Logique 2021
Devoir à la Maison #1

David Baelde

Ceci est la version finale et corrigée de l'énoncé.
Le devoir était à rendre avant le 10 mars à midi, sous la forme d'un PDF composé en LaTeX, par email à David Baelde. Pour rappel, les devoirs maison sont notés et remplaceront au moins en partie les épreuves sur table cette année.
Vous pouvez travailler le DM en groupe, mais j'attends des rendus rédigés individuellement.
Dans l'énoncé, la substitution de x par t dans A est notée $A\{x \mapsto t\}$ mais j'accepte toute notation usuelle dans vos copies. Tâchez de concentrer votre effort de rédaction sur les points intéressants ; à titre indicatif, aucune question ne justifie de réponse faisant plus d'une page.

1 Axiomes et calculs pour l'arithmétique

La *déduction naturelle modulo* s'obtient en ajoutant aux règles de la déduction naturelle classique la règle de déduction modulo

$$\frac{\Gamma \vdash B \quad A \equiv B}{\Gamma \vdash A}$$

où $\equiv$ est une *congruence* sur les termes et les formules du langage. Une congruence est une relation d'équivalence qui passe au contexte. Concrètement, on demande donc que :

- pour tout symbole de fonction n-aire, $f(t_1, \ldots, t_n) \equiv f(t'_1, \ldots, t'_n)$ quand $t_i \equiv t'_i$ pour tout $i \in [1; n]$;
- pour tout connecteur propositionnel binaire $\star$, on a $A \star B \equiv A' \star B'$ quand $A \equiv A'$ et $B \equiv B'$;
- pour tout quantificateur $\mathcal{Q}$, on a $\mathcal{Q}x.A \equiv \mathcal{Q}x.A'$ quand $A \equiv A'$.

Axiomes de réflexivité et schéma de Leibniz :

$$\forall x.\ x = x \qquad \forall x, y.\ x = y \Rightarrow A\{z \mapsto x\} \Rightarrow A\{z \mapsto y\}$$

Schéma d'induction :

$$A\{z \mapsto 0\} \Rightarrow (\forall x.\ A\{z \mapsto x\} \Rightarrow A\{z \mapsto s(x)\}) \Rightarrow \forall x.\ A\{z \mapsto x\}$$

Axiomes 3 et 4 de Peano :

$$\forall x.\ 0 \neq s(x) \qquad \forall x, y.\ s(x) = s(y) \Rightarrow x = y$$

Axiomes sur l'addition et la multiplication :

$$\begin{array}{ll} \forall y.\ 0 + y = y & \forall x, y.\ s(x) + y = s(x + y) \\ \forall y.\ 0 \times y = 0 & \forall x, y.\ s(x) \times y = (x \times y) + y \end{array}$$

FIGURE 1 – Les axiomes de Peano

On supposera de plus que $\equiv$ est préservée par l'application d'une substitution, et donc en particulier par renommage des variables.

Dans cette exercice nous considérerons des dérivations en déduction naturelle usuelle utilisant l'axiomatique de Peano PA, qu'on rappelle en Figure 1. Plutôt que d'expliciter l'utilisation des axiomes via la composante Γ des séquents, on pourra considérer qu'on a une seconde règle d'axiome qui permet de dériver $\Gamma \vdash A$ quand A est un axiome de la théorie considérée. On explicitera la théorie en annotant les séquents, en écrivant par exemple $\Gamma \vdash_{PA} A$.

On considèrera d'autre part la *théorie calculatoire* C donnée en Figure 2, qui spécifie un ensemble d'axiomes et une congruence $\equiv$. On écrira $\Gamma \vdash_C A$ quand le séquent est dérivable en déduction modulo en utilisant ces axiomes (via la règle axiome étendue comme ci-dessus) et la règle de déduction modulo la congruence donnée par C.

