Préparation Agrégation : Logique
Logique du premier ordre

Christine Paulin

3 novembre 2015

Résumé

Ce cours concerne les leçons suivantes :

- 917-Logique du premier ordre : syntaxe et sémantique.
- 918-Systèmes formels de preuve en logique du premier ordre : exemples.
- 924-Théories et modèles en logique du premier ordre. Exemples.

Programme : Logique du premier ordre

- Aspects syntaxiques. Langages, termes, formules. Variables libres et variables liées, substitutions, capture de variables.
- Systèmes formels de preuve. Calcul des séquents, déduction naturelle. Algorithme d'unification des termes. Preuves par résolution.
- Aspects sémantiques.
  - Interprétation d'une formule dans un modèle. Validité, satisfiabilité.
  - Théories cohérentes, théories complètes. Théories décidables, indécidables. Exemples de théories : égalité, arithmétique de Peano.
  - Théorème de complétude du calcul des prédicats du premier ordre.

Table des matières

Références

[David et al., 2004] David, R., Nour, K., and Raffalli, C. (2004). *Introduction à la Logique. Théorie de la démonstration (2ème édition)*. Sciences Sup. Dunod.

[Gallier, 1987] Gallier, J. H. (1987). *Logic for Computer Science, Fooundations of Automatic Theorem Proving*. Wiley.

[Goubault-Larrecq and Mackie, 1997] Goubault-Larrecq, J. and Mackie, I. (1997). *Proof Theory and Automated Deduction*, volume 6 of *Applied Logic Series*. Kluwer Academic Publishers.

1 Introduction

Le calcul propositionnel a un pouvoir d'expression limité. On peut introduire une infinité de variables propositionnelles, mais chaque formule ne peut traduire qu'une propriété d'un nombre fini de variables. On ne pourra pas exprimer de propriétés comme il existe une infinité de nombres premiers sans faire entrer en jeu des informations explicites sur comment trouver ces nombres premiers de manière bornée.

La logique du premier ordre (aussi appelée calcul des prédicats) est un cadre plus général qui distingue un langage de description d'objets pouvant faire intervenir des constantes, fonctions et variables et un langage de description de formules à partir de symboles de prédicats représentant des notions atomiques.

Le calcul des prédicats est un cadre suffisant pour les mathématiques usuelles à condition de se placer dans les bonnes théories comme la théorie de l'arithmétique de Peano ou la théorie des ensembles.

2 Aspects syntaxiques

2.1 Définitions

Définition 2.1 (Signature) *Une* signature *est un ensemble de* symboles*, chacun associé à un entier appelé son arité. Un symbole d'arité* 0 *est appelé une* constante*. On parle de symbole* unaire *(resp.* binaire*) pour indiquer une arité* 1 *(resp.* 2*).*

Définition 2.2 (Termes)
On se donne une signature *(*$\mathcal{F}$*) et un ensemble infini (*$\mathcal{X}$*) de* variables *de termes.*

On définit l'ensemble $\mathcal{T}_{\mathcal{F}}(\mathcal{X})$ *des termes avec variables construits sur la signature* $\mathcal{F}$ *comme le plus petit ensemble qui contient les variables, les constantes et tel que, pour tout symbole* f *d'arité* $n > 0$ *si on a des termes* $(t_i)_{i\in 1\dots n}$ *dans* $\mathcal{T}_{\mathcal{F}}(\mathcal{X})$ *alors le terme* $f(t_1, \dots, t_n)$ *est aussi dans* $\mathcal{T}_{\mathcal{F}}(\mathcal{X})$*.*

L'ensemble des termes se caractérise comme l'algèbre initiale engendrée par la signature. Deux termes qui ne commencent pas par le même symbole sont différents. On peut de plus utiliser un schéma de définition récursif par cas pour définir des fonctions sur les termes (cf le paragraphe 2.1.1).

Exemple 1 *Exemples de signatures*

- *les formules propositionnelles peuvent se voir comme des termes sur la signature* $\{\top, \bot, \neg, \wedge, \vee, \Rightarrow\}$
- *les entiers naturels peuvent se représenter avec la signature* $\{0, s\}$ *; dans la théorie arithmétique on ajoute les symboles binaires* $\{+, *\}$ *pour l'addition et la multiplication.*
- *Des structures informatiques comme les piles peuvent être modélisées à travers une signature* `empty`*,* `pop`*,* `push`*,* `top`*. En général en informatique on préfèrera une présentation* d'algèbre sortée *qui permet de distinguer plusieurs catégories d'objets comme ici les éléments contenus dans la pile et les piles. L'arité d'un symbole n'est plus alors représenté par un entier mais par un couple* $[s_1; \dots; s_n] \to s$ *formé d'une suite finie de sortes correspondant aux sortes attendues des arguments (suite vide dans le cas des constantes) et la sorte résultat de la fonction. Ainsi pour l'exemple des piles en introduisant deux sortes* e *pour les éléments et* p *pour les piles on aurait* $\texttt{empty} : [] \to p, \texttt{pop} : [p] \to p, \texttt{push}[e; p] \to p, \texttt{top} : [p] \to e$ *plus des opérations permettant de construire des éléments de la sorte* e*.*

2.1.1 Opérations sur les termes

On introduit un certain nombre de définitions sur les termes (récursivement sur la structure des termes)

- l'ensemble $\mathsf{var}(t)$ des variables d'un terme t

$$\mathsf{var}(x) = \{x\} \qquad \mathsf{var}(f(t_1, \dots, t_n)) = \bigcup_{i=1\dots n} \mathsf{var}(t_i)$$

on appelle *terme clos* un terme sans variable.

- Une *substitution* est une application des variables dans les termes qui est l'identité sauf sur un nombre fini de variables (appelé *support* ou *domaine* de la substitution et noté $\mathsf{dom}(\sigma)$).
  Une substitution pourra aussi être notée $[u_1/x_1; \ldots; u_n/x_n]$.
  On introduit l'ensemble varim des variables de l'image de la substitution c'est-à-dire $\mathsf{varim}(\sigma) \stackrel{\text{def}}{=} \bigcup_{x \in \mathsf{dom}(\sigma)} (\mathsf{var}(\sigma(x)))$.
- La substitution des variables est étendue en une opération sur les termes notée $t\sigma$.

$$x\sigma = \sigma(x) \qquad (f(t_1, \ldots, t_n))\sigma = f(t_1\sigma, \ldots, t_n\sigma)$$

  On dira que $t\sigma$ est une *instance* du terme t.
- Les substitutions se composent, on note $\sigma\tau$ la substitution définie par $(\sigma\tau)(x) = (\sigma(x))\tau$. La substitution $\sigma\tau$ correspond à la substitution σ suivie de la substitution τ. On a $t(\sigma\tau) = (t\sigma)\tau$

2.1.2 Formules du calcul des prédicats

Définition 2.3 (Formules du Calcul des Prédicats)

- *On se donne une signature pour les termes ($\mathcal{F}$) et une signature pour les symboles de prédicat ($\mathcal{R}$), chaque symbole est muni d'une arité.*
- *Une* formule atomique *est de la forme $R(t_1, \ldots, t_n)$ avec $R \in \mathcal{R}$ d'arité n et $t_i \in \mathcal{T}_{\mathcal{F}}(\mathcal{X})$*
- *L'ensemble des formules du calcul des prédicats est le plus petit ensemble qui contient les formules atomiques, les constantes propositionnelles $\bot$ et $\top$, qui est clos par les constructions propositionnelles $\{\neg P, P \wedge Q, P \vee Q, P \Rightarrow Q\}$ et par les quantificateurs universels et existentiels $\forall x, P$ et $\exists x, P$.*

Définition 2.4 (Variables libres, variables liées) *On définit l'ensemble des variables libres ($\mathsf{FV}(P)$) et l'ensemble des variables liées ($\mathsf{BV}(P)$) d'une formule par les équations suivantes (avec $\circ \in \{\wedge, \vee, \Rightarrow\}$ et $\mathcal{Q} \in \{\forall, \exists\}$:*

$\mathsf{FV}(R(t_1, \ldots, t_n))$	$= \bigcup_{i=1}^{i=n} \mathsf{var}(t_i)$	$\mathsf{BV}(R(t_1, \ldots, t_n))$	$= \emptyset$
$\mathsf{FV}(\neg P)$	$= \mathsf{FV}(P)$	$\mathsf{BV}(\neg P)$	$= \mathsf{BV}(P)$
$\mathsf{FV}(P \circ Q)$	$= \mathsf{FV}(P) \cup \mathsf{FV}(Q)$	$\mathsf{BV}(P \circ Q)$	$= \mathsf{BV}(P) \cup \mathsf{BV}(Q)$
$\mathsf{FV}(\mathcal{Q}x, P)$	$= \mathsf{FV}(P) \backslash \{x\}$	$\mathsf{BV}(\mathcal{Q}x, P)$	$= \mathsf{BV}(P) \cup \{x\}$

Remarques :
- Une variable peut apparaître à la fois libre et liée (à différentes positions dans la formule).
- Les variables liées sont muettes, dans le sens que le nom introduit sert uniquement à faire le lien entre une occurrence de variable dans un terme et un quantificateur dans la formule.

