* Motivations : théorie de la démonstration / preuves de théorèmes fastidieuses / Prolog

I] La logique du premier ordre

1) Syntaxe.

déf 1 : Un langage (du premier ordre) est la donnée d'une famille de symboles :
- les symboles de constantes $\mathcal{C}$.
- les symboles de fonctions admettant une arité $n \in \mathbb{N}^*$.
- les symboles de prédicats admettant une arité $n \in \mathbb{N}$.

ex 2 : le langage $\mathcal{L}_0$ de l'analyse réelle contient les symboles :
constantes : $0, 1, \dots, e, \pi$ / fonctions : $+, \times, |\cdot|, \sin, \dots$ / relations : $=, \leq, \dots$

déf 3 : l'ensemble des termes T sur un langage $\mathcal{L}$ est le plus petit sous-ensemble de $\mathcal{L} \cup \{(,)\}$ contenant :
- les constantes $\mathcal{C}$
- un ensemble fixé V de variables.
- stable par l'application des symboles de fonctions aux termes.

Autrement dit, $T = \bigcup_{k \in \mathbb{N}} T_k$ où $T_0 = \mathcal{C} \cup V$

$$T_{k+1} = T_k \cup \{ f(t_1, \dots, t_n), t_i \in T_k, f \text{ fonction d'arité } n \in \mathbb{N}^* \}$$

un terme est clos s'il ne contient pas de variable.

la hauteur d'un terme t est le plus petit $k \in \mathbb{N}$ tel que $t \in T_k$.

la taille d'un terme t est définie par $\begin{cases} 1 & \text{si } t \in T_0 \\ 1 + \sum_{1 \leq i \leq n} \text{taille}(t_i) & \text{si } t = f(t_1, \dots, t_n) \end{cases}$

ex 4 : sur $\mathcal{L}_0$, $\sin(x) \times |e - \cos(y)|$ est un terme non-clos de hauteur 5, de taille 4.

déf 5 : l'ensemble atom des formules atomiques sur un langage $\mathcal{L}$ est $\text{atom} = \{ P(t_1, \dots, t_n), P \text{ prédicat d'arité } n, t_i \in T \}$

L'ensemble $\mathcal{F}$ des formules sur $\mathcal{L}$ est défini par la grammaire :

$$\mathcal{F} = \text{atom} \mid \mathcal{F} \vee \mathcal{F} \mid \mathcal{F} \wedge \mathcal{F} \mid \mathcal{F} \to \mathcal{F} \mid \neg \mathcal{F} \mid \exists x \mathcal{F} \mid \forall x \mathcal{F} \mid \bot$$

ex 6 : sur $\mathcal{L}_0$, $\forall x \sin x \leq x$ et $\pi \times \pi = 10$ sont des formules.
$\sin(x) \times |e - \cos(y)|$ n'est pas une formule.

déf 7 : l'ensemble $FV(F)$ des variables libres d'une formule F est défini par

$$FV(F) = \begin{cases} \text{l'ensemble des variables des } t_i & \text{si } F = P(t_1, \dots, t_n) \\ FV(F_1) \cup FV(F_2) & \text{si } F = F_1 \oplus F_2, \oplus \in \{\vee, \wedge, \to\} \\ FV(F_1) & \text{si } F = \neg F_1 \\ FV(F_1) \setminus \{x\} & \text{si } F = \forall x F_1 \text{ ou } \exists x F_1 \end{cases}$$

une formule F est close si $FV(F) = \emptyset$.

déf 8 : une théorie est un ensemble de formules closes.

déf 9 : une substitution est une fonction totale $\sigma : V \to T$
on notera $u[\sigma]$ le terme dans lequel toute variable x de u a été remplacée par $\sigma(x)$. On étend ainsi σ en $\tilde{\sigma} : T \to T$.

déf 10 : deux formules F et G sont α-équivalentes ($F \sim_\alpha G$) s'il existe une substitution σ tq : $\sigma(V) \subseteq V$, $FV(F) \cup FV(G) \subseteq \text{Fix}(\sigma)$ et $F[\sigma] = G[\sigma]$.

ex 11 : $\forall y\, (x.y = y.x)$ et $\forall z\, (x.z = z.x)$ sont α-équivalentes.

ex 12 : si $x \in V$ et $u \in T$, $x := u$ est la substitution $\begin{cases} x \mapsto u \\ y \mapsto y \text{ si } y \neq x \end{cases}$

