Calcul des prédicats

Notes complémentaires (1)

1 Syntaxe

1.1 Langages

Un **langage** (ou **un type de similarité**) **égalitaire** $\mathcal{L}$ est défini par les données suivantes :

• Un ensemble $\mathcal{R}$ de *symboles de relation*, ou *symboles de prédicat*. A chaque symbole $R \in \mathcal{R}$ est associé un entier $n \geq 1$, appelé son *arité*. On dit que R est un symbole de relation n-aire, ou à n arguments. On distingue un symbole binaire particulier, que l'on note $R_=$.

• Un ensemble $\mathcal{F}$ de *symboles de fonction*. A chaque symbole $f \in \mathcal{F}$ est associé un entier $n \geq 1$, appelé son *arité*. On dit que f est un symbole de fonction n-aire, ou à n arguments.

• Un ensemble $\mathcal{C}$ de *symboles de constantes*.

On considère les mots (suites finies) dans le vocabulaire formé des symboles de $\mathcal{R}$, $\mathcal{F}$, $\mathcal{C}$, des parenthèses $\{(\}$ et $\{)\}$, de la virgule $\{,\}$ et des *symboles logiques* suivants :

• Les connecteurs propositionnels $\neg$, $\wedge$ et $\vee$;

• le quantificateurs $\exists$, qui se lit "il existe", et est appelé le quantificateur *existentiel*, et le quantificateur $\forall$, qui se lit "pour tout" et est appelé le quantificateur universel;

• un ensemble dénombrable $\mathcal{V} = \{v_0, \ldots, v_n, \ldots\}$ de variables.

1.2 Termes

L' ensemble des **termes** du langage $\mathcal{L}$, noté $\mathcal{T}$, est, par définition, le plus petit ensemble de mots (suites finies) écrits avec le vocabulaire $\mathcal{V} \cup \mathcal{F} \cup \mathcal{C} \cup \{(\} \cup \{)\} \cup \{,\}$ tel que :

– Chaque variable est un terme.

– Chaque constante est un terme.

– Si f est un symbole de fonction d'arité n, et si $t_1, \ldots, t_n$ sont des termes, alors $f(t_1, \ldots, t_n)$ est un terme.

La *longueur* d'un terme est, par définition, le nombre de symboles de ce terme.

Lemme 1 (Lecture unique) *Chaque terme est, soit une variable, soit un symbole de constante, soit de la forme $f(t_1, \ldots, t_n)$ où f est un symbole de fonction d'arité n, et $t_1, \ldots, t_n$ sont des termes. Cette écriture est unique.*

Existence : immédiate, par récurrence sur la longueur du terme.
Unicité : on utilise le

Lemme 2 *Si t est un terme, alors $ts_1 \dots s_k$ n'en est pas un, quels que soient $k > 0$ et les symboles $s_1, \dots, s_k$ (variables, symboles de constante, symboles de fonction, parenthèses ou virgule).*

Preuve par récurrence sur la longueur du terme : c'est évident si t est une variable x ou un symbole de constante, car un terme de longueur > 1 doit commencer par un symbole de fonction. Supposons que $t = f(t_1, \dots, t_n)$, et que $t' = ts_1 \dots s_k$ soit un terme. Alors t' est un terme qui commence par le symbole f, donc $t' = f(t'_1, \dots, t'_n)$. On ne peut avoir $t_i = t'_i$ pour chaque $i\,(1 \leq i \leq n)$, puisque $t \neq t'$. Soit j le premier entier $\leq n$ tel que $t_j \neq t'_j$. On a donc $f(t_1, \dots, t_{j-1} = f(t'_1 \dots t'_{j-1},$; et donc $t_j \dots t_n)s_1 \dots s_k = t'_j \dots t'_n)$. Comme $t_j \neq t'_j$, on voit que, ou bien $t'_j = t_j s'_1 \dots s'_l$, ou bien $t_j = t'_j s'_1 \dots s'_l$, $s'_1, \dots, s'_l$ étant des symboles. Ceci contredit l'hypothèse de récurrence, puisque t_j est plus court que t (et donc, dans le deuxième cas, t'_j est aussi plus court que t).