Définition 2.5 (Substitution sur les formules)
L'opération de substitution s'étend des termes vers les formules. Elle n'affecte que les variables libres d'une formule, elle est compatible avec l'opération de renommage.

$R(t_1, \ldots, t_n)\sigma$	$= R(t_1\sigma, \ldots, t_n\sigma)$	
$\top\sigma$	$= \top$	
$\bot\sigma$	$= \bot$	
$(\neg P)\sigma$	$= \neg(P\sigma)$	
$(P \circ Q)\sigma$	$= P\sigma \circ Q\sigma$	
$(\mathcal{Q}x, P)\sigma$	$= \mathcal{Q}y, (P([y/x]\sigma))$	$y \notin \mathsf{FV}(\mathcal{Q}x, P) \cup \mathsf{varim}(\sigma) \cup \mathsf{dom}(\sigma)$

On considère l'ensemble des formules modulo le renommage des variables liées :
si $y \notin \mathsf{FV}(\mathcal{Q}x, P)$ alors $\mathcal{Q}x, P \equiv \mathcal{Q}y, P[y/x]$.

3 Aspects Sémantiques

3.1 Interprétation

Définition 3.1 (Interprétation d'une signature) *Pour interpréter une formule logique, on choisit l'univers dans lequel interpréter les objets (on parle du domaine de l'interprétation) on interprète ensuite chaque symbole de la signature comme une opération sur ce domaine (application ou relation). Une interprétation se compose donc des éléments suivants :*

- *le domaine D, qui est un ensemble non vide*
- *l'interprétation de chaque symbole de fonction f d'arité n par une fonction $f_I : D^n \to D$*
- *l'interprétation de chaque symbole de prédicat R d'arité n par une relation $R_I \subseteq D^n$*
- *interprétation des variables par une application de $\mathcal{X}$ dans D (appelée environnement)*
- *on notera $\rho[v/x]$ environnement dans lequel la valeur de x est v et la valeur de $y \neq x$ est $\rho(y)$.*

Définition 3.2 (Sémantique)
Soit une signature $\mathcal{F}$ pour les termes et une signature $\mathcal{R}$ pour les prédicats. On se donne une interprétation $I = (D, (f_I)_{f\in\mathcal{F}}, (R_I)_{R\in\mathcal{R}})$. Pour un environnement ρ quelconque, on définit :

- *La valeur $[\![t]\!]_{I,\rho}$ d'un terme qui est un élément de D*

$$[\![x]\!]_{I,\rho} = \rho(x) \quad x \in \mathcal{X} \qquad\qquad [\![f(t_1,\ldots,t_n)]\!]_{I,\rho} = f_I([\![t_1]\!]_{I,\rho},\ldots,[\![t_n]\!]_{I,\rho})$$

- *On définit la valeur $[\![P]\!]_{I,\rho}$ d'une formule P comme une valeur de vérité, on ne donne ici que le cas des formules atomiques et des quantificateurs, les connecteurs propositionnels se comportant comme dans le cas du calcul propositionnel.*

$$\begin{array}{ll} [\![R(t_1,\ldots,t_n)]\!]_{I,\rho} & = V \text{ ssi } R_I([\![t_1]\!]_{I,\rho},\ldots,[\![t_n]\!]_{I,\rho}) \\ [\![\forall x, P]\!]_{I,\rho} & = V \text{ ssi pour tout } d \in D, [\![P]\!]_{I,\rho[d/x]} = V \\ [\![\exists x, P]\!]_{I,\rho} & = V \text{ ssi il existe } d \in D \text{ tq } [\![P]\!]_{I,\rho[d/x]} = V \end{array}$$

- *Une formule est valide ssi elle est vraie pour toute interprétation et tout environnement.*
- *Une formule est insatisfiable ssi elle est fausse pour toute interprétation et tout environnement, elle est satisfiable dans le cas contraire*
- *La valeur de vérité d'une formule ne dépend que de la valeur de l'environnement sur les variables libres de la formule, en particulier la valeur de vérité d'une formule close ne dépend pas de l'environnement (on écrira plus simplement $[\![P]\!]_I$).*
- *Un modèle d'une formule ou d'un ensemble de formules closes est une interprétation qui valide l'ensemble des formules.*
- *On définit comme dans le cas propositionnel les notions de conséquence logique (notée $\mathcal{E} \models P$), et d'équivalence (notée $P \equiv Q$).*

Remarque Une substitution remplace une variable par des termes syntaxiques. Un environnement interprète les variables comme des valeurs sémantiques dans le domaine.

Définition 3.3 *On peut composer une substitution σ et un environnement ρ dans une interprétation I, cela donne un nouvel environnement noté $(\sigma\rho)$ et défini par $(\sigma\rho)(x) \stackrel{\text{def}}{=} [\![\sigma(x)]\!]_{I,\rho}$*

Proposition 3.1 (Validité et substitution) *Soit P une formule, σ une substitution, I une interpétation et ρ un environnement $[\![P\sigma]\!]_{I,\rho} = [\![P]\!]_{I,\sigma\rho}$*

On déduit de cette propriété que lorsqu'une formule est valide (resp. insatisfiable) alors toutes ses instances sont aussi valides (resp. insatisfiables).

3.2 Equivalence

Parmi les équivalences remarquables on a

- Loi de De Morgan pour les quantificateurs

$$\neg(\exists x, P) \equiv \forall x, \neg P \qquad \neg(\forall x, P) \equiv \exists x, \neg P$$

- L'ordre de deux quantificateurs universels ou deux quantificateurs existentiels n'a pas d'importance

$$(\exists x, \exists y, P) \equiv (\exists y, \exists x, P) \qquad (\forall x, \forall y, P) \equiv (\forall y, \forall x, P)$$

- La quantification existentielle généralise la disjonction et la quantification universelle généralise la conjonction. Cela nous donne des règles qui peuvent se voir comme des règles de distributivité.

$$(\exists x, P) \vee (\exists x, Q) \equiv \exists x, (P \vee Q) \qquad (\forall x, P) \wedge (\forall x, Q) \equiv \forall x, (P \wedge Q)$$

Exercice 3.1

- *Montrer que l'on a* $\exists x, (A \wedge B) \models (\exists x, A) \wedge (\exists x, B)$ *et* $(\forall x, A) \vee (\forall x, B) \models \forall x, (A \vee B)$ *mais qu'il n'y a pas équivalence*
- *Montrer que* $\exists x, \forall y, A \models \forall y, \exists x, A$ *mais qu'il n'y a pas équivalence*
- *Comparer les formules* $\forall x, (A \Rightarrow B)$ *;* $(\exists x, A) \Rightarrow B)$ *;* $(\forall x, A) \Rightarrow B)$ *et* $\exists x, (A \Rightarrow B)$ *lorsque* $x \notin \mathsf{FV}(B)$
- *Montrer que si* $A \models B$ *alors* $C \circ A \models C \circ B$ *et* $\mathcal{Q}x, A \models \mathcal{Q}x, B$
- *Montrer que si* $A \models B$ *alors* $\neg B \models \neg A$ *et* $B \Rightarrow C \models A \Rightarrow C$

Définition 3.4 (Formule prénexe)

- *Une formule est dite en* forme prénexe *(ou encore* formule prénexe*) lorsqu'elle s'écrit sous la forme* $\mathcal{Q}_1 x_1, \ldots, \mathcal{Q}_n x_n, P$ *avec* $\mathcal{Q}_i \in \{\forall, \exists\}$ *et* P *sans quantificateur.*
- *Une formule est dite* universelle *(resp.* existentielle*) si elle est en forme prénexe et que tous les quantificateurs sont des* $\forall$ *(resp.* $\exists$*).*

