1er tour 1 symbole de cste pr avoir $T \neq \emptyset$. ↳ Si ∅ ... on ajoute "a" sans changer la
↳ On a pas autorisé les modèles vides. // classe des modèles ??

924

Théories et modèles en logique du premier ordre. Exemples.

I Syntaxe et sémantique en logique du 1er ordre

1) Syntaxe [DNR] p 11–16

Hyp: il y a au - 1 symb de cte

Déf 1 Un langage $\mathcal{L}$ est une famille de symboles : les constantes, les symboles de fonction et les symboles de relation.
Rq on ne considère que des langages égalitaires.

Ex 2 Théorie des groupes : $\mathcal{L}_1$ contient le neutre "e", deux symboles de fonctions "$*$" et "$^{-1}$" et un symbole de relation "=".

Soit $\mathcal{V} = (x_i)_{i \in \mathbb{N}}$ un ensemble infini dénombrable de variables.

Déf 3 Soit $\mathcal{L}$ un langage, l'ensemble des termes est le plus petit ensemble contenant les variables, les constantes et stable par l'application des symboles de fonctions.

Déf 4 Un terme est clos si il ne contient pas de variables.
Ex 5 $x * y^{-1}$ est un terme sur $\mathcal{L}_1$ et $e^{-1} * e$ est un terme clos sur $\mathcal{L}_1$.

Déf 6 Les formules atomiques de $\mathcal{L}$ sont les formules de la forme $R(t_1, \dots t_n)$ où R est un symbole de relation d'arité n de $\mathcal{L}$ et $t_1 \dots t_n$ sont des termes de $\mathcal{L}$.
On note $\mathcal{A}tom$ l'ensemble de ces formules.

Déf 7 L'ensemble $\mathcal{F}$ des formules de $\mathcal{L}$ est défini par la grammaire : $\mathcal{F} = \mathcal{A}tom \mid (\mathcal{F} \vee \mathcal{F}) \mid (\mathcal{F} \wedge \mathcal{F}) \mid (\mathcal{F} \Rightarrow \mathcal{F}) \mid \neg \mathcal{F} \mid \exists x \mathcal{F} \mid \forall x \mathcal{F}$ pour tout $x \in \mathcal{V}$.

Ex 8 $\forall x \exists y ((x * y = e) \wedge (\neg (y * x = e)))$ est une formule ~~de~~ $\mathcal{L}_1$.

2) Sémantique et modèles [DNR] p 68–70

Déf 9 Une structure $\mathcal{M}$ de $\mathcal{L}$ est la donnée de :
- un ensemble non vide M (domaine)
- pr chaque symbole de cste c de $\mathcal{L}$ un symbole $c^{\mathcal{M}}$ de M
- pr chaque symbole de f° f de $\mathcal{L}$, d'arité n, une fonction $f^{\mathcal{M}} : M^n \to M$
- pr chaque symbole de relat° R de $\mathcal{L}$, d'arité n, un sous-ensemble $R^{\mathcal{M}} \subset M^n$.

Déf 10 Soit $\mathcal{M}$ une structure de $\mathcal{L}$. Une valuation est une fonction $\rho : \mathcal{V} \to M$.

Déf 11 La valeur d'un terme t dans $\mathcal{M}$ par ρ, notée $[\![t]\!]_\rho^{\mathcal{M}}$ est définie par induction :
$[\![c]\!]_\rho = c^{\mathcal{M}}$; $[\![x]\!]_\rho^{\mathcal{M}} = \rho(x)$; $[\![f(t_1, \dots t_n)]\!]_\rho^{\mathcal{M}} = f^{\mathcal{M}}([\![t_1]\!]_\rho^{\mathcal{M}}, \dots [\![t_n]\!]_\rho^{\mathcal{M}})$.

Ex 12 $M = \mathbb{Z}$, $e = 0$, $* = +$; $^{-1} = n \mapsto -n$ est une structure de $\mathcal{L}_1$.

