Chapitre 4

Calcul des prédicats

4.1 Introduction

Le calcul des propositions est bien trop limité pour décrire des situations réelles. En effet il ne permet que de décrire des phrases dont la vérité ne dépend pas des individus (par exemple « Il pleut ») ; il ne peut pas représenter des phrases qui mettent en jeu des individus ou des objets (par exemple « Si x est le père de y et si z est le père de x alors z est un grand-père de y » ou « Tout individu a un père »).

Le calcul des prédicats (ou Logique du Premier Ordre) permet d'exprimer de telles relations entre individus, il est donc bien plus riche que le calcul propositionnel. En premier lieux, il contient des individus (ou entités) (donnés par des symboles de variables $x, y, z, \ldots$). Il contient des fonctions $(f, g, \ldots, s, \ldots)$ permettant de transformer des entités en autres entités (par exemple la fonction qui associe une personne à son père), et des relations $(\ldots, P, Q, R, \ldots)$ permettant de lier les individus entre eux.

Les relations appliquées aux entités (par exemple $R(x, f(y))$) peuvent être évaluées à vrai ou faux (selon les valeurs attribuées aux entités, aux fonctions et aux relations) et servent de briques de base à un langage du premier ordre obtenu à l'aide des connecteurs logiques du calcul propositionnel et de deux autres connecteurs appelés quantificateurs.

Le calcul des prédicats est donc très similaire à celui des propositions. On aura des formules définies inductivement à partir des symboles de prédicats et de fonctions. On les interprétera dans divers mondes possibles et alors elles deviendront vraies ou fausses. On aura également un système formel correct et complet pour démontrer ou réfuter des formules.

Il y a néanmoins une différence algorithmique importante : le calcul des prédicat est indécidable : il est absolument impossible de vérifier qu'une formule est vraie pour toute interprétation. Ceci vient du fait que :

1. il existe un nombre non borné d'interprétations possible. Il n'est donc pas possible de toutes les tester une à une
2. les interprétations comportent en général une infinité d'individus, il est donc pas toujours possible de vérifier qu'une interprétation donnée est modèle d'une formule (par exemple de vérifier que $\forall x \varphi$ puisque x peut prendre une infinité de valeurs différentes).

Il est important pour la suite de commencer par bien revoir les notions de base sur relations et ensembles, ainsi que les définitions inductives et en particulier celle des termes. Toutes ces notions ont été introduites durant la première semaine de cours (section *L'induction* dans AMeTICE).

Un exemple introductif

Avant d'en venir aux définitions formelles, voici quelques formules du premier ordre. Ici, P et Q désignent deux relations binaires et f une fonction unaire. Les lettres x, y et z désignent des variables. Vous pouvez reconnaitre également les connecteurs logique introduits dans le calcul propositionnel, ainsi que deux quantificateurs que vous connaissez certainement $\forall$ qui se lit « pour tout » et $\exists$ qui se lit « il existe ».

$\varphi_G : \forall x \forall y \forall z (P(x, y) \wedge P(y, z)) \Rightarrow G(x, z)$
$\varphi_P : \forall x \exists y P(y, x)$
$\varphi_C : \forall x \exists y G(y, x)$
$\varphi_D : \forall x \forall z P(z, f(x)) \Rightarrow G(z, x)$
$\varphi_F : (\varphi_G \wedge \varphi_P) \Rightarrow \varphi_C$.

Il est ici impossible de donner une valeur de vérité à toutes ces formules, et ce pour différentes raisons :

— on ne sait pas dans quel ensemble D sont prises les valeurs x, y, z
— on ne connait pas la valeur de la fonction $f : D \to D$
— on ne connait pas la valeur des relations $P \subseteq D \times D$, et $G \subseteq D \times D$

Il est donc nécessaire de choisir une interprétation pour évaluer ces formules. Toutefois, nous verrons que c'est inutile pour la formule φ_F qui est vraie pour toute interprétation (c'est une tautologie, ou un théorème).

Considérons donc diverses interprétations de ces formules.

Interprétation 1

Les individus sont les êtres humains. La relation $P(x, y)$ signifie que x est le père de y. La relation $G(x, y)$ signifie que x est un grand-père de y. La fonction f associe à un individu sa mère.

φ_G signifie alors : pour tous êtres humains x, y, z, si (x est le père de y et y est le père de z) alors (x est un grand-père de z).

φ_P signifie : « pour tout individu x il existe un individu y tel que y est le père de x » soit, plus simplement, « tout individu a un père ».

