# Logique informatique 2013-2014. Examen

30 mai 2014. Durée 3h.

Tous les documents sont autorisés. Seuls les résultats du cours peuvent être utilisés sans démonstration.

### Exercice 1

Soit $\mathcal{F} = \{a(0), b(0), f(2)\}$ et $\mathcal{P} = \{P(2), Q(2)\}$. L'ensemble des trois clauses (du premier ordre) suivant est il satisfaisable ? Justifier.

$$\forall x.Q(x,a), \qquad \forall x,y,z.\neg P(y,y) \vee \neg P(f(a,x),z), \qquad \forall x,y,z.P(z,y) \vee P(y, f(x,b)) \vee \neg Q(z,a)$$

### Exercice 2

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

1. Toute théorie du premier ordre est incohérente ou incomplète
2. Toute théorie complète est décidable
3. Toute théorie incohérente est décidable
4. L'arithmétique élémentaire n'a pas de modèle fini
5. Toute théorie engendrée par un sous-ensemble d'une théorie complète et récursive est elle-même récursive.
6. L'intersection de deux théories décidables est décidable.
7. La cohérence de l'arithmétique de Peano peut s'exprimer comme une formule de l'arithmétique de Peano, mais on ne peut pas prouver cet énoncé dans l'arithmétique de Peano.

### Problème

Soit $\mathcal{F} = \{s(1), p(1), 0(0)\}$ et $\mathcal{P} = \{\geq, =\}$.

On considère la théorie $\mathcal{T}$ engendrée par les axiomes de la figure 1 ainsi que les axiomes de l'égalité.

1. Montrer que les énoncés suivants sont dans $\mathcal{T}$ (on prendra soin de détailler tous les axiomes utilisés) :
   (a) $s(0) = 0$
   (b) $p(0) = 0$

$$(1) \quad \forall x, y. \quad x \geq y \vee y \geq x$$

$$(2) \quad \forall x, y. \quad (x \geq y \wedge y \geq x) \rightarrow x = y$$

$$(3) \quad \forall x, y, z. \quad (x \geq y \wedge y \geq z) \rightarrow x \geq z$$

$$(4) \quad \forall x, y. \quad x \geq y \leftrightarrow s(x) \geq s(y)$$

$$(5) \quad \forall x, y. \quad (x \geq y \leftrightarrow (x = y \vee x \geq s(y))$$

$$(6) \quad \forall x, y. \quad (s(x) = x \wedge s(y) = y) \rightarrow x = y$$

$$(7) \quad \forall x. \quad 0 \geq x$$

$$(8) \quad \exists x. \quad p(x) \neq x$$

$$(9) \quad \forall x. \quad s(p(x)) = x$$

FIGURE 1 – Axiomes de la théorie $\mathcal{T}$

(c) $\forall x.p(s(x)) = x$

(d) $\forall x, y. \quad x \geq y \leftrightarrow (x = y \vee p(x) \geq y)$

(e) $\forall x, y. \quad x \geq y \leftrightarrow p(x) \geq p(y)$

(f) $\forall x, y. \quad (x \not\geq y \leftrightarrow (y \geq s(x) \wedge x \neq 0)$

(g) $\forall x, y.(x \neq y \leftrightarrow ((x \geq s(y) \vee y \geq s(x)) \wedge (x \neq 0 \vee y \neq 0))$

2. Montrer que $\mathcal{T}$ est cohérente
3. $\mathcal{T}$ admet elle des modèles finis ?
4. Montrer que $\mathcal{T}$ est complète (**Ind** : on pourra utiliser une méthode d'élimination de quantificateurs)
5. Montrer qu'en enlevant l'un des axiomes 7,8 ou 9, la théorie engendrée est incomplète.

# Solution

## Exercice 1

Il est possible de dériver la clause vide par résolution et factorisation binaires :

$$\dfrac{\dfrac{\dfrac{\neg P(y,y) \lor \neg P(f(a,x),z)}{\neg P(f(a,x),f(a,x))}\,F \qquad \dfrac{P(z,y) \lor P(y,f(x,b)) \lor \neg Q(z,a)}{P(f(x,b),f(x,b)) \lor \neg Q(f(x,b),a)}\,F}{\neg Q(f(a,b),a)}\,R \qquad Q(x,a)}{\bot}\,R$$

L'ensemble de clauses est donc insatisfaisable, par correction du système de preuve.