Proposition 3.2 *Toute formule est logiquement équivalente à une formule prénexe.*

Preuve: *On utilise les équivalences suivantes pour faire "remonter" les quantificateurs avec* $\circ \in \{\wedge, \vee, \Rightarrow\}$, $\mathcal{Q} \in \{\forall, \exists\}, \bar{\forall} = \exists, \bar{\exists} = \forall$.

$$A \circ (\mathcal{Q}x, B) \equiv \mathcal{Q}x, (A \circ B) \quad \neg(\mathcal{Q}x, B) \equiv \bar{\mathcal{Q}}x, \neg B \quad (\mathcal{Q}x, B) \Rightarrow A \equiv \bar{\mathcal{Q}}x, (B \Rightarrow A)$$

□

Développement 1 (forme de Herbrand, forme de Skolem)

- *A toute formule* P *on peut associer une formule* P' *existentielle (appelée* forme de Herbrand *de* P*) qui est valide si et seulement si* P *l'est.*
- *A toute formule* P *on peut associer une formule* P' *universelle (appelée* forme de Skolem *de* P*) qui est satisfiable si et seulement si* P *l'est.*

Preuve: *On introduit ici deux méthodes de mise en forme de Skolem (on dit aussi Skolemisation).*

Une première méthode consiste à mettre la formule sous forme prénexe, puis si on a une alternance de quantificateurs $P \overset{\text{def}}{=} \forall x_1, \ldots \forall x_n, \exists y, Q$ *on choisit un nouveau symbole de fonction* f *d'arité* n *et on remplace* P *par* $\forall x_1, \ldots \forall x_n, Q[f(x_1, \ldots, x_n)/y]$.

On élimine ainsi tous les connecteurs existentiels.

Une seconde méthode consiste à mettre la formule P *en forme normale de négation (on élimine les implications et les négations sont repoussées aux formules atomiques). On s'intéresse ensuite aux sous-formules* B *de la forme* $\exists y, Q$*. Soit* $x_1, \ldots, x_n$ *les variables libres de* B*, on choisit un nouveau symbole de fonction* f *d'arité* n *et on remplace* B *par* $Q[f(x_1, \ldots, x_n)/y]$*. Cette seconde méhode permet parfois d'avoir des symboles d'arité moins importante.*

Exemple. *Mettre sous forme de Skolem la formule* $\forall x, (\exists y, (P(x,y) \vee \exists z, Q(y,z)))$

Exercice 3.2 *Pour les deux transformations ci-dessus, montrer que*

- *toute interprétation qui satisfait* P' *satisfait aussi* P *(i.e.* $P' \models P$*)*
- *toute interprétation de la formule* P *initiale peut s'étendre en une interprétation de la formule* P' *obtenue.*
  On pourra procéder en deux temps
  — *montrer que si* P' *est obtenu à partir de* P *en remplaçant la sous-formule* $(\exists y, Q)$ *par* $Q[f(x_1, \ldots, x_n)/y]$ *et que* $FV(\exists y, Q) = \{x_1, \ldots, x_n\}$ *alors* $\forall x_1 \ldots x_n, ((\exists y, Q) \Leftrightarrow Q[f(x_1, \ldots, x_n)/y]) \models P \Leftrightarrow P'$
  — *Montrer que tout modèle de* P *peut s'étendre en un modèle de* $(\exists y, Q) \Leftrightarrow Q[f(x_1, \ldots, x_n)/y]$

La forme de Herbrand de P *pourrait s'obtenir à partir de la négation de la forme de Skolem de* $\neg P$*. On a* P *valide ssi* $\neg P$ *insatisfiable ssi la forme de Skolem de* $\neg P$ *est insatisfiable ssi la négation de la forme de Skolem de* $\neg P$ *est valide.*

De manière plus directe, si on a une forme prénexe $P \stackrel{\text{def}}{=} \exists x_1, \ldots \exists x_n, \forall y, Q$ *on introduit un nouveau symbole de fonction* n*-aire et on remplace* P *par la formule* P' *définie comme* $\exists x_1, \ldots \exists x_n, Q[f(x_1, \ldots, x_n)/y]$*. La formule* P *est vraie dans une interprétation* I *ssi* P' *est vraie pour toutes les extensions de* I *avec une interprétation de* f_I*.* □

Définition 3.5 (Mise en forme clausale) *En calcul des prédicats, un littéral est une formule atomique ou la négation d'une formule atomique, il peut contenir des variables libres.*

Une clause est une disjonction de littéraux quantifiés universellement (la quantification est souvent laissée implicite).

Pour toute formule P*, il existe un ensemble de clauses équisatisfiable.*

Preuve: *En effet on prend la forme de Skolem prénexe qui fait disparaitre les quantificateurs existentiels et donne une formule universelle equisatisfiable* $\forall x_1 \ldots x_n, Q$ *avec* Q *sans quantificateur. On met* Q *en forme clausale propositionnelle* $C_1 \wedge \ldots \wedge C_m$ *puis on utilise le fait que la quantification universelle est distributive par rapport à la conjonction pour se ramener à un ensemble de clauses* $\{(\forall x_1 \ldots x_n, C_1), \ldots, (\forall x_1 \ldots x_n, C_m)\}$
□

3.3 Modèle de Herbrand

On se donne deux signatures pour les fonctions et les prédicats $(\mathcal{F}, \mathcal{R})$, si $\mathcal{F}$ ne contient pas de symboles de constantes on ajoute une constante a. Dans la suite $\mathcal{F}$ contiendra toujours au moins une constante.

Définition 3.6 (Domaine et interprétation de Herbrand) *Le domaine de Herbrand est l'ensemble des termes clos sur* $\mathcal{F}$*. Dans l'interprétation de Herbrand, on interprète chaque symbole* f *par la fonction de construction* $f_H(t_1, \ldots, t_n) \stackrel{\text{def}}{=} f(t_1, \ldots, t_n)$*. La présence d'au moins une constante garantit que le domaine est non vide.*

Une interprétation de Herbrand *est de plus la donnée d'un ensemble* H *de formules atomiques closes, on aura* $R_H(t_1, \ldots, t_n)$ *est vrai par définition ssi* $R(t_1, \ldots, t_n) \in H$*.*

L'interprétation de Herbrand est un modèle "syntaxique' dans lequel on ne donne pas de sens particulier aux termes. Dans ce modèle, un environnement est un cas particulier de substitution (substitution close). La valeur d'un terme dans un environnement est donc une instance (close) de ce terme.

$$[\![t]\!]_{H,\rho} = t\rho$$

Proposition 3.3 *Une formule existentielle close* P *est valide si et seulement si elle est vraie dans toute interprétation de Herbrand sur l'univers de Herbrand associé à la signature.*

Preuve: *Soit une interprétation* I *quelconque, on considère l'interprétation de Herbrand* H *induite par les formules atomiques closes qui sont vraies dans* I*. La formule* P *est vraie dans cette interprétation, elle s'écrit* $\exists x_1, \ldots, \exists x_n, Q$ *et donc il existe une substitution close* $\sigma = [t_1/x_1; \ldots; t_n/x_n]$ *telle que* $Q\sigma$ *soit vraie dans* H *et donc aussi dans* I*. Si on prend maintenant* $a_i = [\![t_i]\!]_I$ *on a* $[\![Q\sigma]\!]_I = [\![Q]\!]_{I,(a_i/x_i)_i}$ *et donc* Q *est vrai dans l'environnement* a_i/x_i *et donc* P *est vrai dans l'interprétation* I*.*

Remarque *Cette propriété est fausse pour une propriété qui n'est pas existentielle comme* $P(a) \Rightarrow \forall x, P(x)$ *qui n'est pas valide mais qui est vrai dans toute interprétation de Herbrand sur le domaine* $\{a\}$. □

Proposition 3.4 *Une formule universelle close a un modèle si et seulement si elle a un modèle de Herbrand.*

Preuve: *Soit* I *un modèle de la formule* $\forall x_1, \dots x_n, P$. *On considère l'interprétation de Herbrand* H *sur la base* $\{R(t_1, \dots, t_n) | R_I([\![t_1]\!]_I, \dots, [\![t_n]\!]_I)\}$.

