Logique informatique 2016-2017. Examen

23 mai 2017. Durée 3h.

Tous les documents sont autorisés. Les appareils électroniques sont interdits. Seuls les résultats du cours peuvent être utilisés sans démonstration.

Exercice 1 (minimum 10 points)

Parmi les énoncés suivants, dire ceux qui sont vrais, ceux qui sont faux et ceux sur lesquels on ne sait pas conclure. Justifier en donnant si nécéssaire des exemples ou des preuves s'appuyant sur des résultats du cours.

1. La formule $\exists x.(P(x) \to P(s(x)))$ est valide.
2. L'arithmétique élémentaire n'a pas de modèle fini.
3. Si l'arithmétique de Peano est cohérente, alors deux modèles de l'arithmétique de Peano sont toujours élémentairement équivalents.
4. On suppose que $\mathcal{F}$ contient au moins un symbole de constante. Soit ϕ une formule sans quantificateur. $\exists \overline{x}.\phi$ est valide si et seulement si il existe des séquences de termes $\overline{t_1}, \ldots, \overline{t_k}$ telles que $\bigvee_{i=1}^{k} \phi\{\overline{x} \mapsto \overline{t_i}\}$ est valide.
5. Si t_1, t_2, t_3 sont trois termes et qu'il existe σ tel que $t_1\sigma = t_2\sigma = t_3\sigma$, alors il existe une substitution la plus générale, θ, telle que $t_1\theta = t_2\theta = t_3\theta$. De plus, si $\sigma_1 = \mathsf{mgu}(t_2, t_3)$ et $\sigma_2 = \mathsf{mgu}(t_1\sigma_1, t_2\sigma_1)$, $\theta = \sigma_1\sigma_2$.
6. On suppose $\mathcal{F} = \{+\}$ et $\mathcal{P} = \{=\}$ considère les deux structures $\mathbb{N}$ et $\mathbb{Z}$ avec l'interprétation usuelle du symbole $+$. Il n'existe pas d'isomorphisme partiel h de $\mathbb{N}$ dans $\mathbb{Z}$ tel que $\mathsf{Dom}(h) = \{2, 3\}$ et $h(3) = 2$.

Exercice 2

On veut montrer la décidabilité du fragment FO_1 des formules de la logique du premier ordre ne contenant qu'une seule variable. Les formules de FO_1 sont construites sur un ensemble $\mathcal{P}$ de symboles de prédicat, un ensemble de symboles de fonction $\mathcal{F}$ qui ne contient que des constantes, les connecteurs logiques habituelles et une seule variable x. Par exemple, $\exists x.((P(a, x) \wedge Q(x)) \to \exists x.P(x, x)) \in \mathsf{FO}_1$.

1. Montrer que toute formule de FO_1 est logiquement équivalente à une combinaison Booléenne de formules de FO_1 en forme prénexe.
2. En déduire que toute formule de FO_1 est logiquement équivalente à une formule $\exists x_1, \ldots, x_n \forall y_1, \ldots y_m.\psi$ où ψ est sans quantificateur.
3. En déduire un algorithme pour décider de la satisfaisabilité des formules de FO_1.

Exercice 3

On considère $\mathcal{P} = \{P, Q\}$ et $\mathcal{F} = \{0, s\}$ et l'ensemble $\mathcal{A}$ constitué des 4 axiomes :

$$\mathcal{A} = \{P(0), \neg Q(0), \forall x.(P(x) \leftrightarrow Q(s(x))), \forall x.(Q(x) \leftrightarrow P(s(x))\}$$

Montrer que $\mathsf{Th}(\mathcal{A})$ est décidable (par une méthode d'élimination de quantificateurs) et incomplète.

Solution

Exercice 1

1. Vrai. La négation de la formule : $\forall x.(P(x) \wedge \neg P(s(x))$ n'est pas satisfaisable puisque des deux clauses $P(y)$ et $\neg P(s(z))$ on déduit la clause vide en une étape de résolution. La formule est donc valide.

   Commentaires 2.7 points. 34% de réussite.
   La question la plus décevante. Beaucoup d'erreurs. Certains élèves ne savent plus ce que "valide" signifie. D'autres donnent un "contre-modèle" incorrect, en oubliant que $P \Rightarrow Q$ est satisfait par toutes les interprétations dans lesquelles P est faux. Enfin, les alphabets $\mathcal{P}, \mathcal{F}$ n'étaient pas précisés car quelconques ; il ne fallait pas faire d'hypothèse.

2. Vrai. Si l'arithmétique élémentaire avait un modèle fini $\mathcal{M}$, il existerait au moins deux entiers distincts $n, n+k$ tels que $\mathcal{M} \models s^n(0) = s^{n+k}(0)$. Par récurrence sur n et en utilisant l'axiome $\forall x, y.(s(x) = s(y) \to x = y)$, on obtiendrait $\mathcal{M} \models 0 = s^k(0)$, ce qui contredit l'axiome $\forall x.0 \neq s(x)$.

