Soit f la fonction de l'ensemble des formules closes de l'arithmétique de Peano vers l'ensemble $\{vrai, faux, indécidable\}$ qui dit si une formule close est démontrable, de contraire démontrable, ou indécidable. Montrez que f n'est pas calculable.*

Nous considérons des preuves avec le langage et le système d'axiomes de l'arithmétique de Peano, un système de règles de déduction fixé (par exemple celui de Hilbert), et une façon fixée d'écrire les énoncés et preuves de ce système à l'aide d'un alphabet fini. Nous nous intéressons à la fonction qui à chaque théorème T de ce système associe la longueur $l(T)$ de la plus courte preuve de T (nous rappelons qu'un théorème est une formule close prouvable dans le système).

Question 1.7. *Montrez qu'il n'y a pas de fonction récursive totale f de l'ensemble des formules closes de l'arithmétique de Peano telle que pour tout théorème T, $l(T) < f(T)$ (il n'y a aucune contrainte sur les valeurs de $f(T)$ ailleurs que sur les théorèmes).*

On en conclut donc qu'il est impossible de borner *a priori* de façon effective (calculable) la longueur de preuve nécessaire pour prouver un théorème.

2 Des machines de Turing pour les fonctions récursives primitives

L'objectif de cet exercice est de montrer que les machines de Turing ont une expressivité suffisante pour calculer des fonctions récursives primitives. Les notations de la dernière PC sont conservées, en particulier le k-uplet d'entiers $(n_1, \dots, n_k)$ sera représenté par le mot $a^{n_1+1}ba^{n_2+1}b\cdots a^{n_k+1}$ sur l'alphabet $\Sigma = \{a, b\}$; l'alphabet de travail Γ contient Σ et $\mathbf{B} \in \Gamma \setminus \Sigma$ est le caractère blanc. On réutilisera une partie des machines qui ont été construites, notamment

- F_ℓ (pour *Forward*) qui avance la tête de lecture sur le ruban jusqu'à la première occurrence de la lettre $\ell \in \Gamma$ et recule alors sur le caractère précédent ;
- B_ℓ (pour *Backward*) qui recule et termine sur le premier caractère suivant l'occurrence de ℓ précédente ;
- D_ℓ et D'_ℓ (pour *Delete*) qui prennent en entrée un mot ℓw où $\ell \in \Sigma$ et w est un mot sur Σ, et s'arrêtent avec le mot w sur leur ruban, décalé d'une lettre, la tête de lecture sur le premier caractère de w pour D_ℓ, sur le premier caractère suivant w pour D'_ℓ (on pourra aussi noter ces machines simplement D et D' si la lettre ℓ n'importe pas) ;
- I_ℓ, I'_ℓ et I''_ℓ (pour *insert*) qui prennent en entrée un mot w sur l'alphabet $\{a, b\}$, et s'arrêtent avec respectivement les mots ℓw, $w\ell$, $w\ell$ sur leurs rubans. La différence entre I'_ℓ et I''_ℓ est que cette dernière laisse sa tête de lecture sur le caractère suivant $w\ell$;
- Copy_ℓ^m qui prend un mot de la forme $w_1\ell w_2$ où w_1 et w_2 sont des mots sur Σ, ℓ et m sont des lettres différentes de $\mathbf{B}$ dans $\Gamma \setminus \Sigma$, et s'arrête avec le mot $w_1\ell w_2 m w_1$ sur son ruban.

Question 2.1. *Écrire une machine de Turing Proj_i qui calcule la fonction prenant en entrée un k-uplet d'entiers et renvoyant le i^e, avec $1 \leq i \leq k$.*

Question 2.2. *À partir de k machines $\mathsf{G}_1, \ldots, \mathsf{G}_k$ calculant des fonctions $g_1, \ldots, g_k$ de $\mathbb{N}^n$ dans $\mathbb{N}$ et d'une machine F calculant une fonction f de $\mathbb{N}^k$ dans $\mathbb{N}$, construire une machine calculant l'application $(x_1, \ldots, x_n) \mapsto f(g_1(x_1, \ldots, x_n), \ldots, g_k(x_1, \ldots, x_n))$.*