## Exercice 2

1. **Faux** : La théorie des ordres denses est cohérente et complète. (On peut aussi considérer une théorie triviale où l'ensemble des symboles de prédicat est vide).
2. **Faux**. Par exemple l'ensemble des formules construites sur $\geq$ avec les symboles de fonction $0, 1, +, \times$ et valides dans les entiers (avec l'interprétation habituelle des entiers) est une théorie complète et non récursivement énumérable (cf cours).
3. **Vrai**. Lorsqu'une théorie est incohérente, elle contient tous les énoncés.
4. **Vrai**. S'il existait un modèle fini de l'arithmétique élémentaire $\mathcal{M}$, alors il existerait deux entiers $n$ et $m \neq 0$ tels que $\mathcal{M} \models s^n(0) = s^{n+m}(0)$. Mais, en utilisant l'axiome $\forall x, y. s(x) = s(y) \to x = y$ et par récurrence sur $n$, on obtient $\mathcal{M} \models 0 = s^m(0)$, ce qui contredit l'axiome $\forall x. 0 \neq s(x)$.
5. **Faux**. Il suffit de considérer par exemple l'arithmétique élémentaire $Q$ et toutes les formules closes sur le même alphabet $E$. $E$ est complète, incohérente et donc récursive. $Q$ est engendrée par un sous-ensemble de 7 formules et n'est pas récursive.
6. **Vrai**. Pour savoir si une formule est dans les deux théories, il suffit d'appliquer successivement les deux algorithmes de décision pour chacune des deux théories et répondre oui ssi les deux algorithmes répondent oui.
7. **On ne sait pas** : la cohérence de l'arithmétique s'exprime bien comme un énoncé de l'arithmétique. Si l'arithmétique est cohérente, on ne peut pas le prouver dans l'arithmétique. En revanche, si l'arithmétique est incohérente, on peut démontrer tous les énoncés, en particulier sa propre cohérence.

## Problème

1. Les axiomes de l'égalité sont utilisés sans mention ; les autres axiomes utilisés à chaque étape sont indiqués dans la colonne de droite.

| | | |
|---|---|---|
| (10) | $0 \geq s(0)$ | (7) |
| (11) | $s(0) \geq 0$ | (5) |
| (1$a$) | $s(0) = 0$ | $(10, 11, 2)$ |
| (12) | $\forall x.s(p(s(x))) = s(x)$ | (9) |
| (1$b$) | $\forall x.p(s(x)) = x$ | $(4, 2)$ |
| (13) | $p(s(0)) = 0$ | $(1b)$ |
| (1$c$) | $p(0) = 0$ | $(13, 1a)$ |
| (14) | $\forall x, y.p(x) \geq y \to x \geq s(y)$ | $(4, 9)$ |
| (15) | $\forall x, y(x = y \vee p(x) \geq y) \to x \geq y$ | $(14, 5)$ |
| (16) | $\forall x, y.p(x) \geq y \vee y \geq p(x)$ | (1) |
| (17) | $\forall x, y, p(x) \geq y \vee y = p(x) \vee y \geq s(p(x))$ | $(16, 5)$ |
| (18) | $\forall x, y.p(x) \geq y \vee y \geq x$ | $(17, 9, 5)$ |
| (19) | $\forall x, y.x \geq y \to (p(x) \geq y \vee (y \geq x \wedge x \geq y))$ | (18) |
| (1$d$) | $\forall x, y.x \geq y \to (x = y \vee p(x) \geq y)$ | $(19, 2)$ |
| (20) | $\forall x, y.p(x) \geq p(y) \to x \geq y$ | $(4, 9)$ |
| (21) | $\forall x, y.p(x) \geq p(y) \vee p(y) \geq p(x)$ | (1) |
| (22) | $\forall x, y.x \geq y \to (p(x) \geq p(y) \vee y = x)$ | $(21, 20, 2)$ |
| (23) | $\forall x, y.x \geq y \to p(x) \geq p(y)$ | (22) |
| (1$e$) | $\forall x, y.x \geq y \leftrightarrow p(x) \geq p(y)$ | $(23, 20)$ |
| (24) | $\forall x, y.x \not\geq y \to (y \geq x \wedge y \neq x)$ | $(1, 5)$ |
| (25) | $\forall x, y.x \not\geq y \to y \geq s(x)$ | (5) |
| (26) | $\forall x, y.x \not\geq y \to x \neq 0$ | (7) |
| (27) | $\forall x.s(x) \geq x$ | (5) |
| (28) | $\forall x.x \geq s(x) \to x = 0$ | $(6, 27, 2, 1a)$ |
| (29) | $\forall x, y.(x \neq 0 \wedge y \geq s(x)) \to x \not\geq y$ | $(28, 5)$ |
| (1$f$) | $\forall x, y.x \not\geq y \leftrightarrow (x \neq 0 \wedge y \geq s(x))$ | $(29, 25, 26)$ |
| (30) | $\forall x, y.x \neq y \leftrightarrow (x \not\geq y \vee y \not\geq x)$ | (1) |
| (31) | $\forall x, yy \geq s(x) \vee y \neq 0$ | (7) |
| (1$g$) | $\forall x, y.x \neq y \leftrightarrow ((x \geq s(y) \vee y \geq s(x)) \wedge (x \neq 0 \vee y \neq 0))$ | $(30, 1f, 31)$ |