   Commentaires 2.4 points. 85% de réussite
   La question la mieux traitée. Il faut faire attention dans la rédactionà distinguer la syntaxe ($s^n(0) = 0$ par exemple) de la sémantique, i.e., l'interprétation de ces formules dans un modèle,

3. Faux. L'arithmétique de Peano est incomplète ou incohérente (théorème de Gödel). Or une théorie est complète si et seulement si tous ses modèles sont éléentairement équivalents (vu en cours).

   Commentaires 2.4 points. 56% de réussite

4. Vrai. $\forall \overline{x}.\neg\phi$ est insatisfaisable ssi elle n'a pas de modèle de Herbrand (en étendant $\mathcal{F}$ avec une constante s'il n'y en a pas) ssi $\{\neg\phi\{\overline{x} \mapsto \overline{t}\} \mid \overline{t} \in T(\mathcal{F}')\}$ est insatisfaisable ssi il existe des séquences de termes $\overline{t_1}, \ldots, \overline{t_k} \in T(\mathcal{F})$ tels que $\{\neg\phi\{\overline{x} \mapsto \overline{t_1}\}, \ldots, \neg\phi\{\overline{x} \mapsto \overline{t_k}\}\}$ est insatisfaisable (par compacité) ssi $\bigwedge_{i=1}^{k} \neg\phi\{\overline{x} \mapsto \overline{t_i}\}$ est insatisfaisable ssi $\bigvee_{i=1}^{k} \phi\{\overline{x} \mapsto \overline{t_i}\}$ est valide.

   Commentaires 2.9 points. 14% de réussite
   La question la moins réussie. Mais elle était difficile, puisqu'il fallait enchainer le passage à la négation, le théorème de Herbrand et le théorème de compacité. La question 1 aurait dû aider à répondre en donnant un exemple où deux termes sont nécessaires.
   S'il est pardonable de ne pas répondre à la question, dire que $\exists x.\phi$ valide entraine $\phi\{x \mapsto t\}$ valide pour un certain terme t est impardonable : le théorème de Herbrand ne peut être utilisé que sur des formules purement universelles. Des (contre-)exemples ont été vus en cours pour les formules existentielles.

5. Vrai. On considère le système d'équations $t_1 = t_2 \wedge t_2 = t_3$, s'il a une solution, il a une forme résolue $x_1 = u_1 \wedge \ldots \wedge x_n = u_n$; $\theta = \{x_1 \mapsto u_1, \ldots, x_n \mapsto u_n\}$ est une solution la plus générale. De plus, comme les règles de résolution des équations sont appliquées dans un ordre arbitraire, $t_1 \wedge t_2 \wedge t_2 = t_3 \rightsquigarrow^* t_1\psi = t_2\psi \wedge \psi \rightsquigarrow^* \theta$ où $\psi = \mathsf{mgu}(t_2, t_3)$.

Commentaires 1.9 points. 37% de réussite
Apparemment, il y a plusieurs définitions de mgu, certaines incluant l'idempotence. Il n'a pas été tenu compte ici de la preuve ou non d'idempotence.

6. Faux. $h(3) = 2$ et $h(2) = 3$ est un isomorphisme partiel puisque, pour tous $a, b, c \in \{2, 3\}$, $a + b \neq c$ et donc $a + b = c$ ssi $h(a) + h(b) = h(c)$.

   Commentaires 1.9 points. 54% de réussite
   La définition d'isomorphisme partiel du cours est équivalente à l'équisatisfaction des formules atomiques plates. Donc par exemple, $h(3) = 2$ et $h(2) = 1$ n'est *pas* un isomorphisme partiel puisque $h(2)+h(2) = h(3)$ et $2+2 \neq 3$. En revanche, $x+x+x = y+y$ n'est pas une formule atomique plate, on ne peut donc pas objecter que $h(2) + h(2) + h(2) = h(3) + h(3)$ ne peut pas être réalisé. Les élèves ayant utilisé une de ces deux définitions alternatives à la définition d'isomorphisme partie du cours ont obtenu la moitié des points.