Les interprétations I *et* H *coincident sur toutes les formules propositionnelles closes. Soit* ρ *un environnement dans l'univers de Herbrand, on a pour toute formule propositionnelle*

$$[\![P]\!]_{H,\rho} = [\![P\rho]\!]_H = [\![P\rho]\!]_I = [\![P]\!]_{I,\rho'}$$

avec $\rho'(x) = [\![\rho(x)]\!]_I$. *On en déduit que si* I *rend vrai la formule* $\forall x_1, \dots x_n, P$ *alors* H *aussi.*

Pour une formule P *qui n'est pas en forme universelle, on peut calculer sa forme de Skolem* P'. *Si* P *a un modèle alors* P' *a un modèle et donc* P' *admet un modèle de Herbrand et comme* $P' \models P$, *ce modèle de Herbrand est aussi un modèle de* P *(mais attention en général la signature sera plus large que la signature de la formule initiale).*

□

Développement 2 (Théorème de Herbrand sémantique) *On suppose qu'il y a au moins une constante dans le langage.*

Soit P *une formule existentielle close* $\exists x_1, \dots, \exists x_n, Q$ *avec* Q *sans quantificateurs. La formule* P *est valide si et seulement si il existe un entier* k *et* k *substitutions closes* $\sigma_1, \dots, \sigma_k$ *telles que* $Q\sigma_1 \vee \dots \vee Q\sigma_k$ *est valide.*

De manière duale, soit P *une formule universelle close* $\forall x_1, \dots, \forall x_n, Q$ *avec* Q *sans quantificateurs. La formule* P *est insatisfiable si et seulement si il existe un entier* k *et* k *substitutions closes* $\sigma_1, \dots, \sigma_k$ *telles que* $Q[\sigma_1] \wedge \dots \wedge Q[\sigma_k]$ *est insatisfiable.*

Preuve: *On peut toujours ramener le cas général au cas d'une formule close en remplaçant les variables libres par de nouvelles constantes toutes différentes.*

- *Montrer que si* $\forall x_1, \dots, \forall x_n, Q$ *avec* Q *sans quantificateurs est insatisfiable alors l'ensemble des instances* $Q\sigma$ *pour toutes les substitutions closes est aussi insatisfiable.*
- *En déduire le résultat.*

□

Remarque : on pourrait vouloir une propriété plus forte de constructivité : si $\exists x, Q$ est valide alors il existe une substitution σ telle que $Q\sigma$ est valide, mais ce n'est pas le cas. Par exemple si on prend la formule $\exists x, (P(a) \vee P(b)) \Rightarrow P(x)$ elle est valide mais ni $(P(a) \vee P(b)) \Rightarrow P(a)$ ni $(P(a) \vee P(b)) \Rightarrow P(b)$ n'est valide.

Proposition 3.5 *L'ensemble des formules valides (sur une signature dénombrable) est récursivement énumérable.*

Preuve:*[Goubault-Larrecq and Mackie, 1997, thm 6.19 p 204] On énumère les formules, et pour chaque formule* P, *on la met en forme de Herbrand* $\exists x_1 \dots x_n, Q$ *sur la signature obtenue, on énumère les suites finies de substitutions* $(\sigma_1, \dots, \sigma_k)$ *par taille croissante. On teste la validité de la formule propositionnelle disjonctive associée. Si une des formules disjonctive est valide alors a fortiori la formule existentielle* $\exists x_1 \dots x_n, Q$ *l'ait, et réciproquement si la formule existentielle est valide alors il y a une formule disjonctive propositionnelle qui est valide et qui sera testée à un moment donné.* □

Développement 3 (Indécidabilité de la logique du premier ordre) *Il n'existe pas d'algorithme décidant la validité des formules du premier ordre.*

Preuve: *[Goubault-Larrecq and Mackie, 1997, thm 6.20 p 205] On se ramène à un problème de Post*

A un alphabet fini, on considère un ensemble de couples de mots (u_i, v_i) on cherche s'il existe k non nul tel que $u_{i_1} \dots u_{i_k} = v_{i_1} \dots v_{i_k}$.

On introduit un symbole unaire pour chaque lettre de l'alphabet et une constante ϵ pour le mot vide.

Si u est un mot et t est un terme on note $u(t)$ le terme construit en ajoutant les lettres de u en tête de t. On introduit un symbole de relation binaire P tel que $P(t_1, t_2)$ représente le fait que t_1 correspond à un mot $u_{i_1} \dots u_{i_k}$ et t_2 à un mot $v_{i_1} \dots v_{i_k}$ avec chaque couple (u_i, v_i) dans la correspondance de poste.

- *Donner un ensemble fini d'axiomes qui caractérise le relation P.*
- *Donner une formule dont la validité est équivalente à l'existence d'une solution au problème de Post.*

□

Développement 4 *Compacité*

Si $\Gamma \models P$ alors il existe Δ un sous ensemble fini de Γ tel que $\Delta \models P$.

Preuve:*[Goubault-Larrecq and Mackie, 1997, th 6.21 p208] On peut se ramener à un ensemble Γ de formule universelles insatisfiables. On considère toutes les instances closes de la partie sans quantificateur. Cet ensemble ne contient que des formules propositionnelles et est insatisfiable. Il y a donc un sous-ensemble fini de formules insatisfiables à partir duquel on récupère un sous ensemble de la formule originale qui est insatisfiable.* □

Développement 5 (Classe de formules de Bernays-Schönfinkel) *[Goubault-Larrecq and Mackie, 1997, exo 6.6 p210&395]*

On s'intéresse aux formules $\exists x_1, \ldots, x_n, \forall y_1, \ldots, y_m, Q$ avec Q sans quantificateur et une signature sans symbole de fonction.

Montrer que la satisfiabilité de telles formules est décidable.

Preuve: *La mise en forme de Skolem introduit n nouvelles constantes et comme il n'y a pas de symboles de fonction le domaine de Herbrand est fini de taille N. Il y a N^m environnements possibles pour les variables $y_1, \ldots, y_m$, il suffit de transformer la formule universelle en une conjonction sur toutes les interprétations et d'en tester la satisfiabilité.* □

3.4 Théories du premier ordre et cardinalité

Si on se donne un langage avec un prédicat d'égalité, il est facile d'écrire des formules qui contraignent le nombre d'éléments dans les modèles correspondant.

Exercice 3.3 *Donner pour chacune des propriétés suivantes des ensembles de formules closes de la logique du premier ordre qui garantissent que tout modèle de cette théorie aura la propriété demandée :*

- *Au moins n éléments.*
- *Au plus n éléments.*
- *Une infinité d'éléments.*

En déduire que l'on ne peut pas construire une théorie qui ait des modèles de cardinal fini arbitrairement grand mais pas de modèle infini.

On ne peut donc pas avoir de théorie du premier ordre qui caractérise les groupes finis (c'est-à-dire dont les modèles soient exactement les groupes finis).

Si on peut distinguer parmi les cardinaux finis, le théorème suivant montre que l'on ne peut pas distinguer parmi les différents cardinaux infinis.

On commence par une remarque. Le théorème de Herbrand nous dit qu'une formule existentielle est valide si et seulement elle est vrai dans tout modèle de Herbrand. Ce résultat est encore vrai si on ajoute un ensemble quelconque de constantes à la signature. En prenant les contraposées, on en déduit qu'une formule universelle est satisfiable si et seulement si elle admet un modèle de Herbrand sur une base de constantes fixée a priori.

Développement 6 *Théorème de Lowenheim-Skolem [Goubault-Larrecq and Mackie, 1997, th 6.22 p208]*

Si une formule a un modèle infini, alors elle a des modèles infinis de n'importe quelle cardinalité.

Si de plus la théorie comporte un symbole binaire d'égalité et qu'il existe un modèle équationnel (l'égalité syntaxique est interprétée comme l'égalité dans le domaine) infini, alors il existe des modèles équationnels infinis de n'importe quelle cardinalité.

Preuve:

Cas sans égalité *On skolémise la formule ce qui introduit possiblement un nombre fini de nouveaux symboles de fonction, la signature reste finie et la théorie obtenue a un modèle. Comme la formule est universelle, elle a un modèle de Herbrand.*

On peut enrichir la signature en ajoutant un nombre arbitraire de constantes dans le domaine de Herbrand. En effet la vérité d'une formule ne dépend que de l'interprétation des symboles qui apparaissent dans cette formule.

On se donne un cardinal infini α et un ensemble G de constantes de cardinal α. On considère le domaine de Herbrand sur la signature composée de la signature originale et de l'ensemble de constantes G. La première remarque est que comme les symboles de fonctions sont dans la signature initiale en nombre fini, et que α est infini donc au moins dénombrable, l'ensemble des termes ainsi obtenus a pour cardinal α. On considère un modèle de Herbrand sur cette signature, il a le cardinal attendu.