Question 1
Montrer que la relation $\equiv$ définie en Figure 2 coincide avec la relation $\sim$ définie inductivement par les règles suivantes, où f, $\star$ et $\mathcal{Q}$ sont des symboles quelconques comme plus haut :

$$\frac{}{u \sim u} \qquad \frac{v \sim u}{u \sim v} \qquad \frac{u \sim u' \quad u' \sim u''}{u \sim u''}$$

La théorie calculatoire C est donnée par le schéma d'induction (comme dans PA) et la relation $\equiv$ définie comme la plus petite congruence satisfaisant, pour tous termes u et v :

$$\begin{array}{rcl@{\qquad\qquad}rcl} 0=0 & \equiv & \top & 0+u & \equiv & u \\ s(u)=s(v) & \equiv & u=v & 0\times u & \equiv & 0 \\ 0=s(v) & \equiv & \bot & s(u)+v & \equiv & s(u+v) \\ s(u)=0 & \equiv & \bot & s(u)\times v & \equiv & (u\times v)+v \end{array}$$

FIGURE 2 – Théorie calculatoire de l'arithmétique

$$\frac{t_1 \sim t'_1 \quad \dots \quad t_n \sim t'_n}{f(t_1,\dots,t_n) \sim f(t'_1,\dots,t'_n)} \qquad \frac{A \star A' \quad B \star B'}{A \star B \sim A' \star B'} \qquad \frac{A \sim A'}{\mathcal{Q}x.A \sim \mathcal{Q}x.A'}$$

$\dfrac{}{0=0 \sim \top}$ et de même pour les autres conditions sur $\equiv$ de la Figure 2.

Correction 1

Il y a eu ici quelques incompréhensions sur la notion de congruence, oubli du passage au contexte, et plusieurs solutions consistant à dire "c'est évident, les relations satisfont les mêmes règles" ce qui ne convient pas car j'attendais des arguments formels basés sur la définition précise de chaque relation.

On montre que $u \sim v$ entraîne $u \equiv v$ par induction sur la dérivation de $u \sim v$. Tous les cas sont immédiats, par définition de $\equiv$. D'autre part, $\sim$ est une congruence [1] qui satisfait les équations de la Figure 2, donc par minimalité de $\equiv$ on a que $u \equiv v$ entraîne $u \sim v$.

Question 2

Montrer que, si $\Gamma \vdash_C A$ est dérivable en déduction modulo, alors $\Gamma \vdash_{PA} A$ est dérivable en déduction naturelle. On privilégiera une approche sémantique, en montrant d'abord que tout ce qui est démontrable dans $\vdash_C$ est correct dans les modèles égalitaires de PA.

Correction 2

Le corrigé ci-dessous suit une approche sémantique. Vous avez généralement suivi une approche syntaxique qui est tout aussi simple (si l'on se permet de ne pas détailler les dérivations faites au moyen des axiomes de PA) : on montre que $u \equiv v$ entraîne la dérivabilité de $\vdash_{PA} u = v$ pour des termes u et v, et que $A \equiv B$ entraîne la dérivabilité de $\vdash_{PA} A \Leftrightarrow B$ pour des propositions A et B. Il ne fallait par contre

1. Par définition c'est une relation d'équivalence qui passe au contexte. On montre aisément que la relation est préservée par substitution : je n'ai pas sanctionné les oublis sur ce point.

surtout pas mélanger déduction et congruences : par exemple, $\Gamma \vdash_C u \sim v \Rightarrow u = v$ *n'a aucun sens.*

Pour montrer que $\vdash_C$ est incluse dans $\vdash_{PA}$, il suffit par complétude de la déduction naturelle de montrer que tout ce qui est dérivable dans C est satisfait dans tous les modèles de PA. On a vu qu'on peut, de façon équivalente, ne considérer que les modèles égalitaires et bivalués de PA.

On cherche donc à montrer que ce qui est dérivable dans C est satisfait dans les modèles égalitaires de PA : on considère une dérivation de $\Gamma \vdash_C A$, un M un modèle égalitaire bivalué de PA et σ une valuation tel que $[\![B]\!]_\sigma = 1$ pour tout $B \in \Gamma$, et on montre que $[\![A]\!]_\sigma = 1$. On procède par induction sur la structure de la dérivation. Le cas de l'axiome est immédiat, que ce soit quand $A \in \Gamma$ ou quand A est un axiome de C et donc aussi de PA. Le cas des règles autres que la déduction modulo est immédiat : on a vu qu'elles sont correctes (si les prémisses sont valides alors la conclusion l'est) et le même argument nous donne la validité pour les modèles égalitaires de PA.

