918 : Systèmes formels de preuve en logique du 1er ordre, exemples.

But : • définir formellement une preuve "concrète".
• automatiser le processus de démonstration

I) Définitions en logique du 1er ordre

1) La logique du 1er ordre

Déf 1 : Un langage du premier ordre est la donnée d'une famille de symboles : des constantes $\mathcal{C}$, des fonctions $\mathcal{F} = \bigcup_m \mathcal{F}_m$ (m arité), des relations $\mathcal{R} = \bigcup \mathcal{R}_m$ (m arité).

Ex 2 : le langage $\mathcal{L}_1$ de la théorie des groupes, contenant $e \in \mathcal{C}$, $*$ et $^{-1}$ deux fonctions resp. binaire et unaire et la relation $=$.

Déf 3 : Soit V un ensemble de variables.
• les termes $\mathcal{T}$ sont définis par la grammaire :
$$\mathcal{T} = V \mid \mathcal{C} \mid \mathcal{F}(\mathcal{T}, \dots, \mathcal{T}).$$
• les formules F sont définies par la grammaire :
$$F = Atom \mid (F \vee F) \mid (F \wedge F) \mid F \Rightarrow F \mid \neg F \mid \exists x F \mid \forall x F$$
où $x \in V$ et $Atom = R(\mathcal{T}, \dots, \mathcal{T})$.

Ex 4 : Sur $\mathcal{L}_1$, $x * y^{-1} \in T$ et $\forall x\ \exists y\ (x * y = e) \in F$.

Déf 5 : • Dans une formule F_0, l'ensemble des variables libres est l'ensemble des variables dont au moins une occurence n'est pas sous la portée d'un quantificateur, et est noté $VL(F_0)$
• Soit $F_0 \in F$, $x \in VL(F_0)$, $t \in \mathcal{T}$. La substitution $F_0[x := t]$ est la formule obtenue en remplaçant dans F_0 toutes les occurences libres de x par t.

Ex 6 : Soit $F_0 : \forall x\ (x.y = yx)$, alors :
• $VL(F_0) = \{y\}$, et si $t = x^{-1}$, alors $F_0[y := x^{-1}]$ est : $(xx^{-1}) = (x^{-1}x)$.

2) Théorie et modèle

Déf 7 : Soit $\mathcal{L}$ un langage du premier ordre. On appelle interprétation de $\mathcal{L}$ un ensemble $\mathcal{M}$ comportant :
• un ensemble non vide $|\mathcal{M}|$, appelé domaine de $\mathcal{M}$.
• pour chaque constante, fonction, relation, une constante, fonction, relation resp., définie sur $|\mathcal{M}|$.

Ex 8 : Pour $\mathcal{L}_1$, on peut prendre pour domaine $\mathbb{Z}$, en interprétant e par 0, $*$ par l'addition, $^{-1}$ par la fonction $m \mapsto -m$.

Déf 9 : Une théorie T est un ensemble de formules closes (càd sans variables libres) appelées axiomes.

Déf 10 : $\mathcal{M}$ est un modèle de T (et on note $\mathcal{M} \models T$) si c'est une interprétation qui satisfait toutes les formules de T. On note $T \models A$ si tout modèle de T est modèle de A.

Ex 11 : Dans $\mathcal{L}_1$, $T = \{\forall x \forall y\ xy = yx\ ;\ \forall x \exists y\ (xy = e)\}$ est une théorie qui admet pour modèle l'interprétation de l'ex 8.

Déf 12 : Une théorie T est contradictoire s'il n'existe pas de modèle pour T.

3) Système formels de preuve

Déf 13 : Un séquent est un couple noté $T \vdash F$ où T est une théorie et F une formule qu'on souhaite montrer.
Un séquent est dit prouvable s'il peut être obtenu par une applications finie de règles de la forme :
$$\frac{\text{prémisses}}{\text{conclusion}}\ \text{nom règle}$$
On appelle système de preuve un ensemble de règles de ce type.

intérêt : en recherche automatique de preuve, il suffit d'en chercher une sans coupure.

