École polytechnique — X2017 — INF412 Fondements de l'informatique

PC6 notée

Sujet proposé par Stéphane Graham-Lengrand et Samuel Mimram et Bruno Salvy

Cet énoncé comporte trois parties indépendantes et qui pourront être résolues dans n'importe quel ordre. Dans chaque partie, on pourra, pour répondre à une question, admettre les résultats dont on demande la démonstration aux questions *précédentes*. Il n'est pas nécessaire de traiter toutes les questions pour avoir la note maximale. Les correcteurs vous remercient d'avance d'écrire lisiblement.

Dans l'ensemble du sujet, on appellera *théorie égalitaire* une théorie dont la signature possède le symbole de relation $=$ (d'arité 2) et dont les axiomes incluent ceux de la théorie de l'égalité.

On admettra dans le sujet que le théorème de compacité est valide pour toute théorie, que sa signature soit dénombrable ou pas.

1 Décidabilité

On note $\mathcal{L}$ le langage sur l'alphabet $\Sigma = \{a, b\}$ constitué des mots qui contiennent autant de a que de b.

Question 1.1. *Donner une machine de Turing explicite permettant de reconnaître le langage $\mathcal{L}$. [Indication : on peut étendre l'alphabet de travail, et 6 états suffisent en comptant celui de rejet (mais les machines correctes qui ont plus d'états seront bien sûr acceptées).]*

Question 1.2. *Dire si le problème suivant est décidable : déterminer si une machine de Turing M reconnaît au moins un mot de $\mathcal{L}$. Argumentez votre réponse.*

Question 1.3. *Dire si le problème suivant est décidable : déterminer si une machine de Turing M ne reconnaît que des mots de longueur 1271 et reconnaît au moins un mot de $\mathcal{L}$. Argumentez votre réponse.*

Question 1.4. *Dire si le problème suivant est décidable : étant donné un couple $(\langle M\rangle, w)$ où l'alphabet de travail de M est $\Sigma = \{0, 1\}$, déterminer si la machine de Turing M accepte le mot w sans jamais que le sous-mot 11 n'apparaisse sur le ruban. Argumentez votre réponse.*

2 Graphes

Question 2.1. *Donner une signature et une théorie égalitaire formée d'un nombre fini d'axiomes, et dont les modèles égalitaires sont les graphes non-dirigés, sans boucle, dont l'un des sommets a exactement un voisin et tous les autres sommets ont exactement deux voisins.*

Question 2.2. *Montrer que cette théorie n'a pas de modèle fini.*

3 Ordres et ordres totaux

Un *ensemble ordonné* $(X, \leq)$ est un ensemble X muni d'une relation d'*ordre*, c'est-à-dire une relation réflexive, transitive et antisymétrique. Un ordre est dit *total* lorsque toute paire d'éléments est comparable (on parle alors d'*ensemble totalement ordonné*).

Question 3.1. *Donnez une théorie égalitaire $\mathcal{T}$ dont les modèles égalitaires sont les ensembles ordonnés. Comment modifier cette théorie pour obtenir les ensembles totalement ordonnés ?*

Une *extension* d'un ensemble ordonné $(X, \leq)$ est un ordre $\preceq$ sur X tel que $a \leq b$ implique $a \preceq b$ pour toute paire d'éléments a et b de X. Une *linéarisation* de $(X, \leq)$ est une extension par un ordre total.

Question 3.2. *Montrez par récurrence que tout ensemble ordonné fini admet une linéarisation.*

Question 3.3. *Étant donné un ensemble ordonné $(X, \leq)$, donnez une signature et une théorie égalitaire dont les modèles égalitaires sont les ensembles ordonnés $(Y, \preceq)$ tel qu'il existe une injection ϕ de X vers Y et pour tous x et y dans X, $x \leq y$ implique $\phi(x) \preceq \phi(y)$.*

Question 3.4. *En vous inspirant de la construction de la question précédente, montrez que tout ensemble ordonné (pas nécessairement fini) admet une linéarisation.*

4 Théorème de Nelson-Oppen

Motivation (qu'il est inutile de lire pour répondre aux questions). *Tout l'enjeu du raisonnement mathématique est de déterminer l'existence de modèles. On essaye si possible de réduire de tels problèmes à des problèmes plus simples. Par exemple, chercher s'il existe des rationnels x et y et une fonction $f : \mathbb{Q} \to \mathbb{Q}$ tels que $f(2x) \neq f(3y)$ repose sur la théorie $\mathcal{T}_1$ de l'arithmétique et la théorie $\mathcal{T}_2$ de l'égalité sur une signature dont le seul symbole de fonction est f. Ce problème est équivalent à l'existence d'un modèle des formules $f(c_x) = f(c_y)$, $c_x = 2x$, $c_y = 3y$, où l'on a introduit des constantes c_x et c_y pour "nommer" les sous-termes $2x$ et $3y$. L'intérêt est qu'on a alors un problème $I_1 = \{c_x = 2x,\ c_y = 3y\}$ dans la théorie de l'arithmétique et un problème $I_2 = \{f(c_x) = f(c_y)\}$ dans la théorie de l'égalité, qui n'ont rien d'autre en commun que les constantes c_x et c_y que l'on a introduites, en nombre fini. Cet exercise permet de résoudre des problèmes impliquant deux théories $\mathcal{T}_1$ et $\mathcal{T}_2$, une fois écrits sous cette forme séparée.*