Question 2.3. *À partir d'une machine G calculant une fonction g de $\mathbb{N}^{n-1}$ dans $\mathbb{N}$ et d'une machine H calculant une fonction h de $\mathbb{N}^{n+1}$ dans $\mathbb{N}$, construire une machine calculant la fonction de $\mathbb{N}^n$ dans $\mathbb{N}$ définie récursivement par*

$$f(0, x_2, \ldots, x_n) = g(x_2, \ldots, x_n),$$
$$f(x_1 + 1, x_2, \ldots, x_n) = h(f(x_1, \ldots, x_n), x_1, \ldots, x_n).$$

Les machines de Turing ont donc au moins l'expressivité des fonctions récursives primitives. Le sujet de la première PC se concluait en mentionnant que ce qui manquait aux fonctions primitives récursives pour avoir toute l'expressivité des machines de Turing était la minimisation non-bornée (correspondant au 'while' des langages de programmation). C'est par contre une opération très facile à implanter sur une machine de Turing.

Question 2.4. *À partir d'une machine F calculant une fonction $f : \mathbb{N}^n \to \{0, 1\}$, construire une machine, qui prend en entrée le codage de $(x_2, \ldots, x_n)$ et s'arrête avec sur son ruban le codage du plus petit $y \in \mathbb{N}$ tel que $f(y, x_2, \ldots, x_n) = 1$ s'il en existe 1, et boucle sinon.*

3 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 1. *Tout système d'axiomes (formules closes) sur une signature au plus dénombrable soit permet d'obtenir une preuve de l'absurde, soit admet un modèle au plus démontrable.*

Quelques points de vocabulaire et de notations :
- Au plus dénombrable = fini ou dénombrable.
- Preuve de l'absurde : preuve de la formule « faux » ou, de façon équivalente, preuve de F et $\neg F$ pour une formule F quelconque.
- 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).

Nous ne préciserons pas le système de preuves utilisé, mais il vérifiera les propriétés usuelles, dont :
- Si $F_1, \ldots, F_n, G$ sont des formules propositionnelles et que pour toute valuation des variables propositionnelles qui satisfait $F_1, \ldots, F_n$, alors cette valuation satisfait G, alors $F_1, \ldots, F_n \vdash G$ (« le système de preuve permet de déduire G à partir de $F_1, \ldots, F_n$ »).
- De toute formule quantifiée universellement $\forall x\ F$ on peut déduire $F[t/x]$ où t est un terme quelconque.

3.1 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 3.1. *Démontrez qu'un ensemble E (éventuellement infini) de formules propositionnelles sur un ensemble fini de variables soit est incohérent (et alors il existe une preuve de l'absurde à partir de ces formules), soit admet un modèle (qui satisfait chaque formule de E).*

Question 3.2. *Démontrez qu'un ensemble E (éventuellement infini) de formules propositionnelles sur un ensemble au plus dénombrable de variables soit est incohérent (et alors il existe une preuve de l'absurde à partir de ces formules), soit admet un modèle.*

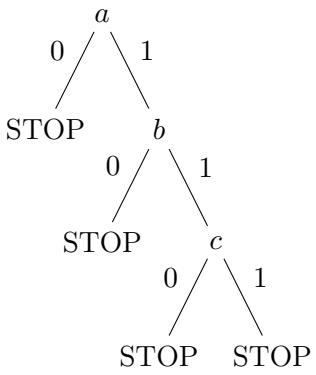
Indice : On ne s'occupera que du cas où l'ensemble de variables est dénombrable, le cas fini ayant été traité à la question précédente. On note E_n l'ensemble des formules de E ne portant que sur les variables $v_1, \ldots, v_n$.

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 point 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 incohérent.

Toute branche de l'arbre est donc soit infinie, so it 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. [1]

Prenons par exemple les variables propositionnelles $a, b, c, \ldots$ et l'ensemble de formules $\{a \implies c, a \implies \neg c, \neg a \implies c, \neg a \implies \neg c, a \wedge b\}$. $E_1 = \emptyset$, $E_2 = \{a \wedge b\}$, $E_3 = E$, et l'arbre est :



3.2 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 un peu plus dénombrable de prédicats.

Question 3.3. *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.*

Question 3.4. *Montrez qu'on peut se passer du prédicat d'égalité en introduisant un prédicat binaire supplémentaire $\equiv$, des axiomes faisant de $\equiv$ une relation d'équivalence, et des axiomes supplémentaires.*

Nous en arrivons à prouver le théorème de complétude pour la signature Σ et les axiomes $\mathcal{A}$ obtenus après les transformations des questions 3.3 et 3.4.

Question 3.5. *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.*

1. En revanche, si un nœud peut avoir une infinité d'arêtes sortantes, alors ce résultat devient faux.