□

Une conséquence de ce théorème est qu'il y a des modèles des entiers qui sont non dénombrables et à l'inverse des modèles des réels qui sont dénombrables.

4 Systèmes de preuves

4.1 Théories

Une théorie T est un ensemble de formules closes (appelés axiomes de la théorie).
On suppose que l'on a un système de preuve qui nous permet de faire des déductions $\Gamma \vdash A$.

- $T \models A$ si tout modèle de T rend vraie A
- $T \vdash A$ s'il existe un sous-ensemble Γ de T tel que $\Gamma \vdash A$
- T est une théorie complète si $T \nvdash \bot$ et pour toute formule A close, on a $T \vdash A$ ou $T \vdash \neg A$

La plupart des théories *ne sont pas complètes*. Si on prend la théorie des groupes, la formule de commutativité $\forall xy, xy = yx$ ne peut pas être prouvée (il y a des groupes non commutatifs) et sa négation ne peut pas non plus être prouvée (il y a des groupes commutatifs).

4.2 Systèmes de Hilbert

Dans ce système, on manipule juste des formules vraies à travers des axiomes et des règles pour déduire de nouvelles formules vraies à partir de formules déjà démontrées.

Pour traiter chaque quantificateur il faut ajouter à la fois un axiome et une règle

$$A[t/x] \Rightarrow \exists x, A \qquad \frac{A \Rightarrow C}{(\exists x, A) \Rightarrow C} x \notin \mathsf{FV}(C)$$

$$(\forall x, A) \Rightarrow A[t/x] \qquad \frac{C \Rightarrow A}{C \Rightarrow \forall x, A} x \notin \mathsf{FV}(C)$$

Le jugement $\Gamma \vdash A$ est défini par les règles suivantes

$$\frac{}{\Gamma \vdash A} A \in \Gamma \qquad \frac{}{\Gamma \vdash A} A \in \textsc{Axiom} \qquad \frac{\Gamma \vdash A \Rightarrow C}{\Gamma \vdash (\exists x, A) \Rightarrow C} x \notin \mathsf{FV}(\Gamma, C) \qquad \frac{\Gamma \vdash C \Rightarrow A}{\Gamma \vdash C \Rightarrow \forall x, A} x \notin \mathsf{FV}(\Gamma, C)$$

Le théorème principal est le théorème de déduction. Il utilise plusieurs résultats préliminaires

- Affaiblissement : si $\Gamma \vdash A$ et $\Gamma \subseteq \Delta$ alors $\Delta \vdash A$. Trivial par récurrence sur la dérivation $\Gamma \vdash A$, avoir plus d'hypothèses permet de faire plus de preuves.
- Autre forme d'affaiblissement : si $\Gamma \vdash A$ alors $\Gamma \vdash B \Rightarrow A$. Il suffit de prendre l'axiome $A \Rightarrow B \Rightarrow A$ et d'appliquer la règle de Modus Ponens.
- Identité : il existe une dérivation de $\vdash A \Rightarrow A$.
  On utilise l'axiome $(A \Rightarrow B \Rightarrow A) \Rightarrow (A \Rightarrow B) \Rightarrow (A \Rightarrow A)$ en prenant pour B la formule $(C \Rightarrow A)$ de manière à ce que $A \Rightarrow C \Rightarrow A$ soit un axiome.
- Composition : Si $\Gamma \vdash A \Rightarrow B$ et $\Gamma \vdash B \Rightarrow C$ alors $\Gamma \vdash A \Rightarrow C$. En effet l'affaiblissement de $\Gamma \vdash B \Rightarrow C$ permet de déduire $\Gamma \vdash A \Rightarrow B \Rightarrow C$ et il suffit ensuite d'utiliser l'axiome $(A \Rightarrow B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow (A \Rightarrow C)$
- Contraction : si $\Gamma \vdash A \Rightarrow A \Rightarrow B$ alors $\Gamma \vdash A \Rightarrow B$. Il suffit d'utiliser l'axiome $(A \Rightarrow A \Rightarrow B) \Rightarrow (A \Rightarrow A) \Rightarrow (A \Rightarrow B)$
- Curryfication : $\Gamma \vdash A \Rightarrow B \Rightarrow C$ si et seulement si $\Gamma \vdash (A \wedge B) \Rightarrow C$.
  On a les axiomes $A \wedge B \Rightarrow A$ et $A \wedge B \Rightarrow B$. Si $\Gamma \vdash A \Rightarrow (B \Rightarrow C)$ alors par composition on obtient $\Gamma \vdash (A \wedge B) \Rightarrow B \Rightarrow C$, puis en utilisant $A \wedge B \Rightarrow B$, on en déduit $\Gamma \vdash (A \wedge B) \Rightarrow C$.
  Dans l'autre sens on suppose $\Gamma \vdash (A \wedge B) \Rightarrow C$, on a l'axiome $A \Rightarrow B \Rightarrow A \wedge B$ et on en déduit $\Gamma \vdash A \Rightarrow B \Rightarrow C$

Proposition 4.1 (Théorème de déduction) *On a $\Gamma, A \vdash B$ si et seulement si $\Gamma \vdash A \Rightarrow B$.*

Preuve: *$\Gamma \vdash A \Rightarrow B$ implique $\Gamma, A \vdash B$ par simple application de la règle de Modus-Ponens.*

Dans l'autre sens on fait une récurrence sur la structure de la preuve de $\Gamma, A \vdash B$. On regarde la dernière règle de déduction utilisée.

- *si c'est une règle axiome ou une règle hypothèse avec $B \in \Gamma$ alors le résultat est immédiat. Si $B = A$ alors c'est une conséquence de la dérivabilité de $A \Rightarrow A$.*

- *si c'est la règle de Modus Ponens* $\dfrac{\Gamma, A \vdash C \Rightarrow B \quad \Gamma, A \vdash C}{\Gamma, A \vdash B}$ *alors par hypothèse de récurrence on a des dérivations de* $\Gamma \vdash A \Rightarrow C \Rightarrow B$ *et de* $\Gamma \vdash A \Rightarrow C$*, on en déduit* $\Gamma \vdash A \Rightarrow B$ *en utilisant l'axiome* $(A \Rightarrow C \Rightarrow B) \Rightarrow (A \Rightarrow C) \Rightarrow A \Rightarrow B$ *et deux fois la règle de Modus Ponens.*
- *si c'est la* $\forall$ *avec* $x \notin \mathsf{FV}(\Gamma, A, C)$ $\dfrac{\Gamma, A \vdash C \Rightarrow B}{\Gamma, A \vdash C \Rightarrow \forall x, B}$*, alors par hypothèse de récurrence on a une dérivation de* $\Gamma \vdash A \Rightarrow C \Rightarrow B$ *on en déduit une dérivation de* $\Gamma \vdash (A \wedge C) \Rightarrow B$ *en utilisant la règle de* $\forall$*, on en déduit* $\Gamma \vdash (A \wedge C) \Rightarrow \forall x, B$ *puis* $\Gamma \vdash A \Rightarrow C \Rightarrow \forall x, B$

□

4.3 Déduction naturelle (NK)

Les règles additionnelles pour les quantificateurs sont

$$\frac{\Gamma \vdash P}{\Gamma \vdash \forall x, P} x \notin \mathsf{FV}(\Gamma) \qquad \frac{\Gamma \vdash \forall x, P}{\Gamma \vdash P[t/x]}$$

$$\frac{\Gamma \vdash P[t/x]}{\Gamma \vdash \exists x, P} \qquad \frac{\Gamma \vdash \exists x, P \quad \Gamma, P \vdash C}{\Gamma \vdash C} x \notin \mathsf{FV}(C, \Gamma)$$

Exercice 4.1

- *Dériver une preuve de* $\exists x, (A \wedge B) \vdash (\exists x, A) \wedge (\exists x, B)$
- *Montrer que la règle suivante est dérivable*

$$\frac{\Gamma, (\forall x, P), P[t/x] \vdash C}{\Gamma, (\forall x, P) \vdash C}$$

- *Dériver le principe du buveur*

$$\exists x, \forall y, P(x) \Rightarrow P(y)$$

Proposition 4.2 (Affaiblissement)

- *si* $\Gamma \vdash A$ *et* $\Gamma \subseteq \Delta$ *alors* $\Delta \vdash A$*.*
- *si* $\Gamma \vdash A$ *alors* $\Gamma[t/x] \vdash A[t/x]$