Étant donné deux signatures du premier ordre $\Sigma_1 = (\mathcal{C}_1, \mathcal{F}_1, \mathcal{R}_1)$ et $\Sigma_2 = (\mathcal{C}_2, \mathcal{F}_2, \mathcal{R}_2)$, on définit leur intersection $\Sigma_1 \cap \Sigma_2$ comme $(\mathcal{C}_1 \cap \mathcal{C}_2, \mathcal{F}_1 \cap \mathcal{F}_2, \mathcal{R}_1 \cap \mathcal{R}_2)$ et leur union $\Sigma_1 \cup \Sigma_2$ comme $(\mathcal{C}_1 \cup \mathcal{C}_2, \mathcal{F}_1 \cup \mathcal{F}_2, \mathcal{R}_1 \cup \mathcal{R}_2)$.

Étant donné une structure $\mathfrak{M}_1$ sur une signature Σ_1 et une structure $\mathfrak{M}_2$ sur une signature Σ_2, on dit que ces structures sont *isomorphes sur leur signature commune*, ou $\cap$*-isomorphes*, si

- il y a une bijection ϕ de l'ensemble de base de $\mathfrak{M}_1$, noté M_1, vers celui de $\mathfrak{M}_2$, noté M_2 ;
- pour toute constante c dans $\Sigma_1 \cap \Sigma_2$, on a $\phi(c^{\mathfrak{M}_1}) = c^{\mathfrak{M}_2}$;
- pour tout symbole de fonction f d'arité k dans $\Sigma_1 \cap \Sigma_2$, et pour tous $a_1, \ldots, a_k$ dans M_1, on a $\phi(f^{\mathfrak{M}_1}(a_1, \ldots, a_k)) = f^{\mathfrak{M}_2}(\phi(a_1), \ldots, \phi(a_k))$
- pour tout symbole de relation R d'arité k dans $\Sigma_1 \cap \Sigma_2$, et pour tous $a_1, \ldots, a_k$ dans M_1, $R^{\mathfrak{M}_1}(a_1, \ldots, a_k)$ si et seulement si $R^{\mathfrak{M}_2}(\phi(a_1), \ldots, \phi(a_k))$.

Question 4.1. *Supposons qu'une structure $\mathfrak{M}_1$ sur une signature Σ_1 et une structure $\mathfrak{M}_2$ sur une signature Σ_2 sont $\cap$-isomorphes. Montrer que :*

- *pour tout terme clos t sur $\Sigma_1 \cap \Sigma_2$, $\phi(t^{\mathfrak{M}_1}) = t^{\mathfrak{M}_2}$;*
- *pour toute formule atomique close F sur $\Sigma_1 \cap \Sigma_2$, $\mathfrak{M}_1 \models F$ si et seulement si $\mathfrak{M}_2 \models F$.*

On pourrait facilement montrer que c'est plus généralement le cas pour toute formule F close (pas forcément atomique) sur la signature $\Sigma_1 \cap \Sigma_2$. On admettra cela pour la suite de l'exercice.

Question 4.2. *Supposons qu'une structure $\mathfrak{M}_1$ sur une signature Σ_1 et une structure $\mathfrak{M}_2$ sur une signature Σ_2 sont $\cap$-isomorphes. Montrer qu'il existe un structure $\mathfrak{M}_\cup$ sur la signature $\Sigma_1 \cup \Sigma_2$ telles que, premièrement, $\mathfrak{M}_\cup$ et $\mathfrak{M}_1$ sont $\cap$-isomorphes (sur leur signature commune Σ_1), et deuxièmement $\mathfrak{M}_\cup$ et $\mathfrak{M}_2$ sont $\cap$-isomorphes (sur leur signature commune Σ_2). [Indication : pour interpréter par exemple une constante c on pourra regarder si c est dans Σ_1 ou dans $\Sigma_2 \backslash \Sigma_1$.]*

Hypothèse pour le reste de l'exercice : Fixons maintenant deux signatures Σ_1 et Σ_2 *disjointes*, c'est-à-dire que $\Sigma_1 \cap \Sigma_2$ est de la forme $(\mathcal{C}_\cap, \emptyset, \{=\})$, où $\mathcal{C}_\cap$ est un ensemble fini de constantes, comme suggéré dans l'introduction de cet exercice. On notera $n_\cap$ son cardinal.