Déf 13 La valeur d'une formule F de $\mathcal{L}$ dans $\mathcal{M}$ par ρ est un élément de $\{0,1\}$, notée $[\![F]\!]_\rho^{\mathcal{M}}$ défini par induction sur $\mathcal{F}$.

Prop 14 La valeur de F ne dépend que de la valeur de ρ sur les variables libres de F. [LR] p 59

On note $\mathcal{M}, \rho \models F$ si $[\![F]\!]_\rho^{\mathcal{M}} = 1$. [DNR] p 71

Déf 15 Dans ce cas, on dit que $\mathcal{M}$ est un modèle de F.

Cor 16 Si F est close alors $[\![F]\!]_\rho^{\mathcal{M}}$ ne dépend pas de ρ, on note $\mathcal{M} \models F$.

Déf 17 Une formule F est valide si pour toute structure $\mathcal{M}$ et toute valuation ρ, $\mathcal{M}, \rho \models F$. On note $\models^* F$. [LR] p 60 et [DNR] p 72

Déf 18 Deux formules F et G sont équivalentes si $\models^* (F \Leftrightarrow G)$. [DNR] p 75

3) Théories

Déf 19 Une théorie T est un ensemble de formules closes. Ses éléments sont appelés axiomes. ([DNR] p 75)

Ex Arithmétique de Peano Soit $\mathcal{L} = \{0, S, +, \times\}$. [DNR] p 111

Déf 20 P_0 (l'arithmétique élémentaire) est l'ensemble des formules suivantes : $A_1 : \forall x (Sx \neq 0)$ $A_2 : \forall x (x = 0 \vee \exists y (x = Sy))$
$A_3 : \forall x y (Sx = Sy \Rightarrow x = y)$ $A_4 : \forall x (x + 0 = x)$ $A_5 : \forall x y (x + Sy = S(x+y))$
$A_6 : \forall x (x \times 0 = 0)$ $A_7 : \forall x, y (x \times Sy = x \times y + x)$.

Déf 21 Soit F une formule, on note $Rec_{F,x}$ la clôture universelle de $(F[x:=0] \wedge \forall y(F[x:=y] \Rightarrow F[x:=Sy])) \Rightarrow \forall x F$.
On note $Rec = \{Rec_{F,x}$ tq F formule$\}$.

Déf 22 Arithmétique de Peano $PA = P_0 \cup Rec$ [CL] p178

Déf 23 $\mathcal{M}$ est un modèle de T si pour toute formule F de T, $\mathcal{M} \models F$.
On note $\mathcal{M} \models T$

Déf 24 • Une théorie est dite consistante si elle admet au moins un modèle. Sinon, on dit qu'elle est contradictoire
• Soient T une théorie et F une formule close. On dit que F est conséquence sémantique de T si tout modèle de T est modèle de F. On note $T \models^* F$.
Si F n'est pas close, on prend sa clôture universelle.
• Deux théories T_1 et T_2 sont équivalentes si toute formule de T_1 est conséquence de T_2 et toute formule de T_2 est conséquence de T_1

Ex 25 PA est une théorie non-contradictoire. Habituellement on prend comme domaine de structure $\mathbb{N}$. [DNR] p112

Th 26 Soient T une théorie et G une formule close : [CL] p181
$T \models^* G$ ssi $T \cup \{\neg G\}$ est contradictoire.

Th 27 (Lowenheim-Skolem) Soit $\mathcal{L}$ un langage au plus dénombrable, soit T une théorie de $\mathcal{L}$ possédant un modèle infini. Alors T possède un modèle dénombrable. DVPT 1

II Déduction : Méthode de résolution

1) Mise sous forme de clauses [DNR] p264

Déf 28 Un littéral est une formule atomique ou sa négation

Déf 29 Une clause est un ensemble fini de littéraux

→ On veut passer d'un ensemble (fini) de formules Σ à un ensemble de clauses. [LR] p84
a) Mise sous forme prénexe normale conjonctive
b) Mise sous forme de Skolem

Th 30 Soit F une formule close. F admet un modèle ssi sa forme de Skolem en admet un.

c) Distribution des quantificateurs par rapport aux conjonctions
d) Décomposition en clauses universelles.