On désignera par $t[v_1, \dots, v_k]$ un terme dont les variables se trouvent dans l'ensemble $\{v_1, \dots, v_k\}$. Un terme sans variable est appelé un *terme clos*. Pour qu'il existe un terme clos, il faut et il suffit qu'il y ait au moins un symbole de constante dans $\mathcal{L}$.

Le lemme de lecture unique nous permet de définir des fonctions par induction sur l'ensemble des termes.

Exemple: **Substitutions dans un terme.**
Une substitution est une application $\sigma : \mathcal{T} \to \mathcal{T}$ telle que

$$\sigma(f(t_1, \dots, t_n)) = f(\sigma(t_1), \dots, \sigma(t_n))$$

quels que soient le symbole de fonction f d'arité n, et les termes $t_1, \dots, t_n$ et telle que $\sigma(c) = c$ pour tout symbole de constante c.
La donnée d'une substitution équivaut à celle d'une fonction $\sigma_0 : \mathcal{V} \to \mathcal{T}$. En effet, il existe alors un unique prolongement à $\mathcal{T}$, et un seul, qui est une substitution.

1.3 Formules du premier ordre

Une **formule atomique** du langage $\mathcal{L}$ est une suite de symboles de la forme $R(t_1, \dots, t_n)$, où R est un symbole de prédicat d'arité n, et $t_i \in \mathcal{T}$ pour $1 \leq i \leq n$.
Lorsque R est un symbole de relation d'arité 2, la formule atomique $R(t, u)$ est parfois écrite tRu. C'est toujours le cas lorsque R est le symbole $R_=$.

L'ensemble des **formules** du langage $\mathcal{L}$ est le plus petit ensemble de mots qui contient les formules atomiques et qui est clos par les opérations suivantes:
– Si F, G sont des formules, alors $\neg F$, $(F \wedge G)$, $(F \vee G)$ sont des formules.
– Si F est une formule et v une variable, alors $\exists v F$ et $\forall v F$ sont des formules.

Une *occurrence* de la variable v dans la formule F, est, par définition, une apparition de v dans la suite finie F.

On définit quand une **occurence** de la variable v dans la formule F est **libre** par induction sur F, de la façon suivante :

– Si F est une formule atomique, chaque occurrence de v dans F est libre.

– Si F est de la forme $\neg G$ (respectivement $(G \wedge H)$) ou $(G \vee H)$), une occurence de v dans F est libre si c'est une occurence libre de v dans G (respectivement si c'est une occurence libre de v dans G ou une occurence libre de v dans H).

– Si F est de la forme $\exists w G$ ou $\forall w G$, il y a deux cas : si $w \neq v$, les occurrences libres de v dans F sont les occurrences libres de v dans G; si $w = v$, alors v n'a aucune occurrence libre dans F.

Une variable v est dite **libre** dans la formule F si elle a au moins une occurrence libre dans F. Si la variable v apparait dans F et n'est pas libre, on dira qu'elle est **liée**. Une formule est dite **close** si elle n'a aucune variable libre. Les formules closes seront aussi appellées des **énoncés**.

On définit par induction les **sous-formules** d'une formule:

– si F est une formule atomique, G est une sous-formule de F ssi $F = G$,

– si $F = \neg H$, G est une sous-formule de F ssi G est une sous-formule de H ou $G = F$,

– si $F = (H_1 \wedge H_2)$, G est une sous-formule de F ssi G est une sous-formule de H_1 ou G est une sous-formule de H_2 ou $G = F$,

– si $F = (H_1 \vee H_2)$, G est une sous-formule de F ssi G est une sous-formule de H_1 ou G est une sous-formule de H_2 ou $G = F$,

– si $F = \exists v\, H$, G est une sous-formule de F ssi G est une sous-formule de H ou $G = F$.

– si $F = \forall v\, H$, G est une sous-formule de F ssi G est une sous-formule de H ou $G = F$.

On dira qu'une variable v est *ambigue* dans la formule F si v est libre dans F mais apparait comme variable liée dans une sous-formule de F. Une formule est dite *propre* si elle n'a pas de variables ambigues.
On utilisera la notation $F[v_0, \ldots, v_k]$ pour désigner une formule F dont toutes les variables libres se trouvent parmi l'ensemble fini de variables $\{v_0, \ldots, v_k\}$.