Pour la règle de déduction modulo nous allons montrer que $[\![A]\!]_\sigma = [\![B]\!]_\sigma$ quand $A \equiv B$. Il suffit de vérifier que les générateurs de la congruence préservent l'interprétation dans ces modèles :

- $[\![0 = 0]\!]_M = 1 = [\![\top]\!]_M$ (réflexivité)
- $[\![s(u) = s(v)]\!]^\sigma_M = [\![u = v]\!]^\sigma_M$ (axiome 4 + modèle égalitaire)
- $[\![s(u) = 0]\!]^\sigma_M = [\![\bot]\!]$ (axiome 3)
- $[\![0 = s(u)]\!]^\sigma_M = [\![\bot]\!]$ (axiome 3 + modèle égalitaire)
- $[\![0 + u]\!]^\sigma_M = [\![u]\!]^\sigma_M$ (axiome de l'addition + modèle égalitaire)
- $[\![s(u) + v]\!]^\sigma_M = [\![s(u + v)]\!]^\sigma_M$ (axiome de l'addition + modèle égalitaire)
- etc.

Question 3

Montrer que les formules suivantes sont dérivables en déduction modulo avec la théorie calculatoire de l'arithmétique :

- $\forall x.\ x = x$
- $\forall x.\ x = 0 \vee \exists y.\ x = s(y)$
- $\forall x, y.\ x = y \Rightarrow y = x$
- $\forall x, y, z.\ x = y \Rightarrow y = z \Rightarrow x = z$

On veillera à préciser quels axiomes et congruences sont utilisés, et à donner les grandes étapes de la construction d'une dérivation, mais il n'est pas nécessaire de dessiner ne serait-ce qu'un morceau d'arbre de preuve.

Correction 3

Je n'exigeais pas ici des dérivations détaillées, par contre beaucoup de copies prenaient quand même trop de libertés avec le formalisme. Je n'ai pas sanctionné quand

il n'y avait pas de contre-sens clair, mais il est de bon ton d'au moins écrire les séquents qu'on dérive. Sinon, on peut s'inquiéter de confusions entre "le séquent $\phi \vdash \psi$ est dérivable" et "si $\vdash \phi$ est dérivable alors $\vdash \psi$ aussi"; ou bien, entre la dérivabilité et la vérité mathématique.

Pour la première, on utilise le schéma d'induction sur $x = 0 \vee \exists y.\ x = s(y)$. On conclut aisément sans même utiliser l'hypothèse d'induction.

Pour la réflexivité on utilise encore le schéma d'induction sur $x = x$. On démontre aisément $0 = 0$ puisque cette formule se réécrit en $\top$. Pour l'hérédité, $s(x) = s(x)$ se réécrit en $x = x$, l'hypothèse d'induction.

Pour la transitivité il faut d'abord montrer $0 = y \Rightarrow y = z \Rightarrow 0 = z$. On procède par induction sur y. On prouve aisément $0 = 0 \Rightarrow 0 = z \Rightarrow 0 = z$. Il n'y a rien à montrer quand y est un successeur car $0 = s(y')$ se réécrit en $\bot$. On veut ensuite montrer $s(x) = y \Rightarrow y = z \Rightarrow s(x) = z$, en supposant la même chose mais pour x. C'est évident si y vaut 0. Sinon cela se réécrit en $x = y' \Rightarrow s(y') = z \Rightarrow s(x) = z$ puis après étude de cas sur z en $x = y' \Rightarrow y' = z' \Rightarrow x = z'$ notre hypothèse d'induction.

Question 4

Montrer que, pour tout terme t, la formule suivante est dérivable en déduction modulo avec la théorie calculatoire de l'arithmétique :

$$\forall x, y.\ x = y \Rightarrow t\{z \mapsto x\} = t\{z \mapsto y\}$$

Correction 4

Cette question a été assez bien traitée. Quelques copies ont oublié les symboles de fonction $+$ et $\times$, peut être par confusion entre syntaxe et sémantique canonique. J'attendais l'identification de lemmes nécessaires pour ces symboles, mais pas leurs preuves détaillées.

