Logique informatique 2013-2014. Examen

30 mai 2013. Durée 3h.

Tous les documents sont autorisés. Seuls les résultats du cours peuvent être utilisés sans démonstration. Le barême et la longueur des solutions sont donnés à titre indicatif.

Exercice 1

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 incohérente est décidable
3. Il existe des théories décidables, cohérentes et incomplètes
4. L'arithmétique élémentaire n'a pas de modèle fini
5. $\{(n,m) \in \mathbb{N}^2 \mid n =< \phi(x) >, m =< \Pi(\phi(\overline{n})) >\}$ est définissable dans l'arithmétique élémentaire.
6. La cohérence de l'arithmétique élémentaire est définissable dans l'arithmétique élémentaire.
7. Si l'on ajoute à l'arithmétique de Peano PA un axiome qui énonce la cohérence de PA, on obtient une théorie incohérente ou incomplète.

Exercice 2

Donner un modèle de l'arithmétique élémentaire dans lequel la relation d'ordre est totale mais n'est pas bien fondée. (On rappelle que l'ordre (strict) est défini par $x > y \stackrel{\text{def}}{=} \exists z.z + y = x \wedge x \neq y$ et qu'un ordre est bien fondé s'il n'existe pas de chaine infinie strictement décroissante $x_1 > \cdots > x_n > \cdots$.)
[5 points, 19 lignes]

Exercice 3

On suppose que $\mathcal{F} = \emptyset$ et $\mathcal{P} = \{R(2), = (2)\}$ et la théorie $\mathcal{T}$ engendrée par les axiomes de l'égalité et les axiomes suivants : On suppose que $\mathcal{F} = \emptyset$ et $\mathcal{P} = \{R(2), = (2)\}$ et la théorie $\mathcal{T}$ engendrée par les axiomes de l'égalité et les axiomes suivants :

(ES)	$\forall x \exists y_1, y_2.$	$R(x, y_1) \wedge R(x, y_2) \wedge y_1 \neq y_2$	
(EP)	$\forall x \exists y.$	$R(y, x)$	
(UP)	$\forall x \forall y \forall z.$	$R(x, y) \wedge R(z, y) \rightarrow x = z$	
(US)	$\forall x \forall y_1 \forall y_2 \forall y_3.$	$R(x, y_1) \wedge R(x, y_2) \wedge R(x, y_3) \rightarrow y_1 = y_2 \vee y_1 = y_3 \vee y_2 = y_3$	
(T_n)	$\forall x_1 \forall x_2 \cdots \forall x_n.$	$R(x_1, x_2) \wedge \ldots \wedge R(x_{n-1}, x_n) \rightarrow x_1 \neq x_n$	Pour tout $n \in \mathbb{N}, n > 0$