2) Sémantique.

déf 13 : un modèle $\mathcal{M}$ sur un langage $\mathcal{L}$ est la donnée de :
- un domaine $|\mathcal{M}|$, ensemble non-vide.
- Pour chaque symbole de constante $c \in \mathcal{C}$, un élément $c_{\mathcal{M}} \in |\mathcal{M}|$
- Pour chaque symbole de fonction f d'arité n, une fonction totale $f_{\mathcal{M}} : |\mathcal{M}|^n \to |\mathcal{M}|$
- Pour chaque symbole de prédicat P d'arité n, un sous-ensemble $P_{\mathcal{M}} \subseteq |\mathcal{M}|^n$

ex 14 : Un modèle de Herbrand sur un langage $\mathcal{L}$ est un modèle tel que :
- $|\mathcal{M}|$ est l'ensemble des formules closes sur $\mathcal{L}$.
- Pour $c \in \mathcal{C}$, $c_{\mathcal{M}} := c$.
- Pour f une fonction, $f_{\mathcal{M}} := f$.

déf 15 : Un modèle $\mathcal{M}$ satisfait une formule close F, et on note $\mathcal{M} \models F$, si F est vraie dans le modèle $\mathcal{M}$. Un modèle $\mathcal{M}$ satisfait une théorie T ($\mathcal{M} \models T$) si elle satisfait toutes les formules de T.

déf 16 : Deux formules closes F_1, F_2 sont sémantiquement équivalentes si pour tout modèle $\mathcal{M}$, $\mathcal{M} \models (F_1 \to F_2) \wedge (F_2 \to F_1)$.

déf 17 : Une théorie T est contradictoire si pour tout modèle $\mathcal{M}$, $\mathcal{M} \not\models T$.

Problème 18 : VALIDE.
Entrée : une formule F close
Sortie : oui si F est valide (ie : satisfaite par tout modèle)

Problème 19 : T-VALIDE (où T est une théorie)
Entrée : une formule F close
Sortie : oui si pour tout modèle $\mathcal{M}$, $(\mathcal{M} \models T) \Rightarrow (\mathcal{M} \models F)$

II] Systèmes de preuve.

1) La déduction naturelle (DN)

déf 20 : un séquent est un couple, noté $\Gamma \vdash A$, où Γ est un ensemble fini de formules et A une formule.

déf 21 : les règles de la DN sont composées d'une prémisse (ensemble de séquents) et d'une conclusion (un séquent). Les axiomes sont les règles pour lesquelles la prémisse est vide. [cf Annexe 1]

déf 22 : un séquent est prouvable par DN s'il existe un arbre de règles enraciné en ce séquent dont les feuilles sont obtenues avec les axiomes.

déf 23 : une formule F est prouvable par DN si le séquent $\varnothing \vdash F$ est prouvable.

ex 24 : la formule de De Morgan $\neg(A \wedge B) \to (\neg A \vee \neg B)$ est prouvable par DN. [cf Annexe 2] pour un arbre de preuve.

Rq 25 : il est parfois plus simple de noter les preuves "linéairement" :

ex 26 : dérivation de la règle de coupure : $\dfrac{\Gamma, A \vdash B \quad \Gamma \vdash A}{\Gamma \vdash B}$ coupure

$\to_i$ $\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}$ $\quad \dfrac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B} \to_e$

$\Gamma \vdash B$ $\quad \to_e(1)(2)$
(1) $\Gamma \vdash A \to B$ $\quad \to_i$
$\Gamma, A \vdash B$ $\quad$ (prémisse gauche)
(2) $\Gamma \vdash A$ $\quad$ (prémisse droite)

ex 27 : le séquent $\neg(\exists x\, \neg F) \vdash \forall x\, F$ est prouvable pour toute formule F.

déf 28 : Pour toute théorie T et toute formule F, on note $T \vdash F$ s'il existe un sous-ensemble fini $T' \subseteq T$ tel que le séquent $T' \vdash F$ est prouvable.

T est inconsistante si $T \vdash \bot$, consistante sinon.

T est complète si T est consistante et pour toute formule close F, $T \vdash F$ ou $T \vdash \neg F$.

Théorème 29 : toute théorie consistante est non-contradictoire. DEV 1

Corollaire 30 : (Théorème de complétude)
Soient T une théorie et F une formule close. Alors :
$$T \models F \iff T \vdash_{DN} F$$

Application 31 : les problèmes VALIDE et T-VALIDE pour T dénombrable sont dans la classe RE.