On procède par induction sur t pour montrer que le jugement $x = y \vdash t(x) = t(y)$ est dérivable. Si t est restreint à z, on produit aisément une dérivation, réduite à la règle axiome. Si t est une autre variable, ou la constante 0 on conclut par réflexivité de l'égalité. Pour tous les autres cas on conclut par hypothèse(s) d'induction(s) en utilisant des lemmes intermédiaires :

- Pour tout u et u', $u = u' \Rightarrow s(u) = s(u')$ se dérive aisément par congruence puis axiome.
- Pour tous u, v, u', v' on dérive $u = u' \Rightarrow v = v' \Rightarrow u + v = u' + v'$. Pour cela on utilise le schéma d'induction avec la formule $\forall u'.\ z = u' \Rightarrow v = v' \Rightarrow u + v = u' + v'$.
  - On sait en effet dériver $\forall u'.\ 0 = u' \Rightarrow v = v' \Rightarrow 0 + v = u' + v'$. Après avoir introduit u' on va faire une étude de cas dessus (question

3) et utiliser $(0 = s(u'') \equiv \bot)$ pour exclure un cas, et dans l'autre cas on se ramènera par congruence à $v = v' \vdash v = v'$.

— Dérivons ensuite $H \vdash \forall u'.\ s(u) = u' \Rightarrow v = v' \Rightarrow s(u) + v = u' + v'$ où H est $\forall u'.\ \ u = u' \Rightarrow v = v' \Rightarrow u + v = u' + v'$. On procède de nouveau par étude de cas sur u' après l'avoir introduit : il doit être de la forme $s(u'')$. Par congruence on se ramène à

$$H, u = u'', v = v' \vdash u + v = u'' + v'$$

ce qui permet de conclure en instanciant la quantification universelle de H par u''.

— Le cas de la multiplication est similaire.

Question 5

Montrer que, pour toute formule A, la formule suivante est dérivable en déduction modulo avec la théorie calculatoire de l'arithmétique :

$$\forall x, y.\ \ x = y \Rightarrow A\{z \mapsto x\} \Rightarrow A\{z \mapsto y\}$$

Correction 5

Question bien traitée, mais souvent avec peu de détails. Les cas intéressants étaient la négation et les quantificateurs, mais j'ai donné les points même quand ils n'étaient traités qu'en survol.

On montre, par induction sur A, que le jugement suivant est dérivable :

$$x = y, A(x) \vdash A(y)$$

— Si A est une constante propositionnelle, c'est à dire $\top$ ou $\bot$, c'est évident.

— Si $A(z)$ est atomique, c'est à dire de la forme $t(z) = t'(z)$, on utilise la question précédente qui nous permet de dériver $x = y \vdash t(x) = t(y)$ et $x = y \vdash t'(x) = t'(y)$. On en déduit $x = y, t(x) = t'(x) \vdash t(y) = t'(y)$ par symétrie et transitivité (question 3).

— Si A est une conjonction $A_1 \wedge A_2$, on procède ainsi :

$$\dfrac{\dfrac{\dfrac{x = y, A_1(x) \vdash A_1(y)}{x = y \vdash A_1(x) \Rightarrow A_1(y)} \quad \dfrac{\overline{x = y, A_1(x) \wedge A_2(x) \vdash A_1(x) \wedge A_2(x)}}{x = y, A_1(x) \wedge A_2(x) \vdash A_1(x)}}{x = y, A_1(x) \wedge A_2(x) \vdash A_1(y)} \quad \dots}{x = y, A_1(x) \wedge A_2(x) \vdash A_1(y) \wedge A_2(y)}$$

La sous-dérivation droite est symétrique de la gauche. Dans la gauche, on a utilisé l'affaiblissement, admissible. Le jugement $x = y, A_1(x) \vdash A_1(y)$ est dérivable par hypothèse d'induction sur A_1.