Preuve: *Par récurrence sur la structure de la dérivation* $\Gamma \vdash A$*.* □

Développement 7 (Correction et complétude de la déduction naturelle) *[David et al., 2004, thm 2.5.6 p 76]*

- *Correction : si* $\Gamma \vdash A$ *alors* $\Gamma \models A$
- *Complétude : si* $\Gamma \models A$ *alors* $\Gamma \vdash A$

Preuve: *La correction se fait par récurrence sur la structure de la dérivation* $\Gamma \vdash A$*. Pour la complétude, on peut se ramener à montrer que si* $\Gamma \models \bot$ *alors* $\Gamma \vdash \bot$*. On va montrer la contraposée : si* $\Gamma \not\models \bot$ *alors* Γ *a un modèle. Pour cela on va construire une théorie* T *complète sur un langage étendu qui étend l'ensemble de formules* Γ*, et telle que pour toute formule* $P(x)$ *à une variable libre, il existe une constante* c *telle que le théorème* $\exists x, P(x) \Rightarrow P(c)$ *soit montrable dans la théorie.*

Exercice 4.2 (Preuve de la complétude) *On se place dans le cas où la signature est dénombrable.*

1. *On suppose donné une théorie T avec les propriétés précédentes. On construit un modèle M sur les termes clos tels que $R_M(t_1, \ldots, t_n)$ est vrai si et seulement si $T \vdash R(t_1, \ldots, t_n)$. Montrer que pour toute formule F à n variables libres (on pourra se contenter des connecteurs $\exists, \vee, \neg$) on a $M \models F(t_1, \ldots, t_n)$ ssi $T \vdash F(t_1, \ldots, t_n)$.*
2. *Pour construire la théorie T, on procède de manière itérative en construisant un langage L_n et une théorie T_n. On prend $L_0 = L$ et $T_0 = \Gamma$. On construit L_{n+1} en ajoutant à L_n une nouvelle constante c_P pour chaque formule à une variable libre $P(x)$ de L_n et on construit T_{n+1} en ajoutant à T_n un axiome $\exists x, P(x) \Rightarrow P(c_P)$. On prend ensuite comme langage L' l'union des langages ainsi construits et comme théorie T', l'union des théories T_n.*

   (a) *Montrer que pour toute formule $P(x)$ de L' on a bien $T' \vdash \exists x, P(x) \Rightarrow P(c_P)$.*

   (b) *Montrer que $T' \nvdash \bot$.*
3. *On complète maintenant T' de la manière suivante, on énumère les formules closes (on est parti d'une signature au plus dénombrable). Tant que la théorie n'est pas complète, on l'étend en ajoutant la formule A_p avec p minimal.*

   Montrer que la théorie ainsi obtenue a les bonnes propriétés pour la construction d'un modèle.

□

4.4 Calcul des séquents (LK)

On ajoute aux règles du calcul propositionnel, les règles suivantes pour les quantificateurs :

$$\frac{\Gamma \vdash P[y/x], \Delta}{\Gamma \vdash (\forall x, P), \Delta} y \notin \mathsf{FV}(\Gamma, \Delta) \qquad \frac{\Gamma, (\forall x, P), P[t/x] \vdash \Delta}{\Gamma, (\forall x, P) \vdash \Delta}$$

$$\frac{\Gamma \vdash P[t/x], (\exists x, P), \Delta}{\Gamma \vdash (\exists x, P), \Delta} \qquad \frac{\Gamma, P[y/x] \vdash \Delta}{\Gamma, (\exists x, P) \vdash \Delta} y \notin \mathsf{FV}(\Delta, \Gamma)$$

On montre par une simple récurrence sur la structure de la preuve les propriétés de substitution et d'affaiblissement.

- Si $\Gamma \vdash \Delta$ et x est une variable libre, t un terme alors $\Gamma[t/x] \vdash \Delta[t/x]$
- Si $\Gamma \vdash \Delta$, $\Gamma \subseteq \Gamma'$ et $\Delta \subseteq \Delta'$ alors $\Gamma' \vdash \Delta'$

La preuve se fait par récurrence sur la structure de la dérivation. La dérivation transformée a la même structure. Il faut néamoins être attentif aux conditions sur les variables des règles $\exists g$ et $\forall d$. En effet une variable qui n'apparaissait pas libre dans Γ, Δ pourrait apparaître libre dans Γ', Δ' ou bien dans $\Gamma[t/x], \Delta[t/x]$ (si elle apparaît dans t). On prendra soin dans le choix des variables de renommage dans les règles $\exists g$ et $\forall d$ de choisir un nom qui n'est pas une variable libre de Γ', Δ' ou bien de celles de t.

Dans le cas du premier ordre, le choix de la structure des contextes (ensemble versus multi-ensemble) devient important, en effet certaines preuves nécessitent de pouvoir faire plusieurs instantiations sur des formules existentielles (à droite) ou universelles (à gauche). Ici on considère des ensembles de formules et la notation Γ, Γ' représente l'union des deux contextes. La duplication de la formule $\forall x, P$ dans la règle gauche du $\forall$ et de la formule $\exists x, P$ dans la règle droite $\exists$ est essentielle pour garder le caractère inversible des règles (et la complétude).

Exercice 4.3

- *Dériver une preuve de* $\exists x, (A \wedge B) \vdash (\exists x, A) \wedge (\exists x, B)$
- *Dériver le principe du buveur* $\exists x, \forall y, P(x) \Rightarrow P(y)$

Développement 8 (Correction et complétude du calcul des séquents) *Le calcul des séquents est correct et complet.*

Preuve: *La correction se fait par récurrence sur la structure de la dérivation.*

Pour la complétude, on peut reprendre le schéma de preuve de complétude de la déduction naturelle et l'adapter au calcul des séquents. Seule la partie 1 sur la correspondance entre vérité dans le modèle et prouvabilité dans la théorie complète a besoin d'être adaptée.

□

Développement 9 (Elimination des coupures) *Si* $\Gamma \vdash \Delta$ *en utilisant la règle de coupure alors* $\Gamma \vdash \Delta$ *sans la règle de coupure.*

Preuve: *On va se limiter au fragment avec* $\forall, \neg$ *et* $\wedge$.

On définit la profondeur d'une formule $d(P)$ *comme le nombre maximal de connecteurs/quantificateurs sur une branche.*

On définit la profondeur d'une preuve $d(\pi)$ *comme le nombre maximal de règles sur une branche.*

Une preuve π *est une coupure de hauteur maximale si elle se termine par une coupure sur la formule* P *avec deux prémisses qui sont des preuves sans coupures notées* π_1 *et* π_2.

Son rang est défini comme le couple $(d(P), d(\pi_1) + d(\pi_2))$ *ordonné de manière lexicographique.*

Si on prend une preuve avec coupure, on va choisir une coupure de hauteur maximale et dont le rang est maximal et on va montrer qu'on peut transformer la preuve pour faire diminuer le rang des coupures.

La coupure est de la forme $\dfrac{\Gamma \vdash \Delta, P \qquad \Gamma', P \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$.

- *si l'une des preuves est une règle hypothèse on a*

$$cut\ \frac{\Gamma_0, P \vdash \Delta, P \qquad \Gamma', P \vdash \Delta'}{\Gamma_0, P, \Gamma' \vdash \Delta, \Delta'}$$

  On peut juste faire un affaiblissement de la preuve de $\Gamma', P \vdash \Delta'$ (qui n'introduit pas de cut).
- *Si l'une des deux premisses est prouvée par une règle dont P n'est pas une formule principale, par exemple de la forme*

$$\frac{\Gamma_0 \vdash \Delta_0, P \quad \Gamma_1 \vdash \Delta_1, P}{\Gamma \vdash \Delta, P}$$

  On peut appliquer la coupure sur les deux prémisses.
  Les autres cas de même nature se traitent de manière identique.

$$cut\ \frac{\Gamma_0 \vdash \Delta_0, P \qquad \Gamma', P \vdash \Delta'}{\Gamma_0, \Gamma' \vdash \Delta_0, \Delta'}\ cut\ \frac{\Gamma_1 \vdash \Delta_1, P \qquad \Gamma', P \vdash \Delta'}{\Gamma_1, \Gamma' \vdash \Delta_1, \Delta'}}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

  On a fait diminuer de au moins 1 la somme des profondeurs des deux prémisses du cut.
- *On s'intéresse donc à des preuves pour lesquelles la formule P est la fomule principale des deux côtés.*

$$\begin{array}{c} \forall d\ \dfrac{\Gamma \vdash \Delta, P[y/x]}{\Gamma \vdash \Delta, (\forall x, P)} \quad \forall g\ \dfrac{\Gamma', (\forall x, P), P[t/x] \vdash \Delta'}{\Gamma', (\forall x, P) \vdash \Delta'} \\ cut\ \dfrac{\qquad\qquad\qquad\qquad\qquad\qquad}{\Gamma, \Gamma' \vdash \Delta, \Delta'} \end{array}$$

  On transforme en

$$cut\ \frac{\Gamma \vdash \Delta, P[t/x] \quad cut\ \dfrac{\Gamma \vdash \Delta, (\forall x, P) \qquad \Gamma', (\forall x, P), P[t/x] \vdash \Delta'}{\Gamma', P[t/x] \vdash \Delta'}}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

  La coupure sur $\forall x, P$ se fait sur des preuves de profondeur moindre. La coupure sur $P[t/x]$ se fait sur une formule de hauteur moindre. On a donc bien à chaque fois une décroissance par rapport à l'ordre lexicographique.