Application 32 : (Théorème de compacité) une théorie T est contradictoire si et seulement si il existe un sous-ensemble fini $T' \subseteq T$ contradictoire.
→ En particulier, il n'existe pas de théorie satisfaite par uniquement les modèles finis.

Application 33 : (Théorème de Lowenheim-Skolem) Si $\mathcal{L}$ est dénombrable et T est satisfaite par un modèle infini, alors T est satisfaite par un modèle dénombrable.

ex 34 : il existe un corps clos dénombrable.

2) Le calcul des séquents.

déf 35 : on étend la définition 20 où la prémisse et la conclusion sont des multi-ensembles de formules. On considère la prémisse comme une disjonction et la conclusion comme une conjonction.

déf 36 : un séquent est prouvable dans le calcul des séquents s'il existe un arbre de preuve enraciné en ce séquent, utilisant les règles du calcul des séquents [cf Annexe 3] et dont les feuilles sont des prémisses vides.

ex 37 : (élimination de la double-négation)

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,ax}{\vdash \neg A, A}\,\neg_d}{\neg\neg A \vdash A}\,\neg_g}{\vdash \neg\neg A \to A}\,\to_d$$

$\vdash \neg\neg A \to A$ $\quad \to_d$
$\neg\neg A \vdash A$ $\quad \neg_g$
$\vdash \neg A, A$ $\quad \neg_d$
$A \vdash A$ $\quad$ (axiome)

théorème 38 (Admis) : un séquent $\Gamma \vdash A$ est prouvable en calcul des séquents ssi il est prouvable pour déduction naturelle.

propriété 39 : (Admise) (élimination des coupures)
Si le séquent $\Gamma \vdash A$ est prouvable, alors il existe un arbre de preuve qui n'utilise pas la règle de coupure.

Remarque 40 : Dans l'automatisation des preuves, il suffira donc d'en rechercher une sans coupure.

III] Automatisation des preuves

1) Unification

déf 41 : deux termes u, v sont unifiables s'il existe une substitution σ vérifiant $u[\sigma] = v[\sigma]$. σ est un unificateur de u et v.

ex 42 : $u = f(x,x,y)$ et $v = f(f(y,y,z), f(y,y,z), a)$ sont unifiables.
$\sigma_0 : x \mapsto f(a,a,z)$, $y \mapsto a$ est un unificateur.

ex 43 : $u' = f(x,x,y)$ et $v' = g(f(x,x,y))$ ne sont pas unifiables.

thm-déf 44 : Soient u, v deux termes unifiables. Il existe un unificateur σ de u et v, appelé unificateur principal $UP(u,v)$ tq pour tout σ' unificateur de u et v, il existe une substitution σ'' tq $\sigma' = \sigma'' \circ \sigma$.

déf 46 : un ensemble d'équations $E = \{u_1 \sim v_1, \dots, u_n \sim v_n\}$ est dit unifiable s'il existe une substitution σ tq $u_i[\sigma] = v_i[\sigma]$ pour tout i.

ex 45 : dans l'exemple 42, l'unificateur σ_0 est principal.

lemme 46 : Soient x, u, σ une variable, un terme et une substitution tels que $x[\sigma] = u[\sigma]$. Alors $\sigma = \sigma \circ [x := u]$

lemme 47 : pour toute substitution σ et toute variable x apparaissant dans un terme $u \neq x$, $\text{taille}(x[\sigma]) < \text{taille}(u[\sigma])$

Théorème 48 :
l'algorithme 50 termine, et renvoie un unificateur principal s'il existe

DEV 2

Remarque 49 : La complexité en la taille des termes à unifier est au moins exponentielle, comme en atteste l'exemple suivant :
$\begin{cases} u_0 = x_0 \\ v_0 = x_0 \end{cases}$ et pour $n \geq 0$, $\begin{cases} u_{n+1} = f(u_n, x_n) \\ v_{n+1} = f(x_n, v_n) \end{cases}$ où $\{x_n, v \in \mathbb{N}\} \subseteq V$

Algo 50 : Unification. Entrée : un ensemble E d'équations.
Sortie : oui si E est unifiable (et un unificateur principal), non sinon.