2) Méthode de résolution-correction [DNR] p248/264-267

Déf 31 Deux termes u et v sont unifiables s'il existe une substitution σ telle que $u(\sigma) = v(\sigma)$.
On dit que σ est un unificateur de u et v.

Déf 32 Le terme u filtre le terme v s'il existe une substitution σ tel que $u(\sigma) = v$.

Th 33 Soient u et v deux termes unifiables. Il existe un unificateur σ de u et v, dit principal, tel que pour tout unificateur σ' de u et v, il existe une substitution σ'' tq $\sigma' = \sigma'' \circ \sigma$.
On le note $mgu(u,v)$

→ But : on prend un ensemble de clauses E, on veut dériver la clause vide à partir des règles suivantes

Déf 34 Soient C_1, C_2 deux clauses, soient L_1, L_2 deux littéraux

résolution : $\dfrac{C_1, L_1 \quad C_2, L_2 \quad \sigma = mgu(L_1, \overline{L_2})}{C_1(\sigma), C_2(\sigma)}\ res$

contraction : $\dfrac{C_1, L_1, L_2 \quad \sigma = mgu(L_1, L_2)}{C_1(\sigma), L_1(\sigma)}\ contr$

Rq 35 On définit les unificateurs sur les littéraux comme sur les termes.

Ex 36 $C_1 = \neg R(x,a), R(a,x)$ $\quad C_2 = \neg R(v,f(y)), \neg R(v,y)$
$C_3 = \neg R(z,z), R(z,a)$ $\quad C_4 = R(u,f(y)), R(u,y)$.
cf. Annexe 1.

Déf 37 Un ensemble de clauses E est incohérent si l'on peut dériver la clause vide $\square$ à partir de E.

Th 38 Si E est incohérent, il est contradictoire.

3) Modèles de Herbrand - complétude [LR] p98-99

Soit $\mathcal{L}$ un langage

Déf 39 Le domaine de Herbrand de $\mathcal{L}$ est l'ensemble des termes clos de $\mathcal{L}$. Noté H.

Déf 40 La <u>base de Herbrand</u> $\mathcal{B}$ est l'ensemble des formules atomiques closes de $\mathcal{L}$

Déf 41 Une <u>structure de Herbrand</u> $\mathcal{H}$ pour $\mathcal{L}$ est une structure de domaine H telle que pour tout symbole de fonction f d'arité n de $\mathcal{L}$
$f^{\mathcal{H}} : (t_1, \dots t_n) \in H^n \mapsto f t_1 \dots t_n \in H$.

Déf 42 Soit F une formule close. Un <u>modèle de Herbrand</u> de F est une structure de Herbrand qui satisfait F.

Prop 43 Soit F universelle close. F possède un modèle <u>ssi</u> F possède un modèle de Herbrand.

Lemme 44 Soient E un ensemble de clauses et L un littéral clos.
Si on peut dériver la clause vide à partir de $E \cup \{L\}$ <u>alors</u> à partir de E, on peut dériver la clause vide <u>ou</u> un littéral qui filtre $\bar{L}$ [DNR] p266

DVP2

Th 45 (complétude de la résolution?) Si E est contradictoire <u>alors</u> E est incohérent [DNR] p 267

4) Applications [DNR] p86

Th 46 Soit T une théorie. T est contradictoire <u>ssi</u> il existe un sous-ensemble fini de T qui est contradictoire.

App 47 Si T admet un modèle infini <u>alors</u> T admet un modèle infini non-dénombrable

Th 48 Il existe des modèles non-isomorphes de PA. [DNR] p112

III Décidabilité [DNR] p125-126.