Exercice 2

1. On commence par mettre ϕ en forme normale négative. On montre ensuite, par récurrence sur ϕ (qui contient au plus une variable, qui peut éventuellement avoir des occurrences libres) que ϕ est logiquement équivalente à une combinaison booléenne positive de formules de FO_1 en forme prénexe.
   Si ϕ est un littéral, ϕ est une combinaison booléenne positive de formules en forme prénexe.
   Sinon, si $\phi = \phi_1 \wedge \phi_2$ ou $\phi = \phi_1 \vee \phi_2$, il suffit d'appliquer l'hypothèse de récurrence.
   Si $\phi = \exists x.\psi$. Par hypothèse de récurrence, ψ est une combinaison booléenne positive de formules en forme prénexe. On met ψ en forme normale disjonctive : $\psi \models\!\mid \bigvee \psi_i$ où ψ_i est une conjonction de formules en forme prénexe : $\psi_i = \psi_i^0 \wedge \bigwedge_j Q_j x.\psi_i^j$ où ψ_i^j est sans quantificateur, ψ_i^j a pour seule variable x et $Q_i^j \in \{\exists, \forall\}$. Alors,
   $$\phi \models\!\mid \bigvee_i ((\exists x.\psi_i^0) \wedge \bigwedge_j Q_j x.\psi_i^j)$$
   Si $\phi = \forall x.\psi$, on procède de même : $\psi \models\!\mid \bigwedge_i(\psi_i^0 \bigvee_j Q_j x.\psi_i^j)$ et
   $$\phi \models\!\mid \bigwedge_i ((\forall x.\psi_i^0 \bigvee_j Q_j x.\psi_i^j))$$

   Commentaires 2.6 points, taux de réussite 10%
   Cette question n'a été correctement résolue par aucun élève. L'erreur la plus courante est de ne pas s'apercevoir que x peut être à la fois libre et liée dans une même sous-formule. Personne n'a vu qu'il fallait une étape de mise en forme normale disjonctive (resp. conjonctive) selon le quantificateur à rentrer.

2. Si ϕ est une combinaison booléenne positive de formules de FO_1 en forme prénexe,
   $$\phi \models\!\mid \bigvee_i (\bigwedge_j \exists x.\psi_{i,j}(x) \wedge \bigwedge_j \forall x.\psi'_{i,j}(x) \wedge \bigwedge_j \psi^0_{i,j}(x))$$

où toutes les formules $\psi_{i,j}, \psi'_{i,j}, \psi^0_{i,j}$ sont sans quantificateur. On sort successivement les quantificateurs existentiels, puis universels, en renommant les variables pour éviter les captures (mise en forme prénexe) :

$$\phi \models\!\!\!\!\!\!\!\!= \exists x_1, \ldots x_n. \bigvee_i (\bigwedge_j \psi_{i,j}(x_j) \wedge \bigwedge_j \forall x. \psi'_{i,j}(x) \wedge \bigwedge_j \psi^0_{i,j}(x))$$

$$\phi \models\!\!\!\!\!\!\!\!= \exists x_1, \ldots x_n. \forall y_1, \ldots, y_m. \bigvee_i (\bigwedge_j \psi_{i,j}(x_j) \wedge \bigwedge_j \psi'_{i,j}(y_j) \wedge \bigwedge_j \psi^0_{i,j}(x))$$

Commentaires 1.1 points, 44% de réussite
Une question facile : la seule chose importante à dire est qu'on peut choisir dans quel ordre sortir les quantificateurs, et qu'on commence par $\exists$. Montrer qu'in fine on peut commuter les quantificateurs est plus hasardeux et sujet à erreurs.

3. Il suffit de considérer les formules (sans variable libre) de la forme $\exists x_1, \ldots, x_n. \forall y_1, \ldots, y_m. \psi$ où ψ est sans quantificateur. Par Skolémisation, une telle formule est satisfaisable ssi la formule $\forall y_1, \ldots, y_m. \psi\{x_i \mapsto a_i\}$ est satisfaisable, où les a_i sont des nouvelles constantes. Par le théorème de Herbrand, une telle formule est satisfaisable ssi elle a un modèle de Herbrand. Mais l'univers de Herbrand est ici fini (il ne contient que des constantes). L'ensemble des modèles de Herbrand est ainsi fini. De plus, étant donné un modèle de Herbrand (fini), on peut facilement tester la satisfaction de la formule en énumérant les affectations possibles des variables quantifiées universellement. (**Note :** on peut montrer que le problème de décision est dans PSPACE).

Commentaires 2.4 points. Taux de réussite 17%
Les "procédures de décision" qui marcheraient aussi pour des formules en forme prénexe arbitraires auraient dû conduire à se poser des questions !

Exercice 3

On considère une formule $\exists x. \phi$ où ϕ est sans quantificateur.