— Le cas de la disjonction est similaire, il faut juste éliminer avant d'introduire :

$$\dfrac{\dfrac{}{\ldots \vdash A_1(x) \vee A_2(x)} \quad \dfrac{x = y, A_1(x) \vdash A_1(y)}{x = y, A_1(x) \vdash A_1(y) \vee A_2(y)} \quad \ldots}{x = y, A_1(x) \vee A_2(x) \vdash A_1(y) \vee A_2(y)}$$

— Pour l'implication, on procède ainsi :

$$\dfrac{\dfrac{(1)}{x = y \vdash A_2(x) \Rightarrow A_2(y)} \quad \dfrac{\dfrac{}{\ldots \vdash A_1(x) \Rightarrow A_2(x), A_1(y)} \quad \dfrac{(2)}{x = y, A_1(y) \vdash A_1(x)}}{x = y, A_1(x) \Rightarrow A_2(x), A_1(y) \vdash A_2(x)}}{\dfrac{x = y, A_1(x) \Rightarrow A_2(x), A_1(y) \vdash A_2(y)}{x = y, A_1(x) \Rightarrow A_2(x) \vdash A_1(y) \Rightarrow A_2(y)}}$$

On obtient (1) par hypothèse d'induction et de même pour (2), après utilisation de la symétrie de l'égalité.

— On peut se passer de traiter explicitement la négation, en considérant qu'elle est définie à partir de l'implication. Sinon, son traitement est similaire aux cas précédents.

— Si A est de la forme $\forall w.A$, on peut supposer (quitte à alpha-renommer) que w est distinct de x et y. On procède ainsi :

$$\dfrac{\dfrac{}{x = y \vdash A_1(x) \Rightarrow A_1(y)} \quad \dfrac{\dfrac{}{\ldots, \forall w.A_1(x) \vdash \forall w.A_1(x)}}{\ldots, \forall w.A_1(x) \vdash A_1(x)}}{\dfrac{x = y, \forall w.A_1(x) \vdash A_1(y)}{x = y, \forall w.A_1(x) \vdash \forall w.A_1(y)}}$$

— Enfin, quand A est de la forme $\exists w.A$, en supposant encore w distinct de x et y, on utilise la dérivation suivante :

$$\dfrac{\dfrac{}{\ldots \vdash \exists w.A_1(x)} \quad \dfrac{x = y, A_1(x) \vdash A_1(y)}{x = y, A_1(x) \vdash \exists w.A_1(y)}}{x = y, \exists w.A_1(x) \vdash \exists w.A_1(y)}$$

Question 6

Conclure que toutes les conséquences de l'arithmétique de Peano sont prouvables dans la théorie calculatoire de l'arithmétique.

Correction 6

Les axiomes sur l'égalité, l'addition et la multiplication sont directement prouvés grâce à la congruence. L'axiome de réflexivité a été montré dérivable, ainsi que le schéma d'axiomes de Leibniz.

2 Calculs monadiques des prédicats

Dans cet exercice on suppose que le langage ne comporte qu'une sorte. Pour les preuves d'indécidabilité, il faudra réduire des problèmes indécidables connus ; veillez à mentionner les étapes clé de l'argument, et à précisément décrire l'encodage utilisé. Pour la preuve de décidabilité, vous pourrez vous inspirerer du dernier TD de février ; ici encore, j'attends la description précise de la technique de preuve utilisée (e.g. quel énoncé intermédiaire est prouvé par induction sur quoi) mais la rédaction détaillée des cas évidents est inutile.

Question 7
Montrer l'indécidabilité de la validité dans le calcul des prédicats équipé d'un unique symbole de prédicat, d'arité 2, quand tous les symboles de fonction sont unaires. (Indice : on peut restreindre le symbole de prédicat à être l'égalité.)

Correction 7
La plupart (toutes ?) les copies ont encodé PCP, à contre-sens de mon indication puisque dans ce cas la relation à exprimer est que deux mots identiques non vides peuvent être engendrés par une succession de dominos. Quelques tentatives d'encodage de PCP où les termes représentaient des paires de mots, ou pire, ont eu tendance à échouer : il fallait rester simple, avec des termes qui représentent des mots. Quelques solutions ont produit une formule qui n'était pas du premier ordre (quantification sur une fonction) : attention ! Dans tous les cas, j'attendais des arguments clairs pour montrer l'équivalence de la validité (ou satisfaisabilité) de la formule encodée et de l'existence d'une solution à l'instance du probème considérée au départ.