Tant que $E \neq \emptyset$:
- ① Si $E = E' \sqcup \{f(u_1, \dots, u_p) \sim g(v_1, \dots, v_q)\}$:
  - Si $f = g$: poser $E = E' \cup \{u_1 \sim v_1, \dots, u_p \sim v_q\}$
  - Sinon : échec de type ① ("clash")
- ② Sinon si $E = E' \sqcup \{x \sim x\}$: poser $E = E'$
- ③ Sinon si $E = E' \sqcup \{x \sim u\}$ ou $E = E' \cup \{u \sim x\}$:
  - Si x n'apparaît pas dans u :
    - $E = E'[x := u]$
    - $\sigma = [x := u] \circ \sigma$
  - Sinon échec de type ③ ("occur-check")

Renvoyer oui, E, σ

2) La méthode de résolution

principe 51 : on cherche à montrer qu'un ensemble de clauses est contradictoire. On utilise les deux règles suivantes, où C_1, C_2 sont des clauses; l_1, l_2 des littéraux :

$$\frac{C_1, l_1 \quad C_2, l_2 \quad \sigma = UP(l_1, \neg l_2)}{C_1[\sigma], C_2[\sigma]}\ \text{rés} \qquad \frac{C_1, l_1, l_2 \quad \sigma = UP(l_1, l_2)}{C_1[\sigma], l_1[\sigma]}\ \text{contr}$$

lemme 52 : Une formule close prénexe $F = Q_1 x_1 \dots Q_n x_n\, G$ ($Q_i \in \{\forall, \exists\}$) est démontrable ssi la forme de Skolem de $\neg F$ est contradictoire.

méthode 53 : pour démontrer une formule close F :
① On met $\neg F$ sous forme de Skolem : $\forall x_1 \dots \forall x_k\, G(x_1 \dots x_k)$
② on met $G(x_1 \dots x_k)$ sous forme normale conjonctive : $\bigwedge_{i \in I} \bigvee_{j \in J_i} A_{i,j}$
③ on applique les règles ci-dessous aux clauses $C_i = \{A_{i,j}, j \in J_i\}$

exemple 54 : $F = \exists x \forall y [R(x) \to R(y)] \dashrightarrow \{R(z), \neg R(f(a))\}$ est contradictoire, donc F est prouvable.

3) La méthode des tableaux.

principe 55 : Dans le calcul des séquents (sans coupure), on remplace les règles ax, Aff, Contr, $\forall$ et $\exists$ par les cinq règles de l'[Annexe 4].

méthode 56 : Pour démontrer un séquent, on procède comme suit :
① on écrase chaque quantificateur avec un entier.
② on applique les règles jusqu'à obtenir un ensemble S de séquents dont chacune des formules est atomique.
③ On utilise un algorithme d'unification pour trouver une substitution σ telle que pour tout séquent $\Gamma \vdash \Delta$ de S, $\Gamma[\sigma] \vdash \Delta[\sigma]$ soit une conclusion de ax.

exemple 57 : En choisissant une multiplicité 1 pour tous les quantificateurs, on trouve pour $\exists x \{R(x) \to \forall y R(y)\}$ à l'étape 2 : $\dfrac{R(z) \vdash R(a)}{\vdash \exists^1 x \{R(x) \to \forall^1 y\, R(y)\}}\ \exists^1_{x,z}, \forall^1_y$
La substitution $[z := a]$ convient.

Annexe 1 : règles de la DN

règle	introduction	élimination
implication	$\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ \to_i$	$\dfrac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B}\ \to_e$
conjonction	$\dfrac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge_i$	$\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \wedge_e$
disjonction	$\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee_i$	$\dfrac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\ \vee_e$
négation	$\dfrac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg_i$	$\dfrac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash \bot}\ \neg_e$
$\forall$	$\dfrac{\Gamma \vdash A \text{ où } x \notin FV(\Gamma)}{\Gamma \vdash \forall x A}\ \forall_i$	$\dfrac{\Gamma \vdash \forall x A}{\Gamma \vdash A[x := t]}\ \forall_e$
$\exists$	$\dfrac{\Gamma \vdash A[x := t]}{\Gamma \vdash \exists x A}\ \exists_i$	$\dfrac{\Gamma \vdash \exists x A \quad \Gamma, A \vdash C}{\Gamma \vdash C}\ \exists_e$ où $x \notin FV(\Gamma) \cup FV(C)$
Axiome	$\dfrac{}{\Gamma, A \vdash A}\ ax$	
Affaiblissement	$\dfrac{\Gamma \vdash A}{\Gamma, B \vdash A}\ Aff$	
Absurde	$\dfrac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ Abs$	

