Élimination des quantificateurs en langage fini

Vincent Clapiès

27 septembre 2003

1 Introduction

La structure $(\mathbb{N}, +\ , \times\ ,0,1, =)$ n'élimine pas les quantificateurs. Et le résultat reste vrai si on ajoute au langage un nombre fini de symboles.

Peut-on alors trouver une structure contenant (en un sens que l'on précisera ultérieurement) $(\mathbb{N}, +\ , \times\ ,0,1, =)$, et qui élimine les quantificateurs?

La réponse est oui, et même en fait quelque soit la structure de départ.

1.1 Rappels

Définition 1.1. on dit qu'une $\mathcal{L}$-structure $\mathcal{M}$ élimine les quantificateurs si quelque soit la formule $\phi(\overline{x})$ (à variables libres parmi $\overline{x} = x_1, \ldots ,x_n$), il existe une formule $\psi(\overline{x})$ sans quantificateur telle que $\mathcal{M} \models \forall\overline{x}, (\phi(\overline{x}) \Leftrightarrow \psi(\overline{x}))$

Exemple 1.2. $(\mathbb{R}, +\ , \times\ ,0,1, \leqslant\ , =)$ élimine les quantificateurs.

(comme en fait tous les corps réels clos)

Exemple 1.3. $(\mathbb{C}, +\ , \times\ ,0,1, =)$ élimine les quantificateurs.

(comme en fait tous les corps algébriquement clos)

Exemple 1.4. les algèbres libres de termes:

pour un ensemble B quelconque, on définit l'ensemble A constitués des éléments de B auxquels on ajoute des successeurs: $x,S(x),S^2(x),\ldots,S^n(x),\ldots$ (pour x parcourant B)

On définit sur A une fonction prédécesseur P par $P(x) = y$ si $x = S(y)$, et $P(x) = x$ si $x \in A$.

Alors $(A,S,P, =)$ élimine les quantificateurs.

Tous ces exemples sont détaillés dans [1].

1.2 $\mathbb{N}$ n'élimine pas les quantificateurs

Voici donc le théorème énoncé en introduction:

Théorème 1. *soit un $\mathcal{F}$ un ensemble fini de fonctions, constantes et relations. Alors* $(\mathbb{N}, +, \times, 0,1,\mathcal{F}, =)$ *n'élimine pas les quantificateurs.*

Démonstration. Supposons dans un premier temps que l'on dispose d'une appartenance $\in$ (i.e qui puisse s'écrire par une formule du langage).

La structure $(\mathbb{N}, \in, =)$ est donc supposée vérifier les axiomes de la théorie des ensembles (voir [4]), sauf bien sûr l'axiome de l'infini, qu'elle nie bien évidemment.

On est donc en mesure de "coder" les couples (x,y) (par $\{\{x\},\{x,y\}\}$), puis les n-uples, puis les énoncés (en associant un entier à chaque symbole du langage et à chaque symbole logique, et en disant qu'une formule est une suite d'entiers), puis les formules à une variable libre (en rajoutant un entier pour coder la variable libre), etc...

On peut maintenant écrire la formule $V(x,y)$ qui dit: x est le code d'une formule à une variable libre, sans quantificateurs, et qui est satisfaite par y.

Pour cela, on dit:

- il existe des formules $\phi_0, \ldots, \phi_n$ telles que:

- $\phi_n = x$

- toute formule ϕ_i est soit atomique, soit de la forme $\neg\phi_j$, $\phi_j \wedge \phi_k$ ou $\phi_j \vee \phi_k$

- il existe des booléens $\varepsilon_0, \ldots, \varepsilon_n$ tels que:

- si ϕ_i est atomique, alors ε_i est la valeur de vérité de ϕ_i dans laquelle on a remplacé la variable libre par y

(c'est ici que l'on a besoin de travailler avec un langage fini, car pour tester une formule atomique, on doit rajouter de nouveaux paramètres qui joueront le rôle des sous-termes, et écrire la conversion "entier $\leftrightarrow$ symbole qu'il représente" pour chacun des symboles)

- si ϕ_i est de la forme $\neg\phi_j$, alors ε_i vaut $1 - \varepsilon_j$

- si ϕ_i est de la forme $\phi_j \wedge \phi_k$, alors ε_i vaut $min(\varepsilon_j,\varepsilon_k)$