Comme vu en cours, on peut se limiter aux formules ϕ qui sont des conjonctions de littéraux.

$$\phi = \phi_{-x} \wedge \bigwedge_i Q(s^{n_i}(x)) \wedge \bigwedge_i \neg Q(s^{m_i}(x)) \wedge \bigwedge_i P(s^{k_i}(x)) \wedge \bigwedge_i \neg P(s^{\ell_i}(x))$$

où ϕ_{-x} ne contient pas x. On peut ensuite simplifier la formule à l'aide des axiomes. D'abord, pour tout n, $\mathcal{A} \models (\neg)P(s^n(x)) \leftrightarrow Q(s^{n+1}(x)$. Ensuite, pour tout n, $\mathcal{A} \models Q(s^{2n+b}(x)) \leftrightarrow Q(s^b(x))$. On se ramène donc à une formule

$$\bigwedge_i Q(s^{n_i}(x)) \wedge \bigwedge_i \neg Q(s^{m_i}(x))$$

où $n_i, m_i \in \{0, 1\}$. Si la formule contient la conjonction $Q(x) \wedge \neg Q(x)$ ou $Q(s(x)) \wedge \neg Q(s(x))$, on peut simplement la remplacer par $\perp$. Si elle contient une seule formule atomique $Q(x)$ (resp. $\neg Q(x)$, resp. $Q(s(x))$, resp. $\neg Q(s(x))$) on peut la remplacer par $\top$, grâce aux axiomes (dérivés) $Q(s(0))$ et $\neg Q(0)$, $\neg Q(s(s(0)))$.

Il ne reste que deux cas où la formule

$$\exists x. \bigwedge_i Q(s^{n_i}(x)) \wedge \bigwedge_i \neg Q(s^{m_i}(x)) \wedge \bigwedge_i P(s^{k_i}(x)) \wedge \bigwedge_i \neg P(s^{\ell_i}(x))$$

n'a été remplacée ni par $\bot$, ni par $\top$. C'est le cas où cette formule est $\exists x. Q(x) \wedge Q(s(x))$ ou $\exists x. \neg Q(x) \wedge \neg Q(s(x))$.

Et, en effet, on peut construire un modèle dans lequel la première formule est invalide ($\mathbb{N}$, Q ensemble des entiers impairs, P ensemble des entiers pairs) et un modèle dans lequel cette formule est valide : $\mathbb{N} \uplus \mathbb{Z}$ où on ajoute $\mathbb{Z}$ aux entiers impairs.

On en conclut que la théorie n'est pas complète. En revanche, en ajoutant deux variables propositionnelles $E \leftrightarrow \phi_E = \exists x. Q(x) \wedge Q(s(x))$ et $F \leftrightarrow \phi_F = \exists x. \neg Q(x) \wedge \neg Q(s(x))$. (on étend la théorie par ces définitions), alors on peut éliminer le quantificateur existentiel et, d'après le résultat du cours, pour toute formule ϕ sans variable libre,

$$\mathcal{A}' \models \phi \leftrightarrow \theta_\phi$$

où θ_ϕ est une formule propositionnelle sur les variables propositionnelles E, F.

Montrons que $\mathcal{A} \models \phi$ ssi θ_ϕ est valide en calcul propositionnel.

Dans un sens, c'est immédiat : si θ_ϕ est valide, alors, dans tout modèle de $\mathcal{A}'$, θ_ϕ est valide et donc $\mathcal{A}' \models \phi$ et donc $\mathcal{A} \models \phi$.

Réciproquement, si θ_ϕ n'est pas valide, il existe un contre-modèle qui est un sous-ensemble de $\{E, F\}$. Montrons, que, pour n'importe quel sous-ensemble S de $\{E, F\}$, il existe un modèle de $\mathcal{A}$ qui satisfait ϕ_X pour $X \in S$ et $\neg\phi_X$ pour $X \notin S$.

Pour cela, on considère les 4 modèles suivants (on liste le domaine, et l'interprétation de Q) : $\mathcal{S}_\emptyset = \mathbb{N}, 2\mathbb{N}+1$, $\mathcal{S}_{\{F\}} = \mathbb{N}\uplus\mathbb{Z}, 2\mathbb{N}+1$, $\mathcal{S}_{\{E\}} = \mathbb{N}\uplus\mathbb{Z}, 2\mathbb{N}+1\uplus\mathbb{Z}$, $\mathcal{S}_{\{E,F\}} = \mathbb{N}\uplus\mathbb{Z}\uplus\mathbb{Z}, 2\mathbb{N}+1\uplus\mathbb{Z}$.

Dans tous les cas, si θ_ϕ n'est pas valide, on peut trouver un modèle de $\mathcal{A}$ qui n'est pas un modèle de ϕ.

Commentaires 5.5 points, 15% de réussite

Aucun élève n'a proposé de procédure de décision correcte. Comme la théorie est incomplète (question bien traitée par plusieurs élèves), la procédure d'élimination des quantificateurs doit nécessairement faire appel à l'introduction d'extensions par définition (comme dans la théorie de l'égalité vue en cours). Sinon, comme quelques élèves l'ont remarqué, l'élimination des quantificateurs montre aussi la complétude de la théorie !