Déf 49 Une théorie T est <u>décidable</u> si le problème suivant est décidable.
<u>Entrée</u> F formule du langage de T
<u>Sortie</u> $T \models F$?

Prop 50 PA est indécidable.

Mais **Prop 51** <u>Entrée</u> Une formule écrite sur $\mathcal{L} = \{0, S, +\}$
<u>Sortie</u> Cette formule est-elle vraie dans $\mathbb{N}$?
est décidable.

Annexe 1

$$\dfrac{\dfrac{\dfrac{C_3 \quad C_4}{R(f(y),a),\ R(f(y),y)}\ \text{res}}{R(f(a),a)}\ \text{contr} \qquad \dfrac{\dfrac{C_1 \quad C_2}{\neg R(f(y),a),\ \neg R(f(y),y)}\ \text{res}}{\neg R(f(a),a)}\ \text{contr}}{\square}\ \text{res}$$

Références

David/Nour/Raffalli <u>Introduction à la logique</u>

Lassaigne/Rougemont <u>Logique et fondements de l'informatique</u>

Cori/Lascar <u>Logique mathématiques</u>, Tome 1.

↳ Il faut PRÉPARER l'intro. → Il faut resituer les modèles de la leçon. + MOTIVER la leçon

↳ Ici Au travers d'un ens. de formules, on veut chercher à décrire des structures ($\mathbb{N}$, groupes).

{formules} = façon dont les maths décrivent des formules maths.

Une fois qu'on a 1 {formules} (qui peut être ∞), on veut savoir ce qu'on a défini

(? objets maths qui $\exists$,

Est-ce qu'il y en a qui st remarquables? ↳ Herbrand)

Syntaxe → quelles formules on a le droit d'écrire?

Sémantique ↳ quelle est leur signification?

II → Plutôt mettre en avant les modèles de Herbrand.

↳ puis les applications (résolution, 1 version de L-S) (capturer un modèle remarquable puis ce qu'on en déduit)

cardinalité

$\#$ Modèle de Herbrand $= \#$ Sign.

Modèle de Herbrand.

Th: $\exists\ \mathfrak{M}$ ssi $\exists\ \mathcal{H}$

⚠ S'il y a "=" ds $\mathcal{L}$, c'est pas vrai!

Preuve: Si pas "=" : c'est classique.

Sinon: Soit T une théorie. Soit $\mathfrak{M} \models T$.

On regarde $T' = T \cup \{\text{Axiomes de } \approx\}$

$x_1 \approx y_1 \Rightarrow f(x_1,\dots,x_n) \approx f(y_1,x_2\dots x_n)$ pr ttes les positions, pr ttes les fonctions ...

Toutes les props de l'égalité!

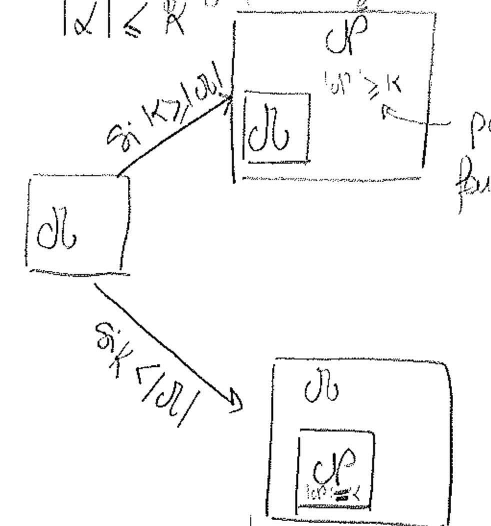
Comme $\mathfrak{M} \models T$, $\mathfrak{M} \models T'$ (il suffit d'interpréter $\approx$ par $=$).

On peut construire $\mathcal{H}$ de Herbrand, modèle de $T \cup \{\text{Axiomes}\}$.

Et on fait $\mathcal{H}/_{\approx}$ pour avoir un modèle de $\tilde{T} = T$ où l'égalité c'est VRAIMENT l'égalité.