- si ϕ_i est de la forme $\phi_j \vee \phi_k$, alors ε_i vaut $max(\varepsilon_j,\varepsilon_k)$

- $\varepsilon_n = 1$ (ce qui a pour but de dire que la valeur vérité de ϕ_n est 1, c'est-à-dire que x est effectivement satisfait par y)

(pour plus de précision, voir [2])

Supposons maintenant que $V(x,x)$ soit équivalente à une formule sans quantificateur: alors $\neg V(x,x)$ est équivalente à une formule sans quantificateur ϕ, codée par un entier $\widehat{\phi}$.

ϕ est-elle satisfaite par $\widehat{\phi}$?

Si oui, alors $V(\widehat{\phi},\widehat{\phi})$ et donc $\neg\phi(\widehat{\phi})$.

Sinon, $\neg V(\widehat{\phi},\widehat{\phi})$ donc $\phi(\widehat{\phi})$.

[Ce raisonnement fonctionne dès que l'on a une appartenance, ou dès que l'on peut en coder une: on écrit alors le paradoxe du menteur, et on obtient la contradiction cherchée]

Il faut maintenant "coder" une appartenance dans $(\mathbb{N},+,\times,0,1,\mathcal{F},=)$. En fait, on va en coder une dans $(\mathbb{N},+,\times,0,1,=)$ (il faut bien que le résultat soit vrai quand $\mathcal{F}$ est vide)

Pour cela, il faut "voir" un entier comme un ensemble(fini), c'est-à-dire trouver une bijection entre $\mathbb{N}$ et l'ensemble des n-uples d'entiers strictement croissants: on dit que $x \in y$ si le x-ième chiffre de y dans son écriture en base 2 est 1 (i.e si avec $y = \sum \alpha_i 2^i$, $\alpha_i \in \{0,1\}$, alors $\alpha_x = 1$)

Cette appartenance vérifie bien les axiomes de la théorie des ensembles (toujours sauf celui de l'infini). De plus, la fonction qui à (x,y) associe 1 si $x \in y$, 0 sinon est récursive, donc représentable (voir [4]). Il existe donc une formule à deux variables libres $\psi(x,y)$ (sur le language $\{+,\times,0,1,=\}$ équivalente à $x \in y$.

La construction précédente est valable, et $(\mathbb{N},+,\times,0,1,\mathcal{F},=)$ n' élimine donc pas les quantificateurs.

□

Remarque 1.5. Comme mentionné ci-dessous, ce résultat est trivialement faux si on s'autorise à rajouter un nombre infini de symboles.

2 Élimination

2.1 Énoncé du problème

Il faut maintenant énoncer précisément ce que l'on cherche à montrer. Mais voici d'abord le:

Théorème 2. *soit $\mathcal{M}$ une $\mathcal{L}$-structure quelconque.*

Pour chaque formule $\phi(\overline{x})$ (du langage $\mathcal{L}$), ajoutons à $\mathcal{L}$ un nouveau symbole de relation R_ϕ (de même arité que ϕ). On obtient alors le langage $\mathcal{L}'$.

Définissons la $\mathcal{L}'$-structure $\mathcal{M}'$ en interprétant R_ϕ par ϕ.

Alors $\mathcal{M}'$ élimine les quantificateurs.

Démonstration. Soit ϕ une formule quelconque du langage $\mathcal{L}'$.

ϕ est équivalente (dans $\mathcal{M}'$) à une formule ψ du langage $\mathcal{L}$ (il suffit de remplacer les R_ρ par ρ).

Et donc ϕ est équivalente (dans $\mathcal{M}'$) à R_ψ.

□

On voit donc que si on veut que $(\mathbb{N},+,\times,0,1,=)$ "vive" dans une structure qui élimine les quantificateurs, il faut exiger que le vocabulaire soit fini (sinon c'est trivial d'après le théorème précédent).

De plus, comme cela est dit dans l'introduction, le résultat est vrai pour toute structure.

