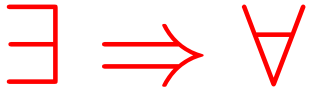
Logique et Calculabilité