φ_C signifie que « pour tout individu x il existe un individu y tel que y est le grand-père de x » soit, plus simplement, « tout individu a un grand-père ».

φ_D dit que si z est le père de la mère de x alors z est un grand père de x.

Ces quatre formules sont vraies dans cette interprétation [1].

L'implication $\varphi_F : ((\varphi_G \wedge \varphi_P) \Rightarrow \varphi_C)$ est donc vraie dans cette interprétation.

On remarquera que les deux formules φ_P et φ_G sont loin de modéliser toutes les propriétés des relations G et P. On n'a pas dit que « le père de chaque individu est unique », ni qu'« un individu x peut-être le grand-père d'un autre z sans qu'il existe un individu dont x soit le père et qui soit le père de z » (le grand-père maternel).

Interprétation 2

Les individus sont les quatre sommets a, b, c, d du graphe suivant : $\begin{array}{ccc} a & \to & b \\ \uparrow & & \downarrow \\ d & \leftarrow & c \end{array}$

$P(x, y)$ signifie que x précède immédiatement y sur le graphe.

$G(x, y)$ signifie que x suit immédiatement y sur le graphe.

La formule φ_P signifie que tout point a un prédécesseur immédiat, et elle vraie.

La formule φ_G signifie que pour tous points x, y, z, si x précède immédiatement y et si y précède immédiatement z, alors x suit immédiatement z. Elle est fausse. Finalement la formule φ_C signifie que tout point a un successeur immédiat. Elle est également vraie.

L'implication $((\varphi_P \wedge \varphi_G) \Rightarrow \varphi_C)$ est donc vraie dans cette interprétation.

Interprétation 3

Les individus sont les nombres entiers positifs.

$P(x, y)$ signifie que $y = x + 1$. Par exemple $P(4, 5)$ est vraie, mais $P(5, 4)$ est fausse.

$G(x, y)$ signifie que $y = x + 2$. Par exemple $P(4, 6)$ est vraie, mais $P(6, 4)$ est fausse.

1. Sauf peut-être φ_P : soit il y a un premier homme et celui-ci n'a pas de père, soit on se retrouve peu à peu, en remontant l'évolution, à inclure dans le genre humains des singes, des poissons, des bactéries, ...

La formule φ_P signifie alors que pour tout entier y, il existe un entier x tel que $y = x + 1$. Elle est fausse : pour $y = 0$ un tel entier positif n'existe pas.

La formule φ_G signifie que pour tous entiers x, y, z, si $y = x + 1$ et $z = y + 1$ alors $z = x + 2$. Elle est vraie.

Finalement la formule φ_C signifie que pour tout entier x, il existe un entier z tel que $x = z + 2$. Elle est fausse : pour $x = 0$ il n'existe pas de tel entier positif.

L'implication $((\varphi_P \wedge \varphi_G) \Rightarrow \varphi_C)$ est donc vraie dans cette interprétation.

Comparaison des interprétations

On est donc tout à fait libre d'interpréter les formules dans un « monde » de son choix, de sorte que certains énoncés deviennent vrais ou faux. On remarque néanmoins que pour chacune des interprétations considérées, l'implication $((\varphi_P \wedge \varphi_G) \Rightarrow \varphi_C)$ est vraie. Ce n'est pas un hasard, cette formule est une tautologie du calcul des prédicats. Elle est vraie dans toute interprétation.

4.2 Expressions et formules

4.2.1 Les termes

On rappelle brièvement la notion de termes introduite Section 2.3.2.

Les termes sont des arbres ordonnés étiquetés particuliers. Ils jouent un rôle essentiel dans beaucoup de structures en informatique.

Définition 4.1 (Signature)**.** Une *signature* est un ensemble $\mathcal{S}$ de symboles muni d'une application $\rho : \mathcal{S} \to \mathbb{N}$, appelée *arité*.

On écrira une signature comme un ensemble de couples. Par exemple, $\{ (f, 2), (g, 1), (h, 0) \}$ est la signature dont les symboles sont f, g, h, d'arité $2, 1$ et 0, respectivement. Formellement, on a ici $\mathcal{S} = \{ f, g, h \}$, $\rho(f) = 2$, $\rho(g) = 1$, $\rho(h) = 0$. Un symbole $f \in \mathcal{S}$ tel que $\rho(f) = 0$ est appelé *constante*.