On a bien sûr un *théorème de lecture unique* pour les formules de $\mathcal{L}$ et on peut donc définir des fonctions par induction.

2 Sémantique

2.1 Interprétation et satisfaction

2.1.1 $\mathcal{L}$-structures

Étant donné un langage $\mathcal{L}$ (égalitaire), on définit la notion de **$\mathcal{L}$-structure (égalitaire)**. Une $\mathcal{L}$-structure (égalitaire) $\mathcal{M}$ est constituée des données suivantes :

– Un ensemble non vide M, ensemble de base de la structure $\mathcal{M}$.

– Pour chaque symbole de relation R de $\mathcal{L}$, d'arité n_R, une partie $R^{\mathcal{M}}$ de M^{n_R}; $R^{\mathcal{M}}$ est donc une relation n_R-aire sur l'ensemble M, appelée l'interprétation du symbole R dans

$\mathcal{M}$. Dans une structure égalitaire la relation $R_=$ est toujours interprétée par la diagonale dans M^2, c'est-à-dire par la relation d'égalité dans M.

– Pour chaque symbole de fonction f de $\mathcal{L}$, d'arité n_f, une fonction $f^{\mathcal{M}} : M^{n_f} \to M$.

– Pour chaque symbole de constante c de $\mathcal{L}$, un élément $c^{\mathcal{M}}$ de M.

On écrira $\mathcal{M} =< M; R^{\mathcal{M}}, f^{\mathcal{M}}, c^{\mathcal{M}}; R \in \mathcal{R}, f \in \mathcal{F}, c \in \mathcal{C} >$.

Exemples:

1. $\mathcal{L} = \{R\}$ avec R un symbole de relation d'arité 2. Alors $\mathcal{M}_1 =< \mathbb{Z}; \leq >$ est une $\mathcal{L}$-structure dans la quelle la relation R est interprétée par la relation d'ordre habituelle. Si $\mathcal{M}_2 =< \mathbb{Z}; \equiv_p >$, alors $\mathcal{M}_2$ est une autre $\mathcal{L}$-structure dans laquelle R est interprétée par la relation de congruence modulo p.

2. $\mathcal{L} = \{f_1, f_2, c\}$ avec f_1 un symbole de fonction d'arité 2, f_2 un symbole de fonction d'arité 1, et c un symbole de constante.
$\mathcal{M}_1 =< \mathbb{Z}; +, -, 0 >$ est une $\mathcal{L}$-structure dans la quelle ${f_1}^{\mathcal{M}_1}$ est l'addition, ${f_2}^{\mathcal{M}_1}(x) = -x$ et ${c}^{\mathcal{M}_1} = 0$.
$\mathcal{M}_2 =< \mathbb{R} \setminus \{0\}; ., ^{-1}, 1 >$ est une $\mathcal{L}$-structure dans la quelle f_1 est interprétée par la multiplication, f_2 par la fonction x^{-1} et la constante c par 1.
Ce langage est celui qu'on utilise pour parler des groupes.

3. $\mathcal{L} = \{f_1, f_2, f_3, c_1, c_2\}$ avec f_1 un symbole de fonction d'arité 2, f_2 un symbole de fonction d'arité 1, f_3 un symbole de fonction d'arité 2 , c_1 et c_2 deux symboles de constantes. $\mathcal{M}_1 =< \mathbb{Z}; +, -, ., 0, 1 >$ est une $\mathcal{L}$-structure dans laquelle ${f_1}^{\mathcal{M}_1}$ est l'addition, ${f_2}^{\mathcal{M}_1}(x) = -x$, f_3 est interprétée par la multiplication , ${c_1}^{\mathcal{M}_1} = 0$ et ${c_2}^{\mathcal{M}_1} = 1$. Ce langage est celui qu'on utilise pour parler des anneaux.