On peut donc maintenant énoncer le:

Théorème 3. *soit $\mathcal{M} = (M,\mathcal{L})$ une structure sur un language fini $\mathcal{L}$ (contenant l'égalité).*

Alors il existe un language fini $\mathcal{L}^\circ$ (contenant l'égalité) et une $\mathcal{L}^\circ$-structure $\mathcal{M}^\circ = (M^\circ,\mathcal{L}^\circ)$ tels que:

- $\mathcal{L} \subset \mathcal{L}^\circ$
- $M \subset M^\circ$
- *$\mathcal{M}$ est une sous-$\mathcal{L}$-structure de $\mathcal{M}^\circ$ (vue comme $\mathcal{L}$-structure)*
- *$\mathcal{L}^\circ$ contient un prédicat unaire B d'appartenance à M, i.e pour $x \in M^\circ$, $\mathcal{M}^\circ \models B(x)$ si et seulement si $x \in M$*
- *$\mathcal{M}^\circ$ élimine les quantificateurs*

2.2 Construction de $\mathcal{M}^\circ$

On remarque tout d'abord que le théorème est trivial si M est fini (pour chaque élément de M, on associe une constante, et on remplace alors les $\exists$ par des disjonctions (finies), et les $\forall$ par des conjonctions (finies)).

On suppose désormais que M est infini.

Quitte à les rajouter, on peut donc supposer que $\mathcal{L}$ contient q, q_1 et q_2, de sorte que q est une bijection de M^2 dans M de réciproque (q_1,q_2).

On va construire $\mathcal{M}^\circ$ de manière explicite.

Comme dans l'exemple 1.4, on va rajouter des termes au moyen d'une fonction successeur. On a également besoin d'un "puits" Π, qui sert à étendre les fonctions et relations de M à M°:

- $M^\circ = (M \times \mathbb{N}) \cup \{\Pi\}$ (on identifie alors M à $M \times \{0\}$)
- $\mathcal{L}^\circ = \mathcal{L} \cup \{B,S,P,V,\Pi\}$
- les interprétations de $\mathcal{L}^\circ$ dans $\mathcal{M}^\circ$ sont:

- Π est un nouvel élément
- les constantes de $\mathcal{L}$ gardent la même interprétation
- une fonction f d'arité n vaut $f(\overline{x})$ si $\overline{x} \in M^n$, Π sinon
- une relation R d'arité n vaut $R(\overline{x})$ si $\overline{x} \in M^n$, $\perp$ sinon
- S fonction unaire (successeur): $S((x,n)) = (x,n+1)$, $S(\Pi) = \Pi$
- P fonction unaire (prédécesseur): $P((x,n)) = (x,n-1)$ si $n > 0$, $(x,0)$ sinon, $P(\Pi) = \Pi$
- $B(x)$ est vrai si et seulement si $x \in M$
- V prédicat unaire: ce qui précède permet de définir une structure $\mathcal{M}'$ sur le langage $\mathcal{L}^\circ \backslash \{V\}$ (de support M°).

On énumère les formules à une variable libre sur le langage $\mathcal{L}^\circ \backslash \{V\}$: $(\xi_n)_{n\in\mathbb{N}}$

On définit V par: $V((x,n))$ est équivalent à $\xi_k(x)$ (i.e $\mathcal{M}' \models V((x,n))$ si et seulement si $\mathcal{M}' \models \xi_k(x)$) si $n = k^2$, faux sinon (en particulier, $V(\Pi)$ est faux).

2.3 Étude de $\mathcal{M}^\circ$

On pourra éliminer les quantificateurs des formules sur $\mathcal{L}$ grâce au prédicat V, et comme dans l'exemple 1.4, les éléments rajoutés seront suffisamment faibles pour conserver l'élimination.

Mais donnons d'abord quelques définitions:

Définition 2.1. la hauteur H d'un élément de $\mathcal{M}^\circ$: $H((x,n)) = n$ et $H(\Pi) = \infty$

Remarque 2.2. $H(x) \leqslant n$ (avec $n \in \mathbb{N}$) se code par $P^{n+1}(x) = P^n(x) \wedge x \neq \Pi$

Donc $H(x) = n$ est équivalente à une formule du premier ordre ($x = \Pi$ si $n = \infty$, $H(x) \leqslant 0$ si $n = 0$, $H(x) \leqslant n \wedge \neg H(x) \leqslant n-1$ sinon).

Définition 2.3.