Définition 4.2 (Termes)**.** Étant donné une signature $\mathcal{S}$ et un ensemble X (de variables individuelles), l'ensemble $\mathcal{T}_{\mathcal{S}}(X)$ est défini inductivement par :

$$\frac{}{x \in X} \qquad \frac{t_1 \quad \dots \quad t_n}{f(t_1, \dots, t_n)} \text{ pour tout } f \in \mathcal{S} \text{ d'arité } n.$$

Un terme est donc une expression formée à partir de X en utilisant les symboles de $\mathcal{S}$ de sorte qu'un symbole f soit appliqué à un nombre de termes égal à $\rho(f)$. En particulier, si $f \in \mathcal{S}$ est une constante, alors elle s'applique a une liste vide de termes : $f()$ est un terme ; pour simplifier la notation, on écrit également f.

4.2.2 Le langage

Définition 4.3 (Langage)**.** Un *langage* (ou *vocabulaire*) du premier ordre est la donnée d'un couple de signatures $\mathcal{S} = (\mathcal{S}_{\mathtt{f}}, \mathcal{S}_{\mathtt{r}})$ disjointes (i.e. avec $\mathcal{S}_{\mathtt{f}} \cap \mathcal{S}_{\mathtt{r}} = \varnothing$).

On considère que :
— les éléments de $\mathcal{S}_{\mathtt{f}}$ sont les *symboles de fonction* du langage ;
— les éléments de $\mathcal{S}_{\mathtt{r}}$ sont les *symboles de relation* (ou de prédicat) du langage.

Remarque 4.4.

1. Rappelons qu'une constante est un symbole (de fonction) d'arité 0.
2. On considérera (sauf mention contraire) que chaque langage contient le symbole de relation binaire $=$ et un symbole de relation d'arité 0, $\perp$ qui représentera le faux. Un langage contenant le symbole binaire $=$ sera appelé **langage égalitaire**.

3. Le rôle des relations et des fonctions est très différent. Les fonctions et constantes seront utilisés pour construire les termes (i.e., les objets du langage) tandis que les relations serviront à construire des formules (i.e., des propriétés sur ces objets)

   Par exemple $1+2$ est un terme, il désigne un objet, tandis que $1+2=3$ désigne une formule logique.

Exemple 4.5.

1. Le langage $\mathcal{L}_1$ de la théorie des groupes contient les symboles
   — de constante : e ;
   — de fonction : $*$ (binaire) et inv (unaire) ;
   — de relation : $=$ (binaire).
   De façon plus compacte, on notera $\mathcal{L}_1 = (\{(e,0),(*,2)\},\varnothing)$ (on ne représente pas la relation $=$ puisqu'on a choisi de la considérer toujours incluse par convention).
2. Le langage $\mathcal{L}_2$ de la théorie des ensembles contient les symboles
   — de constante : $\varnothing$;
   — de fonction : $\cap$ et $\cup$ binaires, C unaire (le complément) ;
   — de relation : $=$, $\in$ et $\subset$, tous binaires. [2]
   De façon plus compacte, on notera $\mathcal{L}_2 = (\{(\varnothing,0),(\cup,2),(\cap,2)\},\{(\in,2),(\subset,2)\})$.

4.2.3 Les formules du calcul des prédicats

On suppose fixés un langage $\mathcal{S} = (\mathcal{S}_\mathtt{f}, \mathcal{S}_\mathtt{r})$, et un ensemble $X = \{x, x_0, x_1, \ldots, y, y_0, y_1, \ldots, z, z_0, z_1, \ldots\}$ de variables.

Les formules du premier ordre sur $\mathcal{S}$ sont construites à partir d'éléments de base en utilisant les connecteurs de la logique propositionnelle $(\wedge, \vee, \neg, \Rightarrow)$ et deux quantificateurs : $\forall$ et $\exists$.

Les éléments de base sont appelés **formules atomiques** et sont construits en appliquant une relation de $\mathcal{S}_\mathtt{r}$ à des termes définis sur $\mathcal{S}_\mathtt{f}$ et X :

Définition 4.6. Une formule atomique sur $\mathcal{S}$ est une expression de la forme :

$$r(t_1, \ldots, t_n)$$

où $r \in \mathcal{S}_r$ est d'arité $n \geq 0$ et $t_1, \ldots, t_n \in \mathcal{T}_{\mathcal{S}_f}$ sont des termes.