On peut encoder le problème du mot. Etant donné un alphabet Σ on se donne un symbole de fonction unaire $\overline{a}(\_)$ pour chaque $a \in \Sigma$. Quand u est un mot $a_1 \dots a_n$, on note $\overline{u}(x)$ pour $a_1(a_2(\dots a_n(x)))$. En particulier, $\overline{\epsilon}(x)$ est x.

Étant donné une instance du problème du mot, i.e. un ensemble d'équations $u_i = v_i$ pour $i \in [1; n]$ et deux mots u et v, on calcule les formules suivantes, où l'on utilise le symbole binaire d'égalité sous sa notation usuelle :

$$\phi \stackrel{\text{def}}{=} \bigwedge_i \forall x.\ \overline{u_i}(x) = \overline{v_i}(x) \qquad \psi \stackrel{\text{def}}{=} \forall x.\ \overline{u}(x) = \overline{v}(x)$$

On considère enfin la théorie de l'égalité :

$$\begin{array}{rl} \mathsf{Eq} \stackrel{\text{def}}{=} & (\forall x.\ x = x) \wedge (\forall x, y.\ x = y \Rightarrow y = x) \wedge \\ & (\forall x, y, z.\ x = y \Rightarrow y = z \Rightarrow x = z) \wedge \\ & \bigwedge_{a \in \Sigma} \forall x, y.\ x = y \Rightarrow \overline{a}(x) = \overline{a}(y) \end{array}$$

Nous allons montrer que l'instance est positive ssi la formule $\phi \wedge \mathsf{Eq} \Rightarrow \psi$ est valide. Le problème du mot étant indécidable, notre problème de validité doit aussi l'être.

Si l'instance est positive, on sait transformer u en v par une série de conversions, et on saura dériver $\phi, \mathsf{Eq} \vdash \psi$. La théorie Eq est ici cruciale.

Pour l'autre direction on considère un modèle canonique, avec comme individus les mots de Σ^*, où $\hat{a} = w \mapsto a.w$ et où l'égalité est interprétée comme la congruence (relation de convertibilité) induite par les équations $u_i = v_i$. Ce modèle satisfait ϕ et Eq. Si $\phi \wedge \mathsf{Eq} \Rightarrow \psi$ est valide, alors notre modèle canonique satisfait ψ et, en interprétant x comme le mot vide, on obtient que u et v sont convertibles, i.e. l'instance du problème du mot est positive.

Question 8

Montrer l'indécidabilité de la validité dans le calcul des prédicats quand tous les symboles de prédicats sont unaires, à l'exception d'un unique symbole de relation binaire. (Lire la question suivante : on ne peut pas restreindre le symbole de prédicat binaire à être l'égalité.)

Correction 8

Ici, je n'avais pas prévu que la généralisation possible du théorème de Church, mentionnée en cours, donnerait lieu à des solutions. C'était possible, et cela a parfois été bien fait, mais souvent les solutions se perdent dans la foule de détails. Point important : il ne fallait pas oublier d'include dans l'encodage les axiomes de l'arithmétique de Robinson, reformulés dans le langage restreint.

On encode PCP, avec tuile de départ fixée : on considère donc une instance composée des dominos $(P_i)_{i\in[1;n]}$ et $(Q_j)_{j\in[1;m]}$. On note $n(i)$ la longueur du domino P_i ; $m(j)$ pour Q_j. On va caractériser l'arbre des développement possibles de dominos, au moyen de prédicats $P_i^j(x)$ (resp. $Q_i^j(x)$) indiquant qu'une position x est couverte par la position j du domino P_i (resp. Q_i).