2. Il suffit de donner un modèle : on choisit $\mathbb{Z} \cup \{\infty\}$. Dans cette structure, 0 est interprété par $\infty$, $s$ est interprété comme le successeur sur les éléments de $\mathbb{Z}$ et $p$ comme le prédécesseur. de plus $\infty$ est invariant par $s$ et $p$. La relation $\geq$ est l'ordre sur $\mathbb{Z}$ avec $\infty \geq z$ pour $z \in \mathbb{Z}$. On vérifie que les 9 axiomes sont satisfaits dans cette structure (...).

3. $\mathcal{T}$ n'admet pas de modl̀e fini : si $\mathcal{M}$ est un modèle de $\mathcal{T}$, par (8), soit $a \in \mathcal{M}$ tel que $p_{\mathcal{M}}(a) \neq a$. Si $\mathcal{M}$ était fini, il existerait deux entiers $n, m$ tels que $m \neq 0$ et $s^n_{\mathcal{M}}(a) = s^{n+m}_{\mathcal{M}}(a)$. Par récurrence sur $n$ et grâce à (5,2), on obtient que $s^m_{\mathcal{M}}(a) = a$. Par récurrence sur $m$ (et grâce à (5,2)) on a alors $a = s_{\mathcal{M}}(a)$ et donc $a = 0_{\mathcal{M}}$ (en utilisant (6) et $s(0) = 0$). Mais comme $p(0) = 0$ est dans la théorie, on doit avoir $p_{\mathcal{M}}(a) = a$, ce qui contredit la construction de $a$.

4. Par la méthode d'élimitation des quantificateurs, il suffit de montrer que, pour toute conjonction littéraux $\phi$, il existe une formule sans quantificateur $\psi$ telle que $\mathcal{T} \models (\exists x.\phi) \leftrightarrow \psi$.

À l'aide de (1f, 1g) on peut supposer sans perte de généralité que les littéraux de $\phi$ sont positif ou bien de la forme $u \neq 0$. En utilisant (9,1a,1b,1c), on peut même supposer que les seuls littéraux négatifs sont de la forme $y \neq 0$ où $y$ est une variable.

En utilisant ensuite (4,1e,9,1c,2), on se ramène à des formules atomiques $x \neq 0, x = 0, x \geq u, u \geq x$ ou bien qui ne contiennent pas la variable $x$. De plus $u$ est d'une des formes $p^n(y)$ ou $s^n(y)$ où $y$ est une variable.

Enfin, on peut remplace $x \geq s^n(x)$ et $p^n(x) \geq x$ par $x = 0$ si $n \geq 1$ et $s^n(x) \geq x$ et $x \geq p^n(x)$ par $\top$. On peut donc supposer sans perte de généralité que les termes $u$ ne contiennent pas $x$.