Définition 4.7 (Formules)**.** Etant donné un langage $\mathcal{S}$, l'ensemble $\mathcal{F}_{\text{po}}(\mathcal{S})$ des formules du premier ordre sur $\mathcal{S}$ est défini inductivement par

$$\frac{}{\varphi}\ \varphi \text{ formule atomique}$$

$$\frac{\varphi_1 \quad \varphi_2}{(\varphi_1 \vee \varphi_2)} \qquad \frac{\varphi_1 \quad \varphi_2}{(\varphi_1 \wedge \varphi_2)} \qquad \frac{\varphi_1 \quad \varphi_2}{(\varphi_1 \Rightarrow \varphi_2)}$$

$$\frac{\varphi}{(\neg\varphi)} \qquad \frac{\varphi}{(\exists x \varphi)}\ x \in X \qquad \frac{\varphi}{(\forall x \varphi)}\ x \in X$$

Les éléments de base $r(t_1, \ldots, t_n)$ sont appelées formules atomiques : il s'agit simplement de relations appliquées à des termes.

Comme pour les formules du calcul propositionnel, les parenthèses sont utilisées pour lever les ambiguité possibles de cette définition. On se permettra souvent de supprimer les parenthèses superflues.

Exemple 4.8. Reprenons le langage $\mathcal{L}_1$ de l'exemple 4.6. Les expressions suivantes sont des formules atomiques :

$=(*(x,y),e)$ qu'on pourra écrire $x * y = e$ pour plus de lisibilité,
$=(*(y,x),e)$ qu'on pourra écrire $y * x = e$,
$=(x,e)$ qu'on pourra écrire $x = e$,
$=(y,e)$ qu'on pourra écrire $y = e$

2. En fait, en théorie des ensembles, seulement les symboles $=$ et $\in$ sont considérés élémentaires. Les autres se définissent à partir de ces deux.

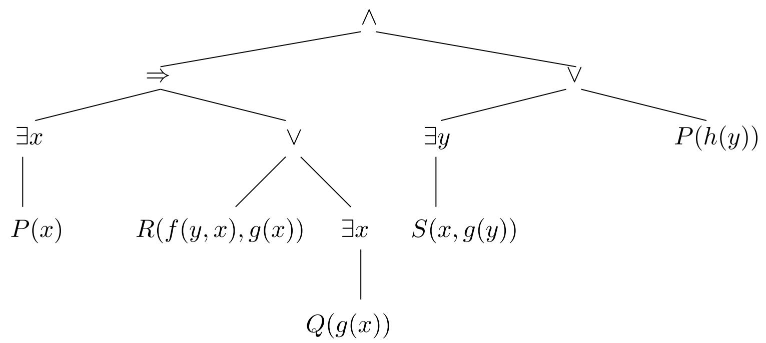
Par conséquent, les expressions suivantes sont des formules du premier ordre :
$\forall x \exists y((x * y = e) \wedge (\neg(y * x = e)))$
$\forall x((x = e) \vee \exists y(\neg(y = e) \wedge (y + x = e)))$

Dans le langage $\mathcal{L}_2$ du même exemple, $\forall x \forall y(x \cap y = \varnothing \Rightarrow (x = \varnothing \wedge y = \varnothing))$ est une formule.

Remarquez que, comme pour les termes, les formules peuvent être vues comme des arbres dont les feuilles sont des formules atomiques et les noeuds sont les connecteurs et quantificateurs. Par exemple, la formule

$$[(\exists x P(x)) \Rightarrow (R(f(y,x), g(x)) \vee [\exists x Q(g(x))])] \wedge [(\exists y S(x, g(y))) \vee P(h(y))] \tag{4.1}$$

sera représentée **de façon unique** par l'arbre suivant :



4.2.4 Occurrences libres et liées d'une variable

Une variable x peut apparaitre plusieurs fois à l'intérieur d'une formule. Chaque apparition de la variable (excepté quand elle apparait derrière un quantificateur) est appelée une occurrence. Par exemple, dans la formule $(\forall y\, P(x,y)) \vee Q(y)$, la variable x a une seule occurrence (dans $P(x,y)$), et la variable y en a deux : la première dans $P(x,y)$ et la seconde dans $Q(y)$.

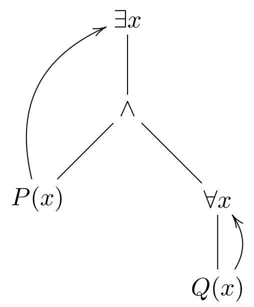
Définition 4.9. Une occurrence d'une variable x dans une formule φ est dite **liée** si elle apparait dans une sous-formule de φ de la forme $\exists x \psi$, ou bien $\forall x \psi$.