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, A, B \vdash A}\,ax \quad \dfrac{}{\Gamma, A, B \vdash B}\,ax}{\Gamma, A, B \vdash A \wedge B}\,\wedge_i \quad \dfrac{}{\Gamma, A, B \vdash \neg(A \wedge B)}\,ax}{\Gamma, A, B \vdash \bot}\,\neg_e}{\Gamma, A \vdash \neg B}\,\neg_i \quad \dfrac{}{\Gamma, A \vdash \neg(\neg A \vee \neg B)}\,ax}{\Gamma, A \vdash \bot}\,\neg_e \quad \dfrac{\dfrac{}{\Gamma, A \vdash \neg A \vee \neg B}\,\vee_i}{\Gamma, A \vdash \bot}\,\neg_e$$

$$\dfrac{\dfrac{}{\Gamma \vdash \neg(\neg A \vee \neg B)}\,ax \quad \dfrac{\dfrac{\dfrac{}{\Gamma = \neg A \wedge B, \neg(\neg A \vee B) \vdash \bot}\,\neg_e}{\neg(A \wedge B) \vdash \neg A \vee \neg B}\,\bot_c}{\emptyset \vdash \neg(A \wedge B) \to (\neg A \vee \neg B)}\,\to_i}{\Gamma \vdash \neg A \vee \neg B}\,\vee_i}{\Gamma \vdash \bot}\,\neg_e$$

Annexe 2 : loi de Deforgan (sens 1)

Annexe 3 : règles du calcul des séquents

Axiomes	$\dfrac{}{\bot \vdash}\ \bot_g$	$\dfrac{}{A \vdash A}\ ax$
Affaiblissement	$\dfrac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\ aff_g$	$\dfrac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}\ aff_d$
Contraction	$\dfrac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\ contr_g$	$\dfrac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}\ contr_d$
implication	$\dfrac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta}\ \to_g$	$\dfrac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}\ \to_d$
conjonction	$\dfrac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ \wedge_g$	$\dfrac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\ \wedge_d$
disjonction	$\dfrac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta}\ \vee_g$	$\dfrac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\ \vee_d$
négation	$\dfrac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}\ \neg_g$	$\dfrac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\ \neg_d$
$\forall$	$\dfrac{\Gamma, A[x := t] \vdash \Delta}{\Gamma, \forall x A \vdash \Delta}\ \forall_g$ ★	$\dfrac{\Gamma \vdash A, \Delta \quad x \notin FV(\Gamma) \cup FV(\Delta)}{\Gamma \vdash \forall x A, \Delta}\ \forall_d$
$\exists$	$\dfrac{\Gamma, A \vdash \Delta \quad x \notin FV(\Gamma) \cup FV(\Delta)}{\Gamma, \exists x A \vdash \Delta}\ \exists_g$	$\dfrac{\Gamma \vdash A[x := t], \Delta}{\Gamma \vdash \exists x A, \Delta}\ \exists_d$ ★
coupure	$\dfrac{\Gamma \vdash A, \Delta \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\ coupure$	

Annexe 4 : règles alternatives pour la méthode des tableaux.

axiome$_0$	$\dfrac{}{\Gamma, A \vdash A, \Delta}\ ax_0$	
$\forall$	$\dfrac{\Gamma, A[x := y], \forall^n \vec{x} A \vdash \Delta}{\Gamma, \forall^n x A \vdash \Delta}\ \forall_g^n(*)$	$\dfrac{\Gamma \vdash A[x := f(x_1, \dots, x_k)], \Delta, \forall^n x A}{\Gamma \vdash \forall^n x A, \Delta}\ \forall_d^n(**)$
$\exists$	$\dfrac{\Gamma, A[x := f(x_1 \dots x_k)] \vdash \Delta}{\Gamma, \exists^n x A \vdash \Delta}\ \exists_g^n(**)$	$\dfrac{\Gamma \vdash A[x := y], \exists^n \vec{x} A, \Delta}{\Gamma \vdash \exists^n x A, \Delta}\ \exists_d^n(*)$

(*) : y est fraîche. Si $n = 1$, on efface la formule $\forall^0 x A$ ou $\exists^0 x A$.

(**) : $x_1 \dots x_n \neq x$ sont libres dans A et f est fraîche.