2.1.2 Morphismes

Soient $\mathcal{L}$ un langage, $\mathcal{M}$ et $\mathcal{N}$ deux $\mathcal{L}$-structures et h une application de M dans N. L'application h est un **$\mathcal{L}$-homomorphisme** de $\mathcal{M}$ dans $\mathcal{N}$ si h vérifie:

– (1) pour tout symbole c de constante de $\mathcal{L}$, $h(c^{\mathcal{M}}) = c^{\mathcal{N}}$,

– (2) pour tout symbole f de fonction de $\mathcal{L}$, d'arité k, pour tout $(m_1, \ldots, m_k) \in M^k$, $h(f^{\mathcal{M}}(m_1, \ldots, m_k)) = f^{\mathcal{N}}(h(m_1), \ldots, h(m_k))$ (c'est-à-dire $h \circ f^{\mathcal{M}} = f^{\mathcal{N}} \circ h$),

– (3) pour tout symbole R de relation de $\mathcal{L}$, d'arité k, pour tout $(m_1, \ldots, m_k) \in M^k$, si $R^{\mathcal{M}}(m_1, \ldots, m_k) \in R^{\mathcal{M}}$, alors $(h(m_1), \ldots, h(m_k)) \in R^{\mathcal{N}}$.

L'application h est un **$\mathcal{L}$-plongement** de $\mathcal{M}$ dans $\mathcal{N}$ si h est un $\mathcal{L}$-homomorphisme et satisfait en plus que pour tout symbole R de relation de $\mathcal{L}$, d'arité k, pour tout $(m_1, \ldots, m_k) \in M^k$, $(m_1, \ldots, m_k) \in R^{\mathcal{M}}$, **si et seulement si** $(h(m_1), \ldots, h(m_k)) \in R^{\mathcal{N}}$.
En particulier, dans le cas de langages et de structures égalitaires, un $\mathcal{L}$-plongement est injectif.
Un $\mathcal{L}$-plongement surjectif est appelé un **$\mathcal{L}$-isomorphisme**. Un $\mathcal{L}$-isomorphisme de $\mathcal{M}$ dans $\mathcal{M}$ est appelé un **$\mathcal{L}$-automorphisme** de $\mathcal{M}$.

Remarque: un $\mathcal{L}$-homomorphisme injectif n'est pas forcément un $\mathcal{L}$-plongement. C'est le cas si le langage $\mathcal{L}$ ne comprend pas de symbole de relation autre que l'égalité, mais si on considère le langage $\mathcal{L}$ d'une relation binaire, et les deux $\mathcal{L}$-structures $\mathcal{M}_1 =< \mathbb{Z}, \equiv_6 >$

et $\mathcal{M}_2 =< \mathbb{Z}, \equiv_3 >$, où $\equiv_n$ est la congruence modulo n, alors l'identité est un $\mathcal{L}$-homomorphisme bijectif de $\mathcal{M}_1$ dans $\mathcal{M}_2$ mais n'est pas un $\mathcal{L}$-plongement.

2.1.3 Valeur ou interprétation des termes

Soit $\mathcal{M}$ une $\mathcal{L}$-structure, $\mathcal{M} =< M, \dots >$.

Pour chaque $n \geq 0$, à chaque terme t de $\mathcal{L}$, dont les variables sont parmi $\{v_0, \dots, v_n\}$, on associe sa **valeur** ou son **interprétation** en $(a_0, \dots, a_n) \in M^{n+1}$, notée $t^{\mathcal{M}}[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n]$.
Elle est définie par induction sur la longueur de t :

– Si t est une variable v_i, $t^{\mathcal{M}}[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n] = a_i$.
– Si t est un symbole de constante c de $\mathcal{L}$, $t^{\mathcal{M}}[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n] = c^{\mathcal{M}}$.
– Si $t = f(t_1, \dots, t_k)$, alors $t^{\mathcal{M}}[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n] =$
$f^{\mathcal{M}}(t_1^{\mathcal{M}}[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n], \dots, t_k^{\mathcal{M}}[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n])$.