1. Donner un modèle de $\mathcal{T}$. (**Ind** : on pourra considérer $\mathbb{Z} \times 2^{\mathbb{N}}$)
   [6 lignes, 2 points]
2. Soir $\mathcal{S}$ un modèle de $\mathcal{T}$ et a, b deux éléments du domaine D de $\mathcal{S}$
   (a) Montrer que, pour tout entier n, il existe une unique suite $a = a_0, \ldots a_n \in D$ telle que, pour tout $1 \leq i \leq n$, $(a_i, a_{i-1}) \in R^{\mathcal{S}}$. On note alors $a_n = u_{\mathcal{S}}(a, n)$ et $c \geq_{\mathcal{S}} a$ ssi il existe un n tel que $c = u_{\mathcal{S}}(a, n)$.
   (b) Montrer que si $c \geq_{\mathcal{S}} a$, alors il existe un unique entier n (noté $d_{\mathcal{S}}(a, c)$) tel que $c = u_{\mathcal{S}}(a, n)$. Montrer que $\geq_{\mathcal{S}}$ est une relation d'ordre.
   (c) Montrer que, s'il existe c tel que $c \geq_{\mathcal{S}} a$ et $c \geq_{\mathcal{S}} b$, alors il existe un unique d tel que $d \geq_{\mathcal{S}} a$ et $d \geq_{\mathcal{S}} b$ et ($c \geq_{\mathcal{S}} a$ et $c \geq_{\mathcal{S}} b$) ssi $c \geq_{\mathcal{S}} d$. d est noté $\mathsf{lub}_{\mathcal{S}}(a, b)$. Si un tel majorant n'existe pas, par convention, $\mathsf{lub}_{\mathcal{S}}(a, b) = \perp$.
   (d) Montrer que, pour tout entier n, $\{a' \in D \mid d_{\mathcal{S}}(a', a) = n\}$ a pour cardinal 2^n.
   (e) Montrer que si $a \geq_{\mathcal{S}} c$ et $b \geq_{\mathcal{S}} c$, alors $a \geq_{\mathcal{S}} b$ ou $b \geq_{\mathcal{S}} a$.
   [10 lignes, 2 points]
3. Montrer que deux modèles quelconques de $\mathcal{T}$ sont élémentairement équivalents. (**Ind** : on pourra assurer l'invariant suivant dans un jeu de EF en n rondes : pour toute suite $(a_1, b_1), \ldots, (a_k, b_k)$, pour tous i, j, on est dans l'un des cas suivants :
   (a) ($\mathsf{lub}_{\mathcal{S}_1}(a_i, a_j) = \perp$ ou ($d_{\mathcal{S}_1}(a_i, \mathsf{lub}_{\mathcal{S}_1}(a_i, a_j)) > 2^{n-k}$ ou $d_{\mathcal{S}_1}(a_j, \mathsf{lub}_{\mathcal{S}_1}(a_i, a_j)) > 2^{n-k}$)) et ($\mathsf{lub}_{\mathcal{S}_2}(b_i, b_j) = \perp$ ou ($d_{\mathcal{S}_2}(b_i, \mathsf{lub}_{\mathcal{S}_2}(b_i, b_j)) > 2^{n-k}$ ou $d_{\mathcal{S}_2}(b_j, \mathsf{lub}_{\mathcal{S}_2}(b_i, b_j)) > 2^{n-k}$))
   (b) $d_{\mathcal{S}_1}(a_i, \mathsf{lub}_{\mathcal{S}_1}(a_i, a_j)) = d_{\mathcal{S}_2}(b_i, \mathsf{lub}_{\mathcal{S}_2}(b_i, b_j))$ et $d_{\mathcal{S}_1}(a_j, \mathsf{lub}_{\mathcal{S}_1}(a_i, a_j)) = d_{\mathcal{S}_2}(b_j, \mathsf{lub}_{\mathcal{S}_2}(b_i, b_j))$
)
   Note : On prendra soin de définir précisément la stratégie du duplicateur. Il est recommandé d'utiliser des figures pour expliquer les différents cas de la preuve que cette stratégie satisfait l'invariant.
   [50 lignes, 5 points]
4. Que peut-on en conclure sur la théorie ?
   [1 ligne, 1 point]

Solution

Exercice 2

On considère un modèle dans lequel on a une copie de $\mathbb{N}$ et une copie de $\mathbb{Z}$. On note les éléments de $\mathbb{N}$ préfixés par la lettre n et les éléments de $\mathbb{Z}$ préfixés par la lettre z. Si $n \in \mathbb{N}$, on note z_n l'élément correspondant de $\mathbb{Z}$. Les opérations sont définies comme suit : 0 est interprété comme $0_{\mathbb{N}}$. $S(n), n + n', n \times n'$ sont les opérations de $\mathbb{N}$. $S(z), z + z', z \times z'$ sont les opérations de $\mathbb{Z}$. $n + z$ est défini comme $z_n + z$, de même pour $z + n$. $0_{\mathbb{N}} \times z = 0_{\mathbb{N}} = z \times 0_{\mathbb{N}}$. $n \times z$ et $z \times n$ sont définies comme $z_n \times z$.

Cette structure satisfait les axiomes de l'arithmétique élémentaire :

(A_1) : le successeur d'un élément de $\mathbb{Z}$ est dans $\mathbb{Z}$ et ne peut donc pas être $0_{\mathbb{N}}$

(A_2) : résulte de cette propriété sur $\mathbb{N}$ et $\mathbb{Z}$ respectivement.