Csq : le séquent $\vdash_{LK}$ (qui signifie "absurde") n'est pas dérivable dans LK.

2) Méthode de résolution

Intérêt : adapté à la recherche automatique de preuve.

Déf 19 : Un littéral est une formule atomique sans quantificateurs.
. Une clause est une disjonction de littéraux.

Étape 1 : pour prouver $T \vdash F$, on met $\{T, \neg F\}$ sous forme normale conjonctive, càd comme ensemble de clauses.

Déf 20 : Soit σ une substitution, L et L' deux littéraux et $L[\sigma]$, $L'[\sigma]$ leur image par σ. Si $L[\sigma] = L'[\sigma]$, on dit que L et L' sont unifiables par σ : on note $\sigma \in Unif(L, L')$.

Rq : L'algorithme d'unification détermine si deux littéraux sont unifiables et renvoit un unificateur principal s'il existe.

Étape 2 : à partir des clauses précédemment trouvées, on essaye de prouver $\perp$ en utilisant les règles :

$$\frac{C_1\ L_1 \quad C_2\ L_2}{C_1[\sigma], C_2[\sigma]}\ \text{rés} \quad \sigma \in Unif(L_1, \bar{L_2}) \qquad \text{et} \qquad \frac{C_1, L_1, L_2}{C_1[\sigma], L_1[\sigma]}\ \text{contr} \quad \sigma \in Unif(L_1, L_2)$$

Th 21 : (Complétude) DEV 2
T sous forme normale conjonctive est contradictoire si et seulement si $T \vdash_{Rés} \perp$.

Rq : cette méthode est donc équivalente aux systèmes précédents.

idée : utiliser une stratégie pour savoir quelles clauses utiliser.

Déf 22 (Stratégie SLD) * Un programme logique P est un ensemble fini de clauses qui possède exactement une formule atom. positive.
* Une dérivation SLD de $P \cup \{G\}$ est une suite (G_i, C_i, σ_i) tq :
  → $G_0 = G$ et (G_i) suite de buts
  → $(C_i)_{i \geq 1}$ suite de clauses de P
  → (σ_i) est une suite d'unificateurs principaux tq G_{i+1} soit un résolvant de G_i, C_{i+1} relativement à σ_i.
* la dérivation réussit si c'est une réfutation de $P \cup \{G\}$ et échoue si l'unification avec une clause n'est pas possible.

Th 23 : P programme logique, G clause négative. Si $P \cup \{G\}$ ne possède pas de modèle, il existe une réfutation SLD de $P \cup \{G\}$.

Appl : langage PROLOG.

IV) Logique intuitionniste

En logique classique, si $T \vdash A \vee B$, on ne sait pas si $T \vdash A$ ou $T \vdash B$. De même, si $T \vdash \exists x A$, on aimerait connaître t tq $T \vdash A[t/x]$. Un système qui permet cela est dit constructiviste.

Déf 24 : La logique intuitionniste est obtenue en remplaçant (dans la logique classique) la règle d'absurdité $\perp_c$ par :

$$\frac{T \vdash \perp}{T \vdash A}\ \perp_i$$

Prop 25 : $LC = LI$ + tiers-exclus où $\dfrac{T, A \vdash B \quad T, \neg A \vdash B}{T \vdash B}\ te$

Th 26 : $LI \neq LC$

Prop 27 : La logique intuitionniste est constructiviste, càd :

1) $\vdash_i A_1 \vee A_2$ ssi $\vdash_i A_1$ ou $\vdash_i A_2$
2) $\vdash_i \exists x A$ ssi $\exists t$ tq $\vdash_i A[x:=t]$

II) Principe de déduction naturelle

En déduction naturelle, les règles sont les suivantes :

$$\dfrac{}{T, A \vdash A}\,ax \quad , \quad \dfrac{T \vdash A}{T, B \vdash A}\,aff \quad , \quad \dfrac{T, \neg A \vdash \bot}{T \vdash A}\,\bot_c$$