Nous affirmons alors que

$$\mathcal{T} \models \exists x.\phi \leftrightarrow \phi_{-x} \wedge (\bigwedge_{x \leq u \in \phi, v \leq x \in \phi} v \leq u) \wedge (\bigwedge_{x \neq 0 \in \phi, v \leq x \in \phi} v \neq 0)$$

où $\phi_{-x}$ est la conjonction des littéraux de $\phi$ ne contenant pas $x$. Si nous prouvons ce résultat, nous avons la formule $\psi$ et donc l'élimination des quantificateurs et la complétude de la théorie, puisque pour toute formule sans variable $\theta$, ou bien $\theta \in \mathcal{T}$ ou bien $\neg\theta \in \mathcal{T}$.

Tout d'abord, $\mathcal{T} \models \exists x.(u \leq x \wedge x \leq v \wedge \phi') \rightarrow u \leq v$ (par (3)) et $\mathcal{T} \models \exists x.(x \neq 0 \wedge x \geq v \wedge \phi') \rightarrow v \neq 0$ (par 7,2).

Montrons la réciproque. Soit $\mathcal{M}$ un modèle quelconque de $\mathcal{T}$ et $\sigma$ une affectation quelconque des variables (autres que $x$). Par (1,2,3), si l'ensemble $E_{\leq x} = \{v \,|\, x \geq v \in \phi\}$ est non vide, il existe un élément $v_0 \in E_{\leq x}$ tel que $\mathcal{M}, \sigma \models v_0 \geq v$ pour tous les éléments $v$ de $E_{\leq x}$. (Le cas où l'ensemble est vide sera considéré ultérieurement).

Soit alors $\theta = \sigma \uplus \{x \mapsto v_0\sigma\}$. Par construction, $\mathcal{M}, \theta \models x \geq v$ si $v \in E_{\geq x}$. Comme $\mathcal{M}, \sigma \models u \leq v_0$ pour tous les termes $u$ tels que $u \geq x \in \phi$, on obtient aussi $\mathcal{M}, \theta \models u \geq x$ si $u \geq x$ est dans $\phi$. Enfin, si $x \neq 0$ est dans $\phi$, comme $\mathcal{M}, \sigma \models \psi$, $\mathcal{M}, \sigma \models v_0 \neq 0$ et donc $\mathcal{M}, \theta \models x \neq 0$.

Si maintenant $E_{\leq x}$ est vide. Comme $\mathcal{M} \models \exists x. x \neq p(x)$, il existe $a \in D_{\mathcal{M}}$ tel que $a \neq_{\mathcal{M}} 0_{\mathcal{M}}$. Soit $E_{\geq x} = \{v \mid x \leq v \in \phi\}$. Si $E_{geqx}$ est vide, alors $\phi$ est vide (trivialement satisfaite) ou $\phi$ est la formule $x \neq 0$. Dans ce dernier cas, $\exists x.\phi$ est dans $\mathcal{T}$ (et $\psi = \top$). Soit maintenant $v_0 \in E_{\geq x}$ tel que $\mathcal{M}, \sigma \models v_0 \leq v$ pour tout $v \in E_{\geq x}$. Si $v_0\sigma = 0_{\mathcal{M}}$, on choisit $x\theta = a$. Sinon, on choisit $x\theta = v_0\sigma$. Dans tous les cas $\mathcal{M}, \theta \models \phi$.

L'affirmation est ainsi démontrée : la théorie admet l'élimination des quantificateurs et, comme $\mathcal{T} \models \phi$ ou $\mathcal{T} \models \neg\phi$ pour toutes les formules $\phi$ sans variable, la théorie $\mathcal{T}$ est complète.

5. À chaque fois, construisons un modèle des autres axiomes, dans lequel la formule retirée n'est pas satisfaite.

   **(7)** On considère $\mathbb{Z}$ avec l'interprétation usuelle des symboles et prédicats. En particulier 0 est interprété comme $0_{\mathbb{Z}}$

   **(8)** On considère le modèle réduit à un élément $0_{\mathcal{M}}$. $s, p$ sont donc interpétés comme l'identité, $\geq$ comme l'égalité. Tous les axiomes (sauf (8)) sont trivialement satisfaits.

   **(9)** On considère le modèle $\mathbb{Z} \cup \{\infty\}$ de la question 2, mais en interprétant cette fois $p$ comme $s$.