2.1.4 Satisfaction des formules

Soit $F[v_0, \dots, v_n]$ une formule ayant ses variables libres parmi $\{v_0, \dots, v_n\}$. On définit, pour tout n, pour toute $\mathcal{L}$-structure $\mathcal{M}$, pour tout $n+1$-uple d'éléments de M, $(a_0, \dots, a_n)$, par induction sur la hauteur de F, les expressions synonymes

"$\mathcal{M}$ satisfait $F[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n]$",
ou encore
" F est vraie dans $\mathcal{M}$ pour $(a_0, \dots, a_n)$",
notée
$\mathcal{M} \models F[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n]$:

– Si F est la formule atomique $R(t_1, \dots, t_k)$ (R est un symbole de relation k-aire, $t_1, \dots, t_k$ sont des termes) , alors $\mathcal{M} \models F[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n]$ si et seulement si $(t_1^{\mathcal{M}}[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n], \dots, t_k^{\mathcal{M}}[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n])$ appartient au sous-ensemble de M^k qui est l'interprétation du symbole R, $R^{\mathcal{M}}$.

– Si F est $\neg G$, alors $\mathcal{M} \models F[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n]$ si et seulement si $\mathcal{M}$ ne satisfait pas $G[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n]$.

– Si F est $(G \wedge H)$ alors $\mathcal{M} \models F[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n]$ si et seulement si
$\mathcal{M} \models G[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n]$ *et* $\mathcal{M} \models H[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n]$.

– Si F est $(G \vee H)$ alors $\mathcal{M} \models F[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n]$ si et seulement si
$\mathcal{M} \models G[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n]$ *ou* $\mathcal{M} \models H[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n]$.

– Si F est $\exists w\, G$, $\mathcal{M} \models F[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n]$ si et seulement s'*il existe* $b \in M$ tel que $\mathcal{M} \models G[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n, w \rightsquigarrow b]$.

– Si F est $\forall w\, G$, alors $\mathcal{M} \models F$ si et seulement si, *pour tout* $b \in M$, $\mathcal{M} \models G[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow a_n, w \rightsquigarrow b]$.

On remarque que les deux définitions au-dessus n'ont d'intêret que si effectivement la variable w apparait librement dans la formule G mais que dans les autres cas elle ne pose pas de problèmes: si w n'apparait pas du tout dans G, alors $\mathcal{M} \models G[v_0 \rightsquigarrow a_0, \dots, v_n \rightsquigarrow$

$a_n, w \rightsquigarrow b]$ ssi $\mathcal{M} \models G[v_0 \rightsquigarrow a_0, \ldots, v_n \rightsquigarrow a_n]$. Si w apparaît dans G comme variable liée, il en est de même.

Plus généralement on vérifie que si les variables libres de F sont parmi $\{v_0, \ldots, v_k\}$, pour $k < n$, alors $\mathcal{M} \models F[v_0 \rightsquigarrow a_0, \ldots, v_k \rightsquigarrow a_k, \ldots, v_n \rightsquigarrow a_n]$ si et seulement si $\mathcal{M} \models F[v_0 \rightsquigarrow a_0, \ldots, v_k \rightsquigarrow a_k]$.

En particulier, si F est une formule close, c'est à dire sans aucune variable libre, alors la valeur de vérité de F dans $\mathcal{M}$ ne dépend pas du n-uple auquel on l'applique: la formule est toujours soit vraie, soit fausse dans $\mathcal{M}$. Donc on écrira simplement $\mathcal{M} \models F$ et on dira que $\mathcal{M}$ est un **modèle** *de F.*

Une formule close F du langage $\mathcal{L}$ est dite *universellement valide* si elle est satisfaite par toute $\mathcal{L}$-structure.

• **Connecteurs supplémentaires**:
On utilisera les notations suivantes, si F, G sont des formules:
– $(F \to G)$ pour la formule $(\neg F \vee G)$
– $(F \leftrightarrow G)$ pour la formule $((F \to G) \wedge (G \to F))$

• **Équivalence, conséquence sémantique**
Deux formules $F[v_0, \ldots, v_n]$ et $G[v_0, \ldots, v_n]$ sont dites *équivalentes* si la formule

$$\forall v_0 \ldots \forall v_n (F \leftrightarrow G)$$

est universellement valide. Cela revient à dire que, dans toute $\mathcal{L}$-structure $\mathcal{M}$, pour tout $n+1$-uple $(a_0, \ldots, a_n) \in M^n$, on a que $\mathcal{M} \models F[v_0 \rightsquigarrow a_0, \ldots, v_n \rightsquigarrow a_n]$ si et seulement si $\mathcal{M} \models G[v_0 \rightsquigarrow a_0, \ldots, v_n \rightsquigarrow a_n]$.

Soit Σ un ensemble d'énoncés de $\mathcal{L}$. On dit qu'une $\mathcal{L}$-structure $\mathcal{M}$ est un modèle de Σ si $\mathcal{M}$ est modèle de chaque énoncé F de l'ensemble Σ. On dit que un énoncé F est *conséquence sémantique* (ou, plus simplement, *conséquence*) de Σ si tout modèle de Σ satisfait F. La notation est $\Sigma \vdash F$. Un énoncé F est universellement valide si et seulement si il est conséquence de $\emptyset$, donc noté $\vdash F$.

3 Quelques lemmes "grammaticaux"

3.1 Substitutions dans une formule

Soit $\sigma : \mathcal{V} \to \mathcal{T}$ une substitution. On a vu que σ s'étend en une application, notée aussi σ de $\mathcal{T}$ dans $\mathcal{T}$ (1.2) . On définit alors une application de $F(\mathcal{L})$ dans $F(\mathcal{L})$ ($F(\mathcal{L})$ étant l'ensemble des formules du langage $\mathcal{L}$), que nous noterons encore σ; $\sigma(F)$ est définie par induction:

– Si F est une formule atomique $R(t_1, \ldots, t_n)$, alors $\sigma(F)$ est la formule $R(\sigma(t_1), \ldots, \sigma(t_n))$.

– Si $F = \neg G$ (respectivement $(G \wedge H)$, $(G \vee H)$), alors $F = \neg\sigma(G)$ (respectivement $(\sigma(G) \wedge \sigma(H))$, $(\sigma(G) \vee \sigma(H))$).

– Si $F = \exists v\, G$, (respectivement $F = \forall v\, G$) alors $\sigma(F)$ est la formule $\exists v\, \sigma'(G))$ (respectivement $\sigma(F)$ est la formule $\forall v\, \sigma'(G))$, où $\sigma' : \mathcal{V} \to \mathcal{T}$ est la substitution définie par $\sigma'(w) = \sigma(w)$ pour toute variable $w \neq v$, et $\sigma'(v) = v$.

Lorsque σ est la substitution $[t_1/v_1, \ldots, t_k/v_k]$, la formule $\sigma(F)$ est notée $F[t_1/v_1, \ldots, t_k/v_k]$. C'est donc la formule obtenue en remplaçant simultanément dans F, chaque occurrence *libre* de la variable v_i par le terme t_i $(1 \leq i \leq k)$.
Par exemple, $(\forall v_1(v_1 \leq v_2 \rightarrow v_1 \leq v_3) \rightarrow v_1 + v_2 \leq v_1 + v_3)[t_1/v_1, t_2/v_2, t_3/v_3]$ est la formule $(\forall v_1(v_1 \leq t_2 \rightarrow v_1 \leq t_3) \rightarrow t_1 + t_2 \leq t_1 + t_3)$.

Malheureusement, cette opération de substitution dans les formules n'a pas toujours le comportement attendu, à cause du phénomène dit de "capture des variables". C'est pourquoi on impose habituellement la restriction suivante : la substitution $[t_1/v_1, \ldots, t_k/v_k]$ ne sera effectuée dans une formule F que si *aucune variable liée dans F n'apparaît dans les termes $t_1, \ldots, t_k$*. En particulier, lorsque $t_1, \ldots, t_k$ sont des termes clos, la substitution $[t_1/v_1, \ldots, t_k/v_k]$ peut toujours être effectuée.

La raison de cette restriction est sémantique et non syntaxique : sans cette restriction, le sens de la formule obtenue par substitution peut ne pas être celui qu'on attend. Par exemple, si F est la formule $\forall y(x \leq y)$, la signification de F est "x est le plus petit élément"; on voudrait donc que la signification de $F[t/x]$ soit "t est le plus petit élément". Or $F[y/x]$ est $\forall y(y \leq y)$ dont le sens n'est pas "y est le plus petit élément".

Cette restriction n'est, en fait, pas bien grave. En effet, pour pouvoir effectuer, dans F, la substitution $[t_1/v_1, \ldots, t_k/v_k]$, il suffit de changer le nom des variables liées de F (voir proposition 5 un peu plus loin). Cette opération transforme F en une formule qui a le même sens. Dans l'exemple précédent, on remplace la formule $F = \forall y(x \leq y)$ par la formule $F' = \forall z(x \leq z)$, obtenue en changeant la variable liée y en z dans F. Alors $F'[y/x]$ est $\forall z(y \leq z)$, qui a bien la signification voulue.

3.2 Quelques équivalences

On peut vérifier:

Proposition 3 *$\exists v(F \vee G)$ équivaut à $(\exists v\, F \vee \exists v\, G)$ et $\forall v(F \wedge G)$ équivaut à $(\forall v\, F \wedge \forall v\, G)$ quelles que soient les formules F, G.*
$Qv\,(F * G)$ équivaut à $(Qv\, F * G)$ si la variable v n'est pas libre dans G; quand Q est soit $\forall$, soit $\exists$, et $*$ est soit $\wedge$, soit $\vee$.

Proposition 4 *$\forall v \forall w\, F$ équivaut à $\forall w \forall v\, F$; $\exists v \exists w\, F$ équivaut à $\exists v \exists w\, F$;*
$\exists v\, F$ équivaut à $\neg \forall v \neg\, F$.

La proposition suivante va nous permettre de supposer que l'on ne considère que des formules propres, c'est à dire sans variable ambigue et permettre aussi de changer le nom de variables liées quand cela pose un problème pour effectuer une substitution. On rappelle que si la variable v est libre dans F alors $F[w/v]$ est le résultat de la substitution de toutes les occurences libres de v dans F par la variable w.

Proposition 5 (Changement de nom d'une variable liée) *Si la variable w n'apparaît pas dans la formule F, alors $\forall v\, F$ équivaut à $\forall w\, F[w/v]$, et $\exists v\, F$ équivaut à $\exists w\, F[w/v]$.*

Lemme 6 *Soit F une formule, et G une sous-formule de F. Si G' est une formule équivalente à G, alors la formule F' qui est la formule F dans laquelle on a remplacé la formule G par la formule G', est équivalente à F.*

Maintenant, soit F une formule et soit z une variable apparaissant liée dans une sous-formule G de F. Alors si v est une variable qui n'apparait pas du tout dans F, et si F' est la formule dans laquelle on a remplacé, dans la sous-formule G la variable z par la variable v, alors F et F' sont équivalentes. On en déduit que si $v_1, \ldots, v_n$ sont des variables apparaissant liées dans F et si $z_1, \ldots, z_n$ sont de nouvelles variables n'apparaissant pas dans F alors, la formule F', dans laquelle on a remplacé chaque occurence de v_i par z_i est équivalente à F.

On en déduit:

Corollaire 7 *Soit F une formule, alors il existe une formule propre G telle que F et G sont équivalentes.*

Preuve par induction du corollaire:
Si F est une formule atomique, alors F est propre puisque toutes les occurences des variables dans F sont libres.
Si $F = \neg G$, alors, soit, par induction H une formule propre équivalente à G. Alors F et $\neg H$ sont équivalentes et $\neg H$ est propre.
Si $F = (G \wedge H)$; tout d'abord par induction soient G' et H' des formules propres équivalentes respectivement à G et H. Soient $v_1, \ldots, v_n$ les variables apparaissant liées dans G et ayant au moins une occurence dans H (si il y en a). On choisit alors de nouvelles variables $z_1, \ldots, z_n$ n'apparaissant ni dans G ni dans H et on remplace G par la formule équivalente G' dans laquelle on a remplacé v_i par z_i. On fait ensuite de même pour les variables liées de H.
Si $F = \exists v\, G$, et si G est propre, alors F est propre.
Idem pour $F = (G \vee H)$ et $F = \forall v\, G$.

On peut également montrer:

Proposition 8 *Soit F une formule, alors il existe une formule G équivalente à F qui est sous forme prénexe, c'est-à-dire telle que $G = Q_1 v_1 Q_2 v_2 \ldots Q_n v_n H$, où H est une formule sans quantificateurs et $Q_i v_i$ est soit $\exists v_i$ soit $\forall v_i$.*