Löwenheim-Skolem. Soit $\mathcal{L}$ langage fixé. $|\mathcal{L}| \leq \kappa$

extension élémentaire



pour avoir =, il faut ↑ plus gd puis ↓ "en visant"

$TR_{\mathcal{L}}(\mathfrak{M}) = TR_{\mathcal{L}}(\mathcal{N})$

Par l'absurde: Si T a des modèles finis arbitrairement grands ... sat de ... sat ⇒ modèle ∞. NON

compacité: on peut borner la taille des modèles → il y a un + gd modèle

Cor: L-S ascendant descendant

Soit T sur $\mathcal{L}$

Si T contradictoire bon...

Sinon ou bien T n'a que des modèles finis ou bien T a un modèle infini.

→ Pb: rq après la déf 1. ?

Théorème de Löwenheim - Skolem 12'04 12'17 18'24 (c)

Réf David/Nour/Raffalli

Th Soit $\mathcal{L}$ langage au plus dénombrable, Soit T une théorie sur $\mathcal{L}$ (du 1er ordre)
si T possède un modèle infini **alors** T possède un modèle dénombrable

dém Soit $\mathcal{M}$ un modèle infini de $\mathcal{L}$ tel que $\mathcal{M} \models T$ et soit $P \subset M$

__Étape 1 On construit un modèle $\mathcal{N}$__

Pour toute formule à n variables libres $\{y_1 \dots y_n\}$ de la forme $\exists x F$ et tout n-uplet $(a_1 \dots a_n) \in P^n$ tels que $[\![\exists x F]\!]_{\mathcal{M}}^{\rho} = 1$ où $\rho = (y_i := a_i)$, noté $\mathcal{M}, (y_i := a_i) \models \exists x F$

donc il existe $e_{a_1, \dots a_n, F} \in M$ tel que $[\![F]\!]_{\mathcal{M}}^{\rho[x := e_{a_1 \dots a_n, F}]} = 1$, noté $\mathcal{M}, (y_i := a_i, x := e_{a_1 \dots a_n, F}) \models F$

On considère $E(P) = \{ e_{a_1 \dots a_n, F}$ pour $a_1 \dots a_n$ et F comme précédemment $\}$

Soit $a \in M$, $X_0 = \{a\} \cup \{f_{\mathcal{M}}, f \in \mathcal{F}_0\}$??? et $X_n = X_{n-1} \cup E(X_{n-1})$. On pose $N = \bigcup_{n \geq 0} X_n$

Nou $X_1 = X_0 \cup \{e$ tq $\exists$ F de la forme $\exists x F$ tq $\mathcal{M}(y_i := a, x := e) \models F\}$ de $f_n \in X_0$

On munit N d'une structure de modèle $\mathcal{N}$: pour tout les symboles de relation d'arité m $R_{\mathcal{N}} = R_{\mathcal{M}} \cap N^m$ et pour tout symbole de fonction d'arité n $f_{\mathcal{N}} = f_{\mathcal{M}}/_{N^n}$

__Étape 2 Mq $\mathcal{N}$ est un modèle__ ie pour tout symbole de fonction d'arité n $f_{\mathcal{N}} : N^n \to N$.

Soit $(a_1 \dots a_n) \in N^n$ et F de la forme $\exists x \underbrace{\{x = f_{\mathcal{M}}(a_1 \dots a_n)\}}_{G}$.