Encodage, pour tous i, j, k :

— $\exists x.\ P_0^0(x) \wedge Q_0^0(x)$

— $\forall x.\ \ P_i^k(x) \Rightarrow \exists y.\ x \sim y \wedge P_i^{k+1}(y)$ si P_i de longueur supérieure à k

— $\forall x.\ \ P_i^k(x) \Rightarrow \exists y.\ x \sim y \wedge P_j^0(y)$ si P_i de longueur k

— de même avec Q

— exactement un P et un Q par position x

On considère toutes ces formules réunies dans Γ et on vérifie que l'instance est positive ssi le séquent suivant est valide :

$$\Gamma \vdash \bigvee_{i,j} \exists x.\ \ P_i^{n(i)}(x) \wedge Q_j^{m(j)}(x)$$

Question 9
Montrer la décidabilité de la validité dans le calcul des prédicats avec égalité, sans symboles de fonction, et uniquement des symboles de prédicats unaires. (Indice : montrer que si une formule de ce langage a un modèle, elle en a un avec un domaine de cardinal au plus $n2^k$ où k est le nombre de prédicats unaires utilisé et n le nombre de variables utilisées.)

Correction 9
L'énoncé aurait pu être plus explicite : on suppose que le prédicat d'égalité satisfait les axiomes de l'égalité, ou bien plus simplement qu'il est interprété comme l'égalité. Je choisis la deuxième approche dans le corrigé. Cette question a été peu traitée, et parmi les tentatives des erreurs ont été faites. Bravo à ceux qui ont marqué des points ici !

On fixe ϕ, avec pour ensemble de variables X de cardinal n. Étant donné un modèle M de domaine D, on note $\sim$ la relation d'équivalence induite sur D par les $\hat{p_i}$: deux individus sont équivalents si les $\hat{p_i}$ concordent dessus. On construit M' de domaine D' en gardant n éléments arbitraires par classe d'équivalence modulo $\sim$; quand une classe est de cardinal inférieur à n on en garde tous les éléménts. L'interprétation de chaque symbole de prédicat dans M' est la restriction de son interprétation dans M.

Pour $\sigma : X \to D$ et $\sigma' : X \to D'$ on note $\sigma \sim \sigma'$ quand :
- pour tout $x \in X$ on a $\sigma(x) \sim \sigma(x')$;
- pour tout $x, y \in X$ on a $\sigma(x) = \sigma(y)$ ssi $\sigma'(x) = \sigma'(y)$.

On montre alors que, pour tout $\sigma \sim \sigma$ et tout ϕ sur X, on a $M, \sigma \models \phi$ ssi $M', \sigma' \models \phi$. La seule étape intéressante est celle des quantificateurs, et les deux cas sont symétriques. Considérons donc ϕ de la forme $\forall x.\psi$.

- Supposons $M, \sigma \models \phi$ et montrons $M', \sigma' \models \phi$. On considère donc un élément $v' \in D'$ et on doit établir $M', \sigma'\{x \mapsto v'\} \models \psi$. On pourra conclure par hypothèse d'induction si l'on trouve $v \in D$ tel que $\sigma\{x \mapsto v\} \sim \sigma'\{x \mapsto v'\}$. Si $v' = \sigma'(y)$ pour un $y \neq x$, on prend $v := \sigma(y)$; sinon on prend $v := v'$. On vérifie aisément que ce choix convient.
- Supposons maintenant $M', \sigma' \models \phi$. Soit $v \in D$, montrons $M, \sigma\{x \mapsto v\} \models \psi$. Il nous faut un v' tel que $\sigma\{x \mapsto v\} \sim \sigma'\{x \mapsto v'\}$ pour conclure par hypothèse d'induction. S'il existe $y \neq x$ tel que $\sigma(y) = v$, on prend $v' := \sigma'(y)$. Sinon on prend un élément arbitraire $v' \sim v$ qui soit différent de $\sigma'(y)$ pour tout $y \neq x$ tel que $\sigma(y) \sim v$: il en existe un par construction de D' puisque la classe d'équivalence de v dans D comporte au moins autant d'éléments qu'il y a de variables dans $\{y \in X \mid \sigma(y) \sim v\}$. On

vérifie alors que pour tout z on a $v = \sigma(z)$ ssi $v' = \sigma'(z)$: si $\sigma(z) \not\sim v$ alors, puisque $\sigma(z) \sim \sigma'(z)$, on aura $\sigma'(z) \not\sim v'$ et donc ni $v = \sigma(z)$ ni $v' = \sigma'(z)$; si $z = x$, c'est évident ; sinon on avait $v \neq \sigma(z)$ et on a assuré $v' \neq \sigma'(z)$.