- l'ensemble $\mathcal{E}$ des formules de la forme $S^m(P^n(x)) = S^{m'}(P^{n'}(x'))$ ainsi que celles de la forme $x = \Pi$, où m, n, m', n' sont dans $\mathbb{N}$ et x et x' sont des variables distinctes.
- l'ensemble $\mathcal{V}$ des formules de la forme $V(S^m(P^n(x)))$, où m et n sont dans $\mathbb{N}$, et x est une variable.
- l'ensemble $\mathcal{H}$ des formules de la forme $\phi(\overline{x}) \wedge H(x_1) = k_1 \wedge \cdots \wedge H(x_n) = k_n$ où ϕ est une formule du langage $\mathcal{L}^\circ \backslash \{V\}$.

Remarque 2.4. $\mathcal{H}$ est stable par conjonction, et les formules de la forme $H(x) = k$ sont dans $\mathcal{H}$.

Définition 2.5. soit $\mathcal{A}$ un ensemble de formules:

$\mathcal{B}(\mathcal{A})$ est le plus petit ensemble contenant $\mathcal{A}$ et clos par $\wedge$, $\vee$ et $\neg$

Remarque 2.6. une formule de $\mathcal{B}(\mathcal{A})$ se met sous forme normale disjonctive (disjonction de conjonction de formules de $\mathcal{A}$ ou de $\neg\mathcal{A}$) et sous forme normale conjonctive (conjonction de disjonction de formules de $\mathcal{A}$ ou de $\neg\mathcal{A}$) (voir [3])

Voici maintenant un petit lemme utile pour la suite:

Lemme 2.7. *soit $t(\overline{x})$ un terme de $\mathcal{L}^\circ$, dont les variables libres sont exactement $\overline{x}$, et qui n'est pas un terme du language $\{S,P\}$*

alors $t(\overline{x}) \neq \Pi$ est soit fausse, soit équivalente à $H(x_1) \leqslant k_1 \wedge \cdots \wedge H(x_n) \leqslant k_n$ (où $k_1, \ldots, k_n$ sont dans $\mathbb{N}$)

Démonstration. faisons les simplifications suivantes sur $t(\overline{x})$:

- $P \circ S = id$
- $P \circ f = f$ (où f est un symbole de fonction de $\mathcal{L}$)
- $P(c) = c$ (où c est un symbole de constante de $\mathcal{L}$)
- si f (symbole de fonction de $\mathcal{L}$) s'applique à un terme commençant par S, on le remplace par Π

Si, à la fin, on obtient un terme dans lequel Π apparaît, alors $t(\overline{x}) = \Pi$.

Sinon, on obtient un terme de la forme: $S^k(t'(P^{k_1}(x_1), \ldots, P^{k_n}(x_n)))$ (où t' est un terme de $\mathcal{L}$). Et donc $t(\overline{x}) \neq \Pi$ est équivalent à $H(x_1) \leqslant k_1 \wedge \cdots \wedge H(x_n) \leqslant k_n$ □

Voici enfin un résultat fondamental (l'idée étant simplement que l'on peut contrôler la hauteur dès qu'un élément de $\mathcal{L}$ apparaît):

Lemme 2.8. *toute formule de $\mathcal{L}^\circ \backslash \{V\}$ est équivalente à une formule de $\mathcal{B}(\mathcal{E} \cup \mathcal{H})$.*

Démonstration. Nous allons faire une récurrence sur la longueur des formules.

• Montrons d'abord le résultat pour les formules atomiques:

- pour les formules contenant le prédicat B, il suffit de le remplacer par $H(.) = 0$, et on est ramené aux cas suivants.

- pour les formules de la forme $R(t_1(\overline{x_1}), \ldots, t_n(\overline{x_n}))$ (où R est dans $\mathcal{L}\backslash\{=\}$): séparons les t_i en $u_1, \ldots, u_r$ (termes sur le langage $\{P,S\}$) et $v_1, \ldots, v_s$ (les autres).

On remarque que $R(t_1(\overline{x_1}), \ldots, t_n(\overline{x_n}))$ est équivalente à $R(t_1(\overline{x_1}), \ldots, t_n(\overline{x_n})) \wedge H(u_1(\overline{x_{i_1}})) = 0 \wedge \cdots \wedge H(u_r(\overline{x_{i_r}})) = 0 \wedge v_1(\overline{x_{j_1}}) \neq \Pi \wedge \cdots \wedge v_s(\overline{x_{j_s}}) \neq \Pi$.

Pour les termes sur le langage $\{P,S\}$: on est ramené à $H(S^m(P^{m'}(x))) = 0$ (après la simplification $P \circ S = id$), ce qui est équivalent à $\perp$ si $m \neq 0$, $H(x) \leqslant m'$ sinon.

Pour les autres, on applique le lemme 2.7.

Ainsi, si on note $\overline{y}$ les variables apparaissant dans $x_1, \ldots, x_n$, on obtient une formule de la forme: $R(t_1(\overline{x_1}), \ldots, t_n(\overline{x_n})) \wedge H(y_1) \leqslant k_1 \wedge \cdots \wedge H(y_n) \leqslant k_n$

$H(x) \leqslant k$ est équivalent à $H(x) = 0 \vee \cdots \vee H(x) = k$.

En appliquant ceci et en distribuant $\wedge$ sur $\vee$, on obtient une disjonction de formules de $\mathcal{H}$.

- pour les formules de la forme $t(\overline{x}) = t'(\overline{x'})$: c'est presque pareil.

Si ni t ni t' ne sont sur $\{P,S\}$, on a la formule équivalente suivante:

$(t(\overline{x}) = t'(\overline{x'}) \wedge t(\overline{x}) \neq \Pi \wedge t(\overline{x'}) \neq \Pi) \vee (t(\overline{x}) = \Pi \wedge t(\overline{x'}) = \Pi)$

On procède alors comme précédemment.

Si un seul des deux est sur $\{P,S\}$: $t(\overline{x}) = S^m(P^n(x'))$ est équivalent à:

$(t(\overline{x}) = S^m(P^n(x')) \wedge t(\overline{x}) \neq \Pi \wedge x' \neq \Pi) \vee (t(\overline{x}) = \Pi \wedge x' = \Pi)$

Etudions la première partie de la disjonction: dans la démonstration du lemme 2.7, on a vu que $t(\overline{x}) = S^k(\widetilde{t}(P^{k_1}(x_1), \ldots, P^{k_n}(x_n)))$ (où $\widetilde{t}$ est un terme de $\mathcal{L}$)

Donc $H(S^m(P^n(x'))) = k$, ce qui est équivalent à $\perp$ si $m > k$, à $H(x') \leqslant n$ si $m = k$, à $H(x') = k - n + m$ sinon. On procède alors comme précédemment.

Si les deux termes sont sur $\{P,S\}$: si les deux variables sont distinctes, alors on est dans $\mathcal{E}$.

Sinon, la formule est de la forme $S^m(P^n(x)) = S^{m'}(P^{n'}(x))$ (ce que l'on note ψ), ce qui est équivalent à $(H(x) = 0 \wedge \psi) \vee \cdots \vee (H(x) = r \wedge \psi) \vee (H(x) > r \wedge \psi)$

Il suffit donc d'étudier $H(x) > r \wedge \psi$ (les autres formules sont dans $\neg\mathcal{H}$)

Avec $r = max(n,n') + 1$, quand $H(x) > r$, ψ est vraie si $m - n = m' - n'$, équivalente à $x = \Pi$ sinon.

Dans tous les cas, on est bien dans $\mathcal{B}(\mathcal{H})$.

• $\mathcal{B}(\mathcal{E} \cup \mathcal{H})$ est stable par $\wedge$ et par $\neg$: il suffit de montrer que si ϕ est dans $\mathcal{B}(\mathcal{E} \cup \mathcal{H})$, alors il en est de même pour $\exists x, \phi$

On met ϕ sous forme normale disjonctive, on distribue $\exists x$ sur $\vee$, et on est ramené à $\exists x, \phi_1(\overline{x_1}) \wedge \cdots \wedge \phi_n(\overline{x_n})$ $(= \psi)$, où les ϕ_i sont dans $\mathcal{E} \cup \mathcal{H} \cup \neg\mathcal{E} \cup \neg\mathcal{H}$.

(quitte à les "sortir" du quantificateur, on peut même supposer que x est effectivement une variable libre de chacune des ϕ_i)

- Si l'une des ϕ_i est dans $\mathcal{E}$ (de la forme: $S^m(P^s(x)) = S^{m'}(P^{s'}(x'))$, on écrit ψ sous la forme: $(H(x') = 0 \wedge \psi) \vee \cdots \vee (H(x') = r \wedge \psi) \vee (H(x') > r \wedge \psi)$

On choisit r suffisamment grand pour que l'on puisse écrire $x = S^{s-m+m'-s'}(x')$ ou $x = P^{s'-m'+m-s}(x')$ (suivant le signe de $s - m + m' - s'$)

Et lorsque l'on connaît la hauteur de x', on peut résoudre l'équation (en x) $S^m(P^s(x)) = S^{m'}(P^{s'}(x'))$: il n'y a qu'un nombre fini de solutions, que l'on peut exprimer à l'aide de P, S et x'.

On est alors ramené à montrer que $\exists x, x = t(x') \wedge \phi_1(\overline{x_1}) \wedge \cdots \wedge \phi_n(\overline{x_n})$ (où t est une puissance de P ou de S) est dans $\mathcal{B}(\mathcal{E} \cup \mathcal{H})$.

Cette dernière formule est équivalente à la conjonction des ϕ_i dans laquelle on a remplacé x par $t(x')$, qui est bien dans $\mathcal{B}(\mathcal{E} \cup \mathcal{H})$ (on le vérifie facilement).

- Sinon aucune des ϕ_i n'est dans $\mathcal{E}$: si aucune des ϕ_i n'est dans $\mathcal{H}$, ψ est équivalente à $\top$ (il suffit de prendre x de hauteur suffisamment grande pour le voir).

On peut donc supposer que l'une des ϕ_i est dans $\mathcal{H}$. Comme $\mathcal{H}$ est stable par conjonction, on peut même supposer qu'il n'y en a qu'une (par exemple ϕ_1).

Si l'une des ϕ_i est dans $\neg\mathcal{E}$ (par exemple ϕ_2 de la forme $S^m(P^s(x)) \neq S^{m'}(P^{s'}(x'))$), on écrit encore ψ sous la forme:

$(H(x') = 0 \wedge \psi) \vee \cdots \vee (H(x') = r \wedge \psi) \vee (H(x') > r \wedge \psi)$

On prend r suffisamment grand pour que ϕ_2 soit vraie lorsque $H(x') > r$.

Pour les autres formules, on regroupe ϕ_1, ϕ_2 et $H(x') = k$ pour obtenir une formule de $\mathcal{H}$.

On est donc ramené à montrer le résultat lorsque aucune des ϕ_i n'est dans $\neg\mathcal{E}$, c'est-à-dire lorsque ψ est de la forme: $\exists x, \phi_1(\overline{x_1}) \wedge \cdots \wedge \phi_n(\overline{x_n})$, où ϕ_1 est dans $\mathcal{H}$, et $\phi_2 \ldots \phi_n$ sont dans $\neg\mathcal{H}$.

Montrons le par récurrence sur n: pour $n = 1$, c'est évident ($\phi_1(\overline{x_1})$ est de la forme $\phi(x,\overline{y}) \wedge H(x) = k \wedge H(y_1) = k_1 \wedge \cdots \wedge H(y_m) = k_m$ donc $\exists x, \phi_1(\overline{x_1})$ est équivalent à $(\exists x, \phi(x,\overline{y}) \wedge H(x) = k) \wedge H(y_1) = k_1 \wedge \cdots \wedge H(y_m) = k_m)$

Supposons le résultat vrai au rang $n - 1$:

ϕ_n est de la forme $\phi(x,\overline{y}) \vee H(x) \neq k \vee H(y_1) \neq k_1 \vee \cdots \vee H(y_m) \neq k_m$, ce qui est équivalent à $\widetilde{\phi}(x,\overline{y}) \vee H(y_1) \neq k_1 \vee \cdots \vee H(y_m) \neq k_m$, où $\widetilde{\phi}(x,\overline{y})$ désigne la formule $(\phi(x,\overline{y}) \vee H(x) \neq k) \wedge H(y_1) = k_1 \wedge \cdots \wedge H(y_m) = k_m$

Notons $h(\overline{y})$ la formule $H(y_1) \neq k_1 \vee \cdots \vee H(y_m) \neq k_m$ (qui est dans $\neg\mathcal{H}$)

Alors $\exists x, \phi_1(\overline{x_1}) \wedge \cdots \wedge \phi_n(\overline{x_n})$ est équivalente à :

$(\exists x, \phi_1(\overline{x_1}) \wedge \cdots \wedge \phi_{n-1}(\overline{x_{n-1}}) \wedge \widetilde{\phi}(x,\overline{y})) \vee ((\exists x, \phi_1(\overline{x_1}) \wedge \cdots \wedge \phi_{n-1}(\overline{x_{n-1}})) \wedge h(\overline{y}))$

On remarque que $\phi_1(\overline{x_1}) \wedge \widetilde{\phi}(x,\overline{y})$ est dans $\mathcal{H}$, et on applique alors l'hypothèse de récurrence.

$\square$

2.4 Élimination dans $\mathcal{M}^\circ$

Le lemme précédent contient toute la partie technique. Il ne reste maintenant qu'à étudier les formules contenant V :

Théorème 4. *soit ϕ une formule du langage $\mathcal{L}^\circ$: ϕ est équivalente à une formule de $\mathcal{B}(\mathcal{E} \cup \mathcal{H} \cup \mathcal{V})$*

Démonstration. Nous allons montrer le résultat par récurrence sur la longueur des formules.

• Pour les formules atomiques, il suffit de traiter le cas de celles contenant V (pour les autres, il suffit d'appliquer le lemme 2.8).

Si t est un terme sur le langage $\{P,S\}$, $V(t)$ est équivalent à une formule de $\mathcal{V}$.

Sinon, comme $V(\Pi)$ est faux, $V(t)$ est équivalent à $V(t) \wedge t \neq \Pi$

Comme on peut alors le voir dans la démonstration du lemme 2.7, soit $t = \Pi$, soit $t = S^k(t'(P^{k_1}(x_1), \ldots, P^{k_n}(x_n)))$ (où t' est un terme de $\mathcal{L}$)

Et donc $V(t)$ est équivalent à $\xi_{\sqrt{k}}(t'(P^{k_1}(x_1), \ldots, P^{k_n}(x_n))) \wedge t \neq \Pi$ (avec la convention $\xi_{\sqrt{k}}$ est fausse si k n'est pas un carré).

Cette dernière formule ne contient pas V, et le lemme 2.8 conclut.

• $\mathcal{B}(\mathcal{E} \cup \mathcal{H} \cup \mathcal{V})$ étant stable par $\neg$ et $\wedge$, il suffit de montrer que si ϕ est dans $\mathcal{B}(\mathcal{E} \cup \mathcal{H} \cup \mathcal{V})$, il en est de même pour $\exists x,\phi$

On procède alors comme dans le lemme précédent: on met ϕ sous forme normale disjonctive, on distribue $\exists x$ sur $\vee$, et on est ramené à $\exists x,\phi_1(\overline{x_1}) \wedge \cdots \wedge \phi_n(\overline{x_n})$ $(= \psi)$, où les ϕ_i sont dans $\mathcal{E} \cup \mathcal{H} \cup \mathcal{V} \cup \neg\mathcal{E} \cup \neg\mathcal{H} \cup \neg\mathcal{V}$.

(quitte à les "sortir" du quantificateur, on peut même supposer que x est effectivement une variable libre de chacune des ϕ_i)

Si l'une des ϕ_i est dans $\mathcal{E}$, on procède comme dans le lemme précédent.

Ensuite, on remarque qu'il suffit d'éliminer les V, puis d'appliquer le lemme 2.8.

Dès que l'on connaît la hauteur de x, on peut éliminer V : si l'on note h la hauteur de $S^m(P^s(x))$, $V(S^m(P^s(x))) \wedge H(x) = k$ équivaut à $\xi_{\sqrt{h}}(P^k(x)) \wedge H(x) = k$ ($h = m$ si $k \leqslant s$, $k - s + m$ sinon).

Ainsi, si l'une des ϕ_i est dans $\mathcal{H}$, on peut éliminer les V.

Puis on écrit encore ψ sous la forme:

$(\exists x,H(x) = 0 \wedge \phi) \vee \cdots \vee (\exists x,H(x) = r \wedge \phi) \vee (\exists x,H(x) > r \wedge \phi)$

(avec r suffisamment grand pour que l'on puisse écrire (lorsque $H(x) > r$) $H(S^m(P^n(x))) = H(x) + m - n$ pour chaque ϕ_i de la forme $V(S^m(P^n(x)))$)

Pour les formules de la forme $\exists x,H(x) = k \wedge \phi$, on connaît la hauteur de x.

Pour $\exists x,H(x) > r \wedge \phi$: si deux formules de $\mathcal{V}$ ($V(S^m(P^n(x)))$ et $V(S^{m'}(P^{n'}(x)))$) apparaissent, on peut supposer que $m - n \neq m' - n'$ (sinon, on n'en garde qu'une).

Si il reste encore deux formules de $\mathcal{V}$: il n'y a qu'un nombre fini de façons d'écrire $m - n - m' + n'$ comme différence de deux carrés, chacune d'elle donnant une hauteur pour x, et on est alors ramené au cas précédent.

Finalement, le dernier cas à traiter est celui-ci:

$\exists x, V(S^m(P^n(x))) \wedge \phi_1 \wedge \cdots \wedge \phi_n$, où les ϕ_i sont dans $\neg\mathcal{E} \cup \neg\mathcal{H} \cup \neg\mathcal{V}$.

La formule $\Pi = \Pi \wedge \cdots \wedge \Pi = \Pi$ (r fois) est codée par n_r (i.e. est ξ_{n_r}).

Le codage est injectif donc $n_r \to \infty$ (quand $r \to \infty$).

Donc en choisissant x de hauteur $n_r + n - m$ (pour r assez grand), on voit que la formule précédente est vraie.

□

C'est presque terminé: le prédicat V permet d'éliminer les quantificateurs pour des formules ne contenant pas V, et le théorème précédent permet justement de s'y ramener.

Le lemme suivant permettra alors de conclure facilement.

Lemme 2.9. *une formule de $\mathcal{H}$ est équivalente à une formule sans quantificateur.*

Démonstration. Considérons la formule $\phi(\overline{x}) \wedge H(x_1) = k_1 \wedge \cdots \wedge H(x_n) = k_n$

On va se ramener dans M pour pouvoir utiliser les fonctions q, q_1 et q_2.

Soit $X(\overline{x})$ le terme $q(P^{k_1}(x_1), q(\ldots, q(P^{k_{n-1}}(x_{n-1}), P^{k_n}(x_n))\ldots))$

Soit $\psi(y)$ la formule $\phi(S^{k_1}(q_1(y)), \ldots, S^{k_{n-1}}(q_1(q_2^{n-2}(y))), S^{k_n}(q_2^{n-1}(y)))$

Alors $\phi(\overline{x}) \wedge H(x_1) = k_1 \wedge \cdots \wedge H(x_n) = k_n$ est équivalente à:

$\psi(X(\overline{x})) \wedge H(x_1) = k_1 \wedge \cdots \wedge H(x_n) = k_n$

Il existe k tel que ψ soit égale à ξ_k.

Et donc $\psi(X(\overline{x})) \wedge H(x_1) = k_1 \wedge \cdots \wedge H(x_n) = k_n$ est équivalente à:

$V(S^{k^2}(X(\overline{x}))) \wedge H(x_1) = k_1 \wedge \cdots \wedge H(x_n) = k_n$

□

Le théorème 4 et le lemme précédent permettent alors de montrer qu'une formule de $\mathcal{L}^\circ$ est équivalente à une formule sans quantificateur, ce qui achève la démonstration du théorème 3.

Remarque 2.10. l'élimination proposée est algorithmique.

Remarque 2.11. le théorème 3 reste vrai si $\mathcal{L}$ est dénombrable (en effet, les formules sont encore dénombrables dans ce cas).

Bibliographie

[1] A shorter model theory, W. Hodges, Ed. Cambridge University Press

[2] Les petits cailloux, B. Poizat, Ed. Nur al-Mantiq wal-Ma'rifah

[3] Logique mathématique (tome I), R. Cori et D. Lascar, Ed. Masson

[4] Logique mathématique (tome II), R. Cori et D. Lascar, Ed. Masson