$\mathcal{M}, (y_i := a_i, x := f_{\mathcal{M}}(a_1 \dots a_n)) \models G$ donc $\mathcal{M}, (y_i := a_i) \models \exists x G = F$

Par définition de N, il existe $p \in \mathbb{N}$ tel que $\forall 1 \leq i \leq n$, $a_i \in X_p$ donc $f_{\mathcal{N}}(a_1 \dots a_n) = \overbrace{f_{\mathcal{M}}(a_1 \dots a_n)}^{\in N^n}$ $\in E(X_p) \subset N$

donc $f_{\mathcal{N}}$ est à valeurs dans N. Ainsi $\mathcal{N}$ est un modèle

__Étape 3 Mq $\mathcal{N}$ est au plus dénombrable__ on démontre par récurrence sur $n \in \mathbb{N}$ que X_n est dénombrable

- __n=0__ X_0 est dénombrable
- __n≥1__ si X_n est dénombrable __alors__ $E(X_n)$ l'est aussi car il contient au plus 1 élément par formule F et par k-uplet de X_n où k = nombre de $\forall$ avant le 1er $\exists$ de F (on peut supp F sous forme prénexe)

Ainsi __X_{n+1} est dénombrable__ par union d'ensembles dénombrables

__Étape 4 Mq $\mathcal{N} \models T$__ On montre par induction : "Pour tout $(a_1 \dots a_n) \in N^n$, F à n variables libres, $\mathcal{M}(y_i := a_i) \models F$ __ssi__ $\mathcal{N}(y_i := a_i) \models F$."

Si $F = R t_1 \dots t_s$ avec t_i des termes clos alors comme $a_i \in N$ et $R_{\mathcal{N}} = R_{\mathcal{M}} \cap N^s$, on a ce qu'on voulait

si $F = \neg G$ ou $F = G \wedge H$ ok par ind $\mathcal{M} \models G \iff \mathcal{N} \models G$ donc $\mathcal{M} \models \neg G \iff \mathcal{N} \models \neg G$
$\mathcal{M} \models G \iff \mathcal{N} \models G$ et $\mathcal{M} \models H \iff \mathcal{N} \models H$ donc $\mathcal{M} \models G \wedge H \iff \mathcal{N} \models G \wedge H$

si $F = \forall x G$ → on se ramène au cas $\exists$: $\neg \exists x \neg G$

si $F = \exists x G$, ($\Leftarrow$) si $\mathcal{N}[y_i := a_i] \models F$ alors il existe $a \in N$ tel que $\mathcal{N}[y_i := a_i, x := a] \models G$
← hyp. ind. form. G et (n+1)-uplet $(a_1, \dots, a_n, a)$

donc $\mathcal{M}[y_i := a_i, x := a] \models G$ donc $\mathcal{M}[y_i := a_i] \models F$.

($\Rightarrow$) si $\mathcal{M}[y_i := a_i] \models \exists x G$ alors $\mathcal{M}[y_i := a_i, x := e_{a_1, \dots, a_n, G}] \models G$
← hyp. ind. formule G (n+1)-uplet $(a_1, \dots, a_n, e_{a_1, \dots, a_n})$

donc $\mathcal{N}[y_i := a_i, x := e_{a_1, \dots, a_n, G}] \models G$ donc $\mathcal{N}[y_i := a_i] \models F$ car $e_{a_1, \dots, a_n, G} \in N$

Étape 5 Conclusion

~~Si $\mathcal{M}$ est~~ fini, on considère $\{F_n\}$ telle que F_n exprime que le domaine du modèle a moins de n éléments.

Comme $\mathcal{M}$ est infini, et $\mathcal{M} \models T$, $\mathcal{M} \models T \cup \{F_n, n \in \mathbb{N}\}$.

Alors par le pt (iii), on a $\mathcal{N} \models T \cup \{F_n, n \in \mathbb{N}\}$. donc $\forall n$, $\mathcal{N} \models F_n$ donc ~~$\mathcal{M}$~~ $\mathcal{N}$ est infini et $\mathcal{N} \models T$. D'où $\mathcal{N}$ est (exactement) dénombrable et modèle de T

On peut le faire avec les modèles TP,
mais ça marche plus si $H \leq +\infty$ (pr montrer $\boxed{\text{exact}}$ dénombrable)
↳ si que des P_i et un nbre fini

Si énoncé → "au plus" se faire avec TP
(enrichir le langage!)