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

$$\dfrac{T \vdash A \quad T \vdash B}{T \vdash A \wedge B}\,\wedge_i \qquad \dfrac{T \vdash A \wedge B}{T \vdash A}\,\wedge_e^g \qquad \dfrac{T \vdash A \wedge B}{T \vdash B}\,\wedge_e^d$$

$$\dfrac{T \vdash A}{T \vdash A \vee B}\,\vee_i^g \qquad \dfrac{T \vdash B}{T \vdash A \vee B}\,\vee_i^d \qquad \dfrac{T \vdash A \vee B \quad T, A \vdash C \quad T, B \vdash C}{T \vdash C}\,\vee_e$$

$$\dfrac{T, A \vdash \bot}{T \vdash \neg A}\,\neg_i \qquad \dfrac{T \vdash \neg A \quad , \quad T \vdash A}{T \vdash \bot}\,\neg_e$$

$$\dfrac{T \vdash A}{T \vdash \forall x A}\,\forall_i \ , \ x \notin VL(T) \ , \qquad \dfrac{T \vdash \forall x A}{T \vdash A[x := t]}\,\forall_e$$

$$\dfrac{T \vdash A[x := t]}{T \vdash \exists x A}\,\exists_i \qquad \dfrac{T \vdash \exists x A \quad T, A \vdash C}{T \vdash C}\,\exists_e \ \ x \in VL(T, C)$$

Exemple :*

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \wedge B \vdash A \wedge B}\,ax}{A \wedge B \vdash B}\,\wedge_e^d \qquad \dfrac{\dfrac{}{A \wedge B \vdash A \wedge B}\,ax}{A \wedge B \vdash A}\,\wedge_e^g}{A \wedge B \vdash B \wedge A}\,\wedge_i}{\vdash A \wedge B \to B \wedge A}\,\to_i$$

* les involutions sont des bijections) DEV 1

TR 14 : (Complétude) Soit T une théorie et F une formule close. Alors $T \vdash F$ si et seulement si $T \models F$.

Ce théorème résulte du résultat suivant :

TR 15 : T est contradictoire si et seulement si $T \vdash \bot$ (on dit que T est inconsistante).

Cor 16 : (Compacité) T est contradictoire si et seulement si il existe un sous-ensemble fini de T qui est contradictoire.

III) Autres systèmes de déduction

1) Calcul des séquents

Ce système de déduction présente l'avantage d'être complètement symétrique puisqu'on remplace les règle d'élimination par des règles d'introduction à gauche : (notation : $\vdash_{LK}$)

Quelques règles en calcul des séquents : les séquents sont de la forme $T \vdash \Delta$ où T, Δ sont des multi-ensembles de formules.

$$\dfrac{}{\bot \vdash}\,\bot_g \quad , \quad \dfrac{}{A \vdash A}\,ax \quad , \quad \dfrac{T \vdash \Delta}{T \vdash A, \Delta}\,affd$$

$$\dfrac{T, A, B \vdash \Delta}{T, A \wedge B \vdash \Delta}\,\wedge g \qquad \dfrac{T \vdash A, \Delta \quad T \vdash B, \Delta}{T \vdash A \wedge B, \Delta}\,\wedge d$$

$$\dfrac{T \vdash A, \Delta \qquad T', A \vdash \Delta'}{T, T' \vdash \Delta, \Delta'}\,\text{coupure} \qquad \text{etc...}$$

Théorème 17 : LK est équivalent au système de déduction naturelle.

Csq 18 : $A_1, \dots, A_n \vdash_{LK} B_1, \dots B_m$ si et seulement si $\models A_1 \wedge \dots \wedge A_n \to B_1 \vee \dots \vee B_m$

Thm 18 : (Elimination des coupures) : Si $T \vdash_{LK} \Delta$, alors il existe une démonstration qui n'utilise pas la règle de coupure.