Question 4.3. *Décrire l'ensemble $\mathcal{A}_\cap$ des formules atomiques closes sur $\Sigma_1 \cap \Sigma_2$.*
Donner le cardinal de l'ensemble des parties de $\mathcal{A}_\cap$ (le nombre d'ensembles $P \subseteq \mathcal{A}_\cap$).

Pour toute partie $P \subseteq \mathcal{A}_\cap$, on définit P^* comme l'ensemble de formules $P \cup \{\neg F \mid F \in \mathcal{A}_\cap \backslash P\}$.

On admettra le résultat suivant, dont la preuve est simple mais peu pertinente pour INF412 :
Soient E_1 et E_2 deux ensembles finis inclus dans $\mathbb{N}$ avec une bijection ϕ de E_1 vers E_2.
Il existe une bijection $\bar{\phi}$ de $\mathbb{N}$ dans $\mathbb{N}$ qui étend ϕ, i.e. telle que pour tout $n \in E_1$, $\bar{\phi}(n) = \phi(n)$.

Question 4.4. *Soient $\mathfrak{M}_1$ une structure sur Σ_1 et $\mathfrak{M}_2$ une structure sur Σ_2, dont les ensembles de base sont tous les deux $\mathbb{N}$. Soit $P \subseteq \mathcal{A}_\cap$ telle que $\mathfrak{M}_1 \models P^*$ et $\mathfrak{M}_2 \models P^*$.*

— *Donner une bijection ϕ entre l'ensemble $E_1 = \{n \mid \exists c \in \mathcal{C}_\cap, (n = c^{\mathfrak{M}_1})\}$ (l'ensemble des interprétations par $\mathfrak{M}_1$ des constantes communes) et $E_2 = \{n \mid \exists c \in \mathcal{C}_\cap, (n = c^{\mathfrak{M}_2})\}$ (l'ensemble des interprétations par $\mathfrak{M}_2$ des constantes communes), telle que pour toute constante $c \in \mathcal{C}_\cap$, $\phi(c^{\mathfrak{M}_1}) = c^{\mathfrak{M}_2}$.*
— *En déduire que $\mathfrak{M}_1$ et $\mathfrak{M}_2$ sont $\cap$-isomorphes.*

Question 4.5 (Théorème de Nelson-Oppen)**.** *Étant donné*

— *des ensembles $\mathcal{A}_1$ et $\mathcal{A}_2$ de formules closes, respectivement sur les signatures Σ_1 et Σ_2,*
— *une partie $P \subseteq \mathcal{A}_\cap$,*
— *un modèle $\mathfrak{M}_1$ des formules $\mathcal{A}_1 \cup P^*$ et un modèle $\mathfrak{M}_2$ des formules $\mathcal{A}_2 \cup P^*$, dont les ensembles de base sont tous les deux $\mathbb{N}$,*

montrer qu'il existe un modèle $\mathfrak{M}_\cup$ de $\mathcal{A}_1 \cup \mathcal{A}_2$ (sur la signature $\Sigma_1 \cup \Sigma_2$).

Question 4.6 (Réciproque)**.** *Étant donné*

— *des ensembles $\mathcal{A}_1$ et $\mathcal{A}_2$ de formules closes, respectivement sur les signatures Σ_1 et Σ_2,*
— *un modèle $\mathfrak{M}_\cup$ de $\mathcal{A}_1 \cup \mathcal{A}_2$,*

montrer qu'il existe une partie $P \subseteq \mathcal{A}_\cap$, un modèle $\mathfrak{M}_1$ des formules $\mathcal{A}_1 \cup P^*$ et un modèle $\mathfrak{M}_2$ des formules $\mathcal{A}_2 \cup P^*$.

On étudie maintenant les conséquences algorithmiques du théorème et de sa réciproque.
Une théorie $\mathcal{T}$ sur une signature Σ est dite *sympathique* si

— il existe un algorithme prenant en entrée un ensemble fini I de formules closes sans quantificateurs sur Σ, et renvoie en sortie s'il existe un modèle de $\mathcal{T} \cup I$ ou pas ;
— et pour tout ensemble I de formules sans quantificateurs sur Σ, il existe un modèle de $\mathcal{T} \cup I$ si et seulement s'il en existe un dont l'ensemble de base est $\mathbb{N}$.

Question 4.7. *Étant donné une théorie sympathique $\mathcal{T}_1$ sur Σ_1 et une théorie sympathique $\mathcal{T}_2$ sur Σ_2, donner un algorithme prenant en entrée deux ensembles finis I_1 et I_2 de formules closes sans quantificateurs, respectivement sur Σ_1 et Σ_2, et renvoie en sortie s'il existe un modèle de $\mathcal{T}_1 \cup \mathcal{T}_2 \cup I_1 \cup I_2$ ou pas.*