□

Exercice 4.4 (Applications de l'élimination des coupures)

- *Il n'y a pas de preuve du séquent vide $\vdash$ ni du séquent $\vdash A$ avec A une formule atomique.*
- *On étend la notion de sous-formule au cas du premier ordre de la manière suivante : l'ensemble des sous-formules de $\exists x, P$ et $\forall x, P$ contient l'ensemble de toutes les sous-formules des instances $P[t/x]$ pour n'importe quel terme t. Montrer que s'il y a une preuve de $\Gamma \vdash \Delta$ en calcul des séquents alors il y a une preuve qui ne fait intervenir que des sous-formules de Γ et Δ.*

Développement 10 (Théorème de Herbrand syntaxique) *Soit une formule existentielle $\exists x_1, \ldots, x_n, P$ avec P sans quantificateurs. Si $\vdash \exists x_1 \ldots x_n, P$ est prouvable alors il existe des substitutions $\sigma_1, \ldots, \sigma_k$ telles que $\vdash P\sigma_1, \ldots, P\sigma_k$ soit prouvable.*

Preuve: *On pourrait évidemment passer par le théorème de Herbrand sémantique et la complétude mais on peut aussi faire une preuve syntaxique complète.*

On généralise le résultat. Si on a une preuve de $\Gamma \vdash \Delta$ dans laquelle toutes les formules de Γ sont sans quantificateur et toutes les formules de Δ sont existentielles (éventuellement sans quantificateur) alors on peut trouver pour chaque formule existentielle dans Δ des substitutions $\sigma_1, \ldots, \sigma_k$ telles que $\Gamma \vdash \Delta'$ avec Δ' un contexte dans lequel chaque formule $\exists x_1, \ldots x_n, P$ a été remplacée par $P\sigma_1, \ldots, P\sigma_k$.

La récurrence se fait sur la preuve de $\Gamma \vdash \Delta$. On remarque que toutes les règles applicables garantissent qu'il n'y aura jamais de quantificateur à gauche et que toutes les formules à droite restent existentielles.

Les règles axiomes n'utilisent pas les formules existentielles, donc le théorème s'applique en prenant pour Δ' les formules sans quantificateur de Δ' et un ensemble vide de substitution. Si la règle utilisée est propositionnelle alors elle ne concerne pas les formules existentielles. On applique l'hypothèse de récurrence aux prémisses de la règle. Cela ne change pas la formule principale de la règle qui continue à s'appliquer et les substitutions concernées sont l'union des substitutions dans les deux branches.

La seule règle sur les quantificateurs qui s'applique est la règle existentielle droite. On se retrouve avec une prémisse $\Gamma \vdash (\exists x, Q), Q[t/x], \Delta$. On suppose que Q est de la forme $\exists x_1, \dots x_n, P$.

On obtient récursivement une preuve de $\Gamma \vdash P\sigma_1, \dots, P\sigma_n, P[t/x]\tau_1, \dots, P[t/x]\tau_m, \Delta'$ (si Q ne contient plus de quantificateur existentiel on prendra pour τ_j la substitution identité) et donc le théorème est vrai pour la conclusion de la règle avec pour la formule $\exists x, Q$ l'ensemble de substitutions

$$\{\sigma_1, \dots, \sigma_n, [t/x]\tau_1, \dots [t/x]\tau_m\}$$

.

□

Développement 11 (Traduction de LK dans NK) *[David et al., 2004, thm 5.3.6, p 190] On peut transformer une preuve de $\Gamma \vdash \Delta$ dans LK en une preuve de $\Gamma, \neg\Delta \vdash \bot$ en déduction naturelle.*

Exercice 4.5 *Faire les cas pour les connecteurs $\forall, \neg, \wedge$.*

4.5 Unification

Un *problème d'unification* a pour entrée un ensemble fini $\{(t_1 \stackrel{?}{=} u_1), \dots, (t_n \stackrel{?}{=} u_n)\}$ de couples de termes (sur une signature fixée). On recherche une substitution σ telle que $t_i\sigma = u_i\sigma$ pour $1 \leq i \leq n$.

On parle d'unification *syntaxique*, car l'égalité sur les termes est l'égalité syntaxique. On peut aussi considérer l'unification modulo des théories (associativité, commutativité de certains opérateurs).

Un *problème de filtrage* a pour entrée un ensemble fini $\{(t_1 \stackrel{?}{=} u_1), \dots, (t_n \stackrel{?}{=} u_n)\}$ de couples de termes (sur une signature fixée). On recherche une substitution σ telle que $t_i\sigma = u_i$ pour $1 \leq i \leq n$.

Exercice 4.6 *Résoudre les problèmes d'unification suivants sur la signature $\{f, a\}$*

- $f(x, x, y) \stackrel{?}{=} f(f(y, y, z), f(y, y, z), a)$
- $f(x, x, y) \stackrel{?}{=} f(f(y, y, z), f(y, x, z), a)$

Définition 4.1 (Renommage) *Une substitution qui est une bijection sur les variables est appelée un* renommage.

Développement 12 (Algorithme de Robinson) *[David et al., 2004, thm 7.2.10, p 239] Soit un problème d'unification, soit il n'a pas de solution (on dit que les termes ne sont pas unifiables), soit il admet une solution* la plus générale *σ_0 c'est-à-dire que $t_i\sigma_0 = u_i\sigma_0$ pour $1 \leq i \leq n$ et pour tout σ tel que $\forall 1 \leq i \leq n, t_i\sigma = u_i\sigma$ on a $\sigma = \sigma_0\sigma'$. On notera $mgu(t, u)$ l'unificateur principal des termes t et u quand il existe. mgu est une abbréviation de* most general unifier.

L'unificateur principal est unique à renommage près.

Preuve: *On définit une fonction mgu par les équations suivantes dans lesquelles $x \in \mathcal{X}$.*

$$mgu(\emptyset) = [] \qquad \textit{identité } \sigma(x) = x \qquad (1)$$

$$mgu(\{x \stackrel{?}{=} x\} \cup E) = mgu(E) \qquad \textit{équation triviale} \qquad (2)$$

$$mgu(\{x \stackrel{?}{=} t\} \cup E) = \textbf{\textit{echec}} \qquad \textit{si } x \in FV(t) \qquad (3)$$

$$mgu(\{x \stackrel{?}{=} t\} \cup E) = [t/x]mgu(E[t/x]) \qquad \textit{si } x \notin FV(t) \qquad (4)$$

$$mgu(\{t \stackrel{?}{=} x\} \cup E) = mgu(\{x \stackrel{?}{=} t\} \cup E) \qquad \textit{si } t \notin \mathcal{X} \qquad (5)$$

$$mgu(\{f(t_1, \dots, t_n) \stackrel{?}{=} g(u_1, \dots, u_p)\} \cup E) = \textbf{\textit{echec}} \qquad \textit{si } f \neq g \qquad (6)$$

$$mgu(\{f(t_1, \dots, t_n) \stackrel{?}{=} f(u_1, \dots, u_n)\} \cup E) = mgu(\{t_1 \stackrel{?}{=} u_1; \dots; t_n \stackrel{?}{=} u_n\} \cup E) \qquad (7)$$

Exercice 4.7 • *Justifier la terminaison de cette fonction vue comme un algorithme.*

- *Montrer que les cas d'échec correspondent à une absence de solution.*
- *Montrer que la propriété de mgu est préservée dans les équations (4) et (7).*
- *[David et al., 2004, exercice 7.6, p 259] On considère une suite de variables $(x_n)_{n\in\mathbb{N}}$ et une signature avec un symbole de fonction binaire f. Soit les deux suites de termes*

$$u_0 = x_0 \quad u_{n+1} = f(u_n, x_n) \quad v_0 = x_0 \quad v_{n+1} = f(x_n, v_n)$$

  — *appliquer l'algorithme d'unification au problème $u_n \stackrel{?}{=} v_n$, quelle est la taille du terme solution ?*
  — *compter le nombre d'étapes nécéssaires à l'unification des termes $f(u_n, u_n) \stackrel{?}{=} f(v_n, v_n)$*

□

L'algorithme proposé est dans le cas le pire exponentiel en la taille des termes à unifier (même en considérant l'occur-check et la substitution comme des opérations élémentaires). On verra plus tard d'autres algorithmes plus efficaces (mais moins intuitifs).