(A_3) : $n + 0_{\mathbb{N}} = n$ et $z + 0_{\mathbb{N}} = z$

(A_4) : la propriété résulte de ces propriétés sur $\mathbb{N}$ et $\mathbb{Z}$ respectivement, sauf dans les deux cas :
- $z + S(n) = z + z_{n+1} = S(z + z_n) = S(z + n)$.
- $n + S(z) = z_n + z + z_1 = S(z_n + z)$

(A_5) par définition

(A_6) la propriété est satisfaite quand les deux arguments sont dans $\mathbb{N}$ (resp. dans $\mathbb{Z}$). Sinon ;
- $n \times s(z) = z_n \times s(z) = z_n \times z + z_n = n \times z + n$
- $z \times s(n) = z \times z_{s(n)} = z \times z_n + z = z \times n + z$

(A_7) si $n \in \mathbb{N}$ et $n \neq 0_{\mathbb{N}}$, alors $n = s(n-1)$. Si $z \in \mathbb{Z}$, $z = s(z-1)$.

Montrons maintenant que $>$ n'est pas bien fondé. Il suffit de remarquer que $z + z_1 > z$.

Exercice 3

1. On considère $\mathbb{Z} \times 2^{\mathbb{N}}$ avec l'interprétation de R suivante : $((z, E), (z', E')) \in R^{\mathcal{S}}$ ssi $z' = z + 1$ et $E = \{n - 1 \mid n \in E', n \neq 0\}$.
   EP et UP sont satisfaits par construction.
   Les axiomes ES et US sont satisfaits : $((z, E), (z', E')) \in R^{\mathcal{S}}$ ssi ($E' = \{n + 1 \mid n \in E\}$ et $z' = z + 1$) ou bien ($E' = \{0\} \cup \{n + 1 \mid n \in E\}$ et $z' = z + 1$).
   T_n est satisfait car $\mathcal{S}, (z_1, E_1), \ldots (z_n, E_n) \models R(x_1, x_2) \wedge \ldots \wedge R(x_{n-1}, x_n)$ entraine $z_n = z_1 + n$ et donc $z_n > z_1$ si $n > 0$.
2. (a) Par récurrence sur n : l'existence est une conséquence de EP, l'unicité est une conséquence de UP.
   (b) Il suffit de montrer l'unicité. Si $c = u_{\mathcal{S}}(a, n) = u_{\mathcal{S}}(a, n')$, supposons sans perte de généralité que $n' \geq n$. Par définition, $u_{\mathcal{S}}(u_{\mathcal{S}}(a, n), n' - n) = u_{\mathcal{S}}(a, n)$. Comme $\mathcal{S} \models T_{n'_n}$ on a nécécessairement $n' = n$.
   $\geq_{\mathcal{S}}$ est réflexive car $a = u_{\mathcal{S}}(a, 0)$
   $\geq_{\mathcal{S}}$ est transitive car $u_{\mathcal{S}}(u_{\mathcal{S}}(a, n), m) = u_{\mathcal{S}}(a, n + m)$
   $\geq_{\mathcal{S}}$ est antisymétrique par transitivité et unicité de n, comme nous l'avons vu ci-dessus.

(c) si $c \geq_{\mathcal{S}} a$ et $c \geq_{\mathcal{S}} b$, $\{n \in \mathbb{N} | u_{\mathcal{S}}(a,n) \geq_{\mathcal{S}} b\}$ est non vide et admet donc un minimum n_0. Si $d = u_{\mathcal{S}}(a, n_0)$, on a bien $d \geq_{\mathcal{S}} a$ et $d \geq_{\mathcal{S}} b$ par construction. De plus, si $e \geq_{\mathcal{S}} a$ et $e \geq_{\mathcal{S}} b$, alors il existe un m tel que $e = u_{\mathcal{S}}(a, m)$. Par construction, $m \geq n_0$ et donc $e \geq_{\mathcal{S}} d$. D'où l'unicité.

(d) Soit $\mathcal{E}_n = \{a' \in D \,|\, d_{\mathcal{S}}(a', a) = n\}$. On montre la propriété par récurrence sur n : si $n = 0$, $\{a' \in D \,|\, d_{\mathcal{S}}(a', a) = 0\} = \{a\}$ est de cardinal $1 = 2^0$. Supposons maintenant que $|\mathcal{E}_n| = 2^n$. Si $x \in \mathcal{E}_{n+1}$, par **??**, il existe un $p(x) \in \mathcal{E}_n$ tel que $(p(x), x) \in R^{\mathcal{S}}$. D'après (ES), p est surjective et d'après (US), pour tout $y \in \mathcal{E}_n$, $|p^{-1}(y)| = 2$. Il en résulte que $|\mathcal{E}_{n+1}| = 2 \times |\mathcal{E}_n| = 2^{n+1}$.