Autrement, elle est dite **libre**.

Exemple 4.10. Dans la formule $(\forall y\, P(x,y)) \vee Q(y)$, l'occurrence de x est libre, la première occurrence de y à liée à $\forall y$, et la seconde est libre.

Définition 4.11. Une occurrence liée d'une variable x est liée au quantificateur Qx (avec $Q \in \{\exists, \forall\}$) qui est son ancêtre le plus proche, dans l'arbre de représentation de la formule.

Exemple 4.12. Considérons la formule $\exists x P(x) \wedge \forall x Q(x)$. Les variables sont liées de la façon suivante :

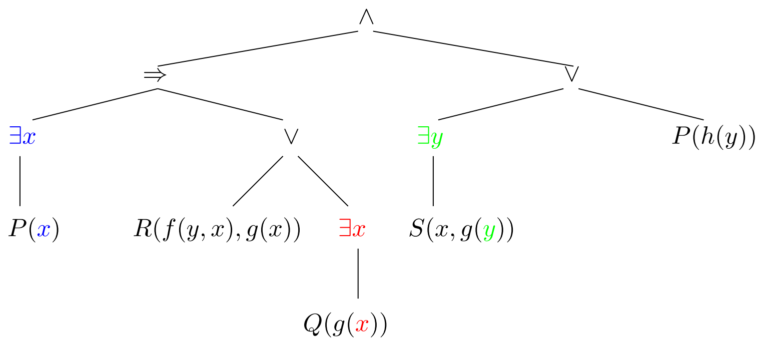


La distinction entre occurrence libre et occurrence liée est importante. Une occurrence liée ne possède pas d'identité propre et peut être remplacée par n'importe quel autre nom de variable qui n'apparaît pas dans la formule. Ainsi, $\exists x(x < y)$ est identique à $\exists z(z < y)$ mais pas à $\exists x(x < z)$ et encore moins à $\exists y(y < y)$.

Définition 4.13. Une variable est libre quand elle admet une occurrence libre, et elle est liée quand elle admet une occurrence liée.

Une variable peut donc être libre et liée comme dans la formule $P(x) \wedge \exists x Q(x)$: la première occurrence de x est libre, tandis que la seconde est liée.

Exemple 4.14. Considérons la formule (4.1) et son arbre :



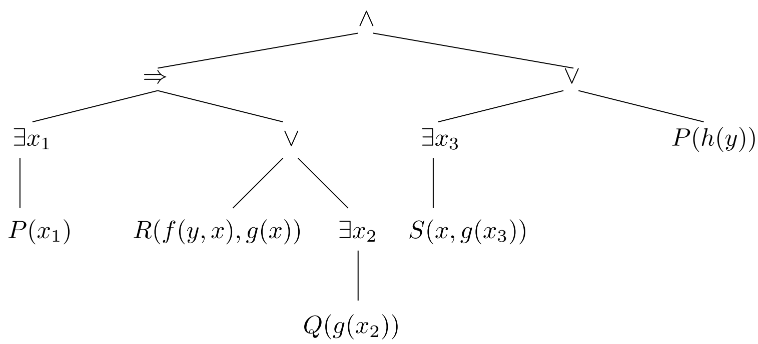
En observant cet exemple, on intuite que le fait d'avoir des variables à la fois libres et liées peut être source d'ambiguïté. Pour cela, on préférera considérer des formules **polies**.

Définition 4.15. Une formule est **polie** si pour toute variable x :

1. x n'est pas à la fois libre et liée
2. si deux occurrences de x sont liées, elle sont liées au même quantificateur (plus exactement, à la même occurrence d'un quantificateur).

Nous verrons par la suite que les occurrences des variables liées peuvent être renommée sans modifier la sémantique d'une formule, pour obtenir une formule polie.

Par exemple, la formule précédente peut-être renommée de la façon suivante :



La nouvelle formule est donc

$$(\,[\exists x_1 P(x_1)\,] \;\Rightarrow\; [\,(\exists x_2 Q(g(x_2))) \vee R(f(y,x),g(x))\,]\,) \wedge [\,(\exists x_3 S(x,g(x_3))) \vee P(h(y))\,]\;.$$

Définition 4.16 (Formule close)**.** Une formule φ est dite **close** ssi elle n'admet aucune variable libre.