4.6 Méthode des tableaux

C'est une méthode de démonstration automatique qui s'appuie sur le calcul des séquents et l'unification pour rechercher des preuves.

L'idée est de borner l'utilisation des règles $\exists$ droite et $\forall$ gauche de manière arbitraire pour chaque quantificateur présent dans le séquent à prouver et de choisir comme terme t pour l'instantiation une nouvelle variable dont la valeur sera déterminée plus tard dans les règles axiomes.

$$\frac{\Gamma, (\forall^n x, P), P[Y/x] \vdash \forall x, P}{\Gamma, (\forall^{n+1} x, P) \vdash \Delta} \qquad \frac{\Gamma \vdash P[Y/x], (\exists^n x, P), \Delta}{\Gamma \vdash (\exists^{n+1} x, P), \Delta}$$

On peut ainsi décomposer tous les connecteurs jusqu'à arriver à des séquents ne contenant que des formules atomiques et des formules quantifiées $\forall^0 x, P$ et $\exists^0 x, P$ dont on a "épuisé" le nombre de décompositions possibles.

L'idée en arrivant aux feuilles est de chercher une substitution qui choisit des valeurs pour les variables introduites précédemment telles que les séquents indécomposables deviennent des règles axiomes.

Cette méthode ne fonctionne pas vraiment car il nous faut aussi garantir que les conditions sur les variables des règles $\exists$ gauche et $\forall$ droite sont satisfaites.

$$\frac{\Gamma \vdash P[y/x], \Delta}{\Gamma \vdash (\forall x, P), \Delta} y \notin \mathsf{FV}(\Gamma, \Delta) \qquad \frac{\Gamma, P[y/x] \vdash \Delta}{\Gamma, (\exists x, P) \vdash \Delta} y \notin \mathsf{FV}(\Delta, \Gamma)$$

En effet sinon on pourrait montrer $\forall x, \exists y, P(x, y) \vdash \exists y, \forall x, P(x, y)$

Pour résoudre ce problème, soit on part de formules en forme de Herbrand (formule existentielle pour laquelle on n'aura jamais à appliquer les règles problématiques) soit on modifie les deux règles précédentes en faisant une mise en forme de Herbrand à la volée en choisissant pour chaque application de règle f un nouveau symbole de fonction dont l'arité est n avec $\mathsf{FV}(P)\backslash\{x\} = \{x_1, \ldots, x_n\}$.

$$\frac{\Gamma \vdash P[f(x_1, \ldots, x_n)/x], \Delta}{\Gamma \vdash (\forall x, P), \Delta} \qquad \frac{\Gamma, P[f(x_1, \ldots, x_n)/x] \vdash \Delta}{\Gamma, (\exists x, P) \vdash \Delta}$$

On peut appeler ces deux règles $\forall_d^h$ et $\exists_g^h$. Si on admet ces deux règles alors on peut en déduire les règles usuelles, en effet si $\Gamma \vdash P, \Delta$ avec $x \notin \mathsf{FV}(\Gamma, \Delta)$ alors par substitution on a $\Gamma \vdash P[f(x_1, \ldots, x_n)/x]$ et la règle $\forall_d^h$ nous permet de déduire la conclusion de $\forall_d$. Le théorème de Herbrand nous dit par ailleurs que si le séquent en prémisse de chacune de ces règles est valide alors il en est de même de la conclusion (l'existentielle à gauche du séquent se comporte vis-à-vis de la validité comme un quantificateur universel).

Exercice 4.8 *Utiliser la méthode des tableaux en mettant tout d'abord la formule $(\forall x, \exists y, P(x, y)) \Rightarrow \exists y, \forall x, P(x, y)$ sous forme de Herbrand puis en utilisant la méthode avec les règles modifiées pour les quantificateurs.*

4.7 Résolution

On part d'un ensemble de clauses (disjonction de littéraux). On note $\texttt{mgu}(L_1, L_2)$ l'unificateur principal (s'il existe) des littéraux L_1 et L_2.

Chaque clause C représente une formule close du calcul des prédicats obtenur en quantifiant universellement les variables de la clause, on la note $\forall C$. Une clause peut être interprétée comme un ensemble de clauses propositionnelles dans le domaine de Herbrand, c'est l'ensemble des clauses $C\sigma$ avec σ une substitution close.

Les règles de résolution sont

1. Résolution binaire ($\mathsf{FV}(L_1 \vee C) \cap \mathsf{FV}(\neg L_2 \vee C') = \emptyset$, $\sigma = \texttt{mgu}(L_1, L_2)$)
$$\frac{L_1 \vee C_1 \quad \neg L_2 \vee C_2}{C_1[\sigma] \vee C_2[\sigma]}$$
2. Factorisation ($\sigma = \texttt{mgu}(L_1, L_2)$)
$$\frac{L_1 \vee L_2 \vee C}{L_1[\sigma] \vee C[\sigma]}$$
3. Renommage (σ *bijection* sur les variables)
$$\frac{C}{C[\sigma]}$$

Exercice 4.9 $A \stackrel{\text{def}}{=} \exists x, \forall y, (S(y) \Rightarrow R(x)) \Rightarrow (S(x) \Rightarrow R(y))$

- *mettre la formule $\neg A$ en forme clausale*
- *appliquer les règles de résolution pour obtenir la clause vide*

Exercice 4.10 $C_1 \stackrel{\text{def}}{=} P(x, y) \vee P(y, x), C_2 \stackrel{\text{def}}{=} \neg P(z, u) \vee \neg P(u, z)$

- *appliquer les règles de résolution à partir des deux clauses C_1 et C_2 pour obtenir la clause vide*

Soit $\mathcal{E}$ un ensemble de clauses :

- une *déduction par résolution* à partir de $\mathcal{E}$ est une suite de clauses $C_1, \ldots, C_n$ telle que pour toute clause C_i dans cette suite
  — soit $C_i \in \mathcal{E}$;
  — soit il existe une clause C_j telle que $j < i$ et telle que C_i est le résultat de la règle de factorisation ou de renommage appliquée à C_j ;
  — soit il existe deux clauses C_j et C_k telles que $j, k < i$ et telle que C_i est le résultat de la règle de résolution appliquée à C_j et C_k.
- une *réfutation* de $\mathcal{E}$ est une *déduction par résolution* à partir de $\mathcal{E}$ qui contient la clause vide $\bot$
- une *preuve par résolution* (*réfutation*) d'une formule A à partir des clauses $\mathcal{E}$ est une réfutation de l'ensemble $\mathcal{E} \cup C_{\neg A}$ avec $C_{\neg A}$ forme clausale de $\neg A$.

Proposition 4.3 (Correction de la résolution) *La méthode de résolution est correcte : si on peut dériver une clause C à partir d'un ensemble de clauses $\mathcal{E}$ alors la formule $\forall(C)$ est conséquence logique de l'ensemble des formules $\{\forall(D) | D \in \mathcal{E}\}$*

Développement 13 (Lemme de relèvement) *[Gallier, 1987, p. 400] Soit deux clauses C_1, C_2 du premier ordre et D_1, D_2 deux instances closes de C_1, C_2, si on peut déduire par une étape de résolution propositionnelle la clause D_3 alors on peut obtenir par résolution du premier ordre une clause C_3 dont D_3 est une instance.*

Développement 14 (Complétude de la résolution) *La méthode de résolution est correcte et complète.*

Preuve: *C'est une conséquence du lemme de relèvement et de la complétude propositionnelle de la résolution.* □