(e) D'après **??**, il existe deux entiers p, q tels que $a = u_{\mathcal{S}}(c, p)$ et $b = u_{\mathcal{S}}(c, q)$. Si $p \geq q$ (par exemple), $a = u_{\mathcal{S}}(u_{\mathcal{S}}(c, q), p - q)$, donc $a = u_{\mathcal{S}}(b, p - q)$ et $a \geq_{\mathcal{S}} b$.

3. dans un jeu en n rondes on montre que le duplicateur peut maintenir l'invariant. On note $a_{ij} = \mathsf{lub}(a_i, a_j)$, $b_{ij} = \mathsf{lub}(b_i, b_j)$. On étend $d_{\mathcal{S}}$ par $d_{\mathcal{S}}(a, a') = +\infty$ si $a = \perp$ ou $a' = \perp$ ou $a \not\geq_{\mathcal{S}} a'$.
   - S'il existe un indice i tel que $a = a_i$, on choisit $b = b_i$ et l'invariant est préservé. Ce cas est désormais écarté.
   - Si, pour tout i, $d_{\mathcal{S}_1}(a, \mathsf{lub}_{\mathcal{S}_1}(a, a_i)) > 2^{n-k-1}$ ou $d_{\mathcal{S}_1}(a_i, \mathsf{lub}_{\mathcal{S}_1}(a, a_i)) > 2^{n-k-1}$, on choisit b tel que, pour tout i, $d_{\mathcal{S}_1}(b_i, \mathsf{lub}_{\mathcal{S}_1}(b, b_i)) > 2^{n-k-1}$ (par exemple en prenant $u_{\mathcal{S}_2}(b_{i_0}, 2^{n-k-1} + 1)$, pour un b_{i_0} maximal pour $\geq_{\mathcal{S}_2}$). L'invariant reste bien satisfait.
   - Sinon, soit $a'_i = \mathsf{lub}(a_i, a)$ pour tout i. L'ensemble des a'_i tels que $d_{\mathcal{S}_1}(a, a'_i) \leq 2^{n-k-1}$ et $d_{\mathcal{S}_1}(a_i, a'_i) \leq 2^{n-k-1}$ est non vide et totalement ordonné pour $\geq_{\mathcal{S}_1}$ (d'après **??**). Soit a'_{i_0} l'élément minimal de cet ensemble.
     Soit $b'_{i_0} = u_{\mathcal{S}_2}(b_{i_0}, d_{\mathcal{S}_1}(a_{i_0}, a'_{i_0}))$. On choisit b tel que $d_{\mathcal{S}_2}(b, b'_{i_0}) = d_{\mathcal{S}_1}(a, a'_{i_0})$ et $b \notin \{b_i | 1 \leq i \leq k\}$. C'est possible puisque (d'après **??**), $\{b' | d_{\mathcal{S}_2}(b', b'_{i_0}) = d_{\mathcal{S}_1}(a, a'_{i_0})\}$ a même cardinal que $\{a' | d_{\mathcal{S}_1}(a', a'_{i_0}) = d_{\mathcal{S}_1}(a, a'_{i_0})\}$ et donc, par l'invariant, $\{b' | d_{\mathcal{S}_2}(b', b'_{i_0}) = d_{\mathcal{S}_1}(a, a'_{i_0})\} \backslash \{b_i | 1 \leq i \leq k\}$ a même cardinal que $\{a' | d_{\mathcal{S}_1}(a', a'_{i_0}) = d_{\mathcal{S}_1}(a, a'_{i_0})\} \backslash \{a_i | 1 \leq i \leq k\}$. En particulier si ce dernier ensemble est non vide, le premier l'est aussi.
     Montrons maintenant que l'invariant est préservé. Soit $1 \leq j \leq k$. Plusieurs cas se présentent :

     Si a_j et a_{i_0} (resp. b_j et b_{j_0}) sont éloignés alors a_j et a (resp. b_j et b) sont éloignés. Plus formellement, montrons que, si $d_{\mathcal{S}_1}(a_j, \mathsf{lub}_{\mathcal{S}_1}(a_j, a_{i_0})) > 2^{n-k}$ ou $d_{\mathcal{S}_1}(a_{i_0}, \mathsf{lub}_{\mathcal{S}_1}(a_j, a_{i_0})) > 2^{n-k}$, alors $d_{\mathcal{S}_1}(a_j, \mathsf{lub}_{\mathcal{S}_1}(a_j, a)) > 2^{n-k-1}$ ou $d_{\mathcal{S}_1}(a, \mathsf{lub}_{\mathcal{S}_1}(a_j, a)) > 2^{n-k-1}$. Nous raisonnons sur la structure $\mathcal{S}_1$, mais par construction de b, le même raisonnement s'applique à la structure $\mathcal{S}_2$.

     Cas 1 : $\mathsf{lub}_{\mathcal{S}_1}(a_j, a_{i_0}) = \perp$. Dans ce cas $\mathsf{lub}_{\mathcal{S}_1}(a, a_j) = \perp$, d'après **??** et puisque $\mathsf{lub}(a, a_{i_0}) \neq \perp$.

     Notons que, de même, si $\mathsf{lub}_{\mathcal{S}_1}(a_j, a_{i_0}) \neq \perp$, alors $\mathsf{lub}_{\mathcal{S}_1}(a, a_j) \neq \perp$ et , d'après **??**, $\mathsf{lub}_{\mathcal{S}_1}(a, a_j)$ et $\mathsf{lub}_{\mathcal{S}_1}(a, a_{i_0})$ sont comparables. Les deux cas suivant considèrent donc les deux ordres possibles entre ces éléments.

     Cas 2 : $\mathsf{lub}_{\mathcal{S}_1}(a, a_j) >_{\mathcal{S}_1} \mathsf{lub}_{\mathcal{S}_1}(a, a_{i_0})$. Dans ce cas, $\mathsf{lub}_{\mathcal{S}_1}(a, a_j) \geq_{\mathcal{S}_1} a_{i_0}, a$, donc $\mathsf{lub}_{\mathcal{S}_1}(a, a_j) \geq_{\mathcal{S}_1} \mathsf{lub}_{\mathcal{S}_1}(a_{i_0}, a_j)$. Par ailleurs, d'après **??**, $\mathsf{lub}_{\mathcal{S}_1}(a, a_{i_0}) \geq_{\mathcal{S}_1} \mathsf{lub}_{\mathcal{S}_1}(a_{i_0}, a_j)$ ou $\mathsf{lub}_{\mathcal{S}_1}(a_{i_0}, a_j) \geq_{\mathcal{S}_1} \mathsf{lub}_{\mathcal{S}_1}(a, a_{i_0})$. Le premier cas n'est pas possible car on aurait $\mathsf{lub}_{\mathcal{S}_1}(a, a_{i_0})$ majore a, a_{i_0}, a_j, ce qui contredit l'hypothèse $\mathsf{lub}_{\mathcal{S}_1}(a, a_j) >_{\mathcal{S}_1} \mathsf{lub}_{\mathcal{S}_1}(a, a_{i_0})$. Dans le deuxième cas, $\mathsf{lub}_{\mathcal{S}_1}(a_{i_0}, a_j)$ majore $a.a_{i_0}, a_j$, donc $\mathsf{lub}_{\mathcal{S}_1}(a_{i_0}, a_j) = \mathsf{lub}_{\mathcal{S}_1}(a_j, a)$.

Si $d_{\mathcal{S}_1}(a_j, \mathsf{lub}_{\mathcal{S}_1}(a_j, a_{i_0})) > 2^{n-k}$, on obtient $d_{\mathcal{S}_1}(a_j, \mathsf{lub}_{\mathcal{S}_1}(a_j, a)) > 2^{n-k} > 2^{n-k-1}$.

Si $d_{\mathcal{S}_1}(a_{i_0}, \mathsf{lub}_{\mathcal{S}_1}(a_j, a_{i_0})) > 2^{n-k}$, alors

$$\begin{array}{rcl} d_{\mathcal{S}_1}(a, \mathsf{lub}_{\mathcal{S}_1}(a_j, a)) & \geq & d_{\mathcal{S}_1}(\mathsf{lub}_{\mathcal{S}_1}(a, a_{i_0}), \mathsf{lub}_{\mathcal{S}_1}(a_j, a)) \\ & \geq & d_{\mathcal{S}_1}(a_{i_0}, \mathsf{lub}_{\mathcal{S}_1}(a_j, a)) - d_{\mathcal{S}_1}(a_{i_0}, \mathsf{lub}_{\mathcal{S}_1}(a, a_{i_0})) \\ & \geq & d_{\mathcal{S}_1}(a_{i_0}, \mathsf{lub}_{\mathcal{S}_1}(a_{i_0}, a_j)) - 2^{n-k-1} \\ & > & 2^{n-k} - 2^{n-k-1} = 2^{n-k-1} \end{array}$$

Cas 3 : $\mathsf{lub}_{\mathcal{S}_1}(a, a_{i_0}) \geq_{\mathcal{S}_1} \mathsf{lub}_{\mathcal{S}_1}(a, a_j)$. Dans ce cas $\mathsf{lub}_{\mathcal{S}_1}(a_{i_0}, a) \geq_{\mathcal{S}_1} \mathsf{lub}_{\mathcal{S}_1}(a_{i_0}, a_j) \geq_{\mathcal{S}_1} a_{i_0}$. Comme $d_{\mathcal{S}_1}(a_{i_0}, \mathsf{lub}_{\mathcal{S}_1}(a_{i_0}, a)) \leq 2^{n-k-1}$, $d_{\mathcal{S}_1}(a_{i_0}, \mathsf{lub}_{\mathcal{S}_1}(a_{i_0}, a_j)) \leq 2^{n-k-1}$. Donc $d_{\mathcal{S}_1}(a_j, \mathsf{lub}_{\mathcal{S}_1}(a_{i_0}, a_j)) > 2^{n-k}$. Par ailleurs, d'après **??**, $\mathsf{lub}_{\mathcal{S}_1}(a, a_j)$ et $\mathsf{lub}_{\mathcal{S}_1}(a_{i_0}, a_j)$ sont comparables.

Si $\mathsf{lub}_{\mathcal{S}_1}(a, a_j) \geq_{\mathcal{S}_1} \mathsf{lub}_{\mathcal{S}_1}(a_{i_0}, a_j)$, alors $d_{\mathcal{S}_1}(a_j, \mathsf{lub}_{\mathcal{S}_1}(a, a_j)) \geq d_{\mathcal{S}_1}(a_j, \mathsf{lub}_{\mathcal{S}_1}(a_{i_0}, a_j)) > 2^{n-k} > 2^{n-k-1}$.

Si $\mathsf{lub}_{\mathcal{S}_1}(a_{i_0}, a_j) \geq_{\mathcal{S}_1} \mathsf{lub}(a, a_j)$, alors

$$d_{\mathcal{S}_1}(a_j, \mathsf{lub}_{\mathcal{S}_1}(a, a_j)) \geq d_{\mathcal{S}_1}(a_j, \mathsf{lub}_{\mathcal{S}_1}(a_j, a_{i_0}) - d_{\mathcal{S}_1}(a, \mathsf{lub}_{\mathcal{S}_1}(a, a_{i_0})) > 2^{n-k} - 2^{n-k-1} = 2^{n-k-1}$$

Si a_j et a_{i_0} (et b_j et b_{j_0}) sont proches : on montre que si $d_{\mathcal{S}_1}(a_j, \mathsf{lub}_{\mathcal{S}_1}(a_j, a_{i_0})) \leq 2^{n-k-1}$ et $d_{\mathcal{S}_1}(a_{i_0}, \mathsf{lub}_{\mathcal{S}_1}(a_j.a_{i_0})) \leq 2^{n-k-1}$, alors $d_{\mathcal{S}_2}(b_j, \mathsf{lub}_{\mathcal{S}_2}(b_j, b_{i_0})) \leq 2^{n-k-1}$ et $d_{\mathcal{S}_2}(b_{i_0}, \mathsf{lub}_{\mathcal{S}_2}(b_j, b_{i_0})) \leq 2^{n-k-1}$

Si $a'_{i_0} \geq_{\mathcal{S}_1} a_j$, par construction de a'_{i_0} (minimalité), $\mathsf{lub}_{\mathcal{S}_1}(a, a_j) = a'_{i_0}$ et $a'_{i_0} \geq_{\mathcal{S}_1} \mathsf{lub}_{\mathcal{S}_1}(a_{i_0}, a_j)$ d'après **??**. Comme par ailleurs $d_{\mathcal{S}_1}(a, a'_{i_0}) = d_{\mathcal{S}_2}(b, b'_{i_0})$ par choix de b et $d_{\mathcal{S}_1}(a_j, a_{i_0 j}) = d_{\mathcal{S}_2}(b_j, b_{i_0 j})$ par l'invariant (noter que $d_{\mathcal{S}_1}(a_j, a_{i_0 j}) \leq d_{\mathcal{S}_1}(a_j, a'_{i_0}) = d_{\mathcal{S}_1}(a_j, a'_j) \leq 2^{n-k-1}$), on a bien la propriété voulue.

Sinon , $a_{i_0 j} \geq_{\mathcal{S}_1} a'_{i_0}$ puisque, d'après **??**, $a_{i_0 j}$ et a'_{i_0} sont comparables et que $a'_{i_0} \not\geq_{\mathcal{S}_1} a_j$. Il en résulte que $a_{i_0,j} \geq_{\mathcal{S}_1} a$ et $a_{i_0 j} \geq_{\mathcal{S}_1} a_j$, donc $a_{i_0 j} \geq_{\mathcal{S}_1} a'_j$. Mais on a aussi $a'_j \geq_{\mathcal{S}_1} a'_{i_0}$ (par minimalité de a'_{i_0}) et donc $a'_j \geq_{\mathcal{S}_1} a_{i_0}$ et $a'_j \geq_{\mathcal{S}_1} a_j$. Donc $a'_j \geq_{\mathcal{S}_1} a_{i_0 j}$. En fin de compte, $a_{i_0 j} = a'_j$. Comme $d_{\mathcal{S}_1}(a, a'_j) \leq 2^{n-k-1}$, $d_{\mathcal{S}_1}(a'_{i_0}, a'_j) \leq 2^{n-k-1}$ et donc $d_{\mathcal{S}_1}(a_{i_0}, a_{i_0 j}) \leq d_{\mathcal{S}_1}(a_{i_0}, a'_{i_0}) + d(a'_{i_0}, a'_j) \leq 2^{n-k-1} + 2^{n-k-1} = 2^{n-k}$. D'après l'invariant, on a donc $d_{\mathcal{S}_2}(b_{i_0}, b_{i_0 j}) = d_{\mathcal{S}_1}(a_{i_0}, a_{i_0 j})$. Comme, par construction, $d_{\mathcal{S}_1}(a_{i_0}, a'_{i_0}) = d_{\mathcal{S}_2}(b_{i_0}, b'_{i_0})$, on en déduit que $d_{\mathcal{S}_2}(b'_{i_0}, b_{i_0 j}) = d_{\mathcal{S}_1}(a'_{i_0}, a_{i_0 j})$. Comme enfin, par construction encore, $d_{\mathcal{S}_1}(a, a'_{i_0}) = d_{\mathcal{S}_2}(b, b'_{i_0})$, on obtient

$$d_{\mathcal{S}_1}(a, a'_j) = d_{\mathcal{S}_1}(a, a_{i_0 j}) = d_{\mathcal{S}_1}(a, a'_{i_0}) + d_{\mathcal{S}_1}(a'_{i_0}, a_{i_0 j}) = d_{\mathcal{S}_2}(b, b'_{i_0}) + d_{\mathcal{S}_2}(b'_{i_0}, b_{i_0 j}) = d_{\mathcal{S}_2}(b, b'_j)$$

Par ailleurs, $d_{\mathcal{S}_1}(a_j, a_{i_0 j}) = d_{\mathcal{S}_2}(b_j, b_{i_0 j})$ (par l'invariant) et donc $d_{\mathcal{S}_1}(a_j, a'_j) = d_{\mathcal{S}_2}(b_j, b'_j)$, ce qui termine la preuve de l'invariant.

4. La théorie $\mathcal{T}$ est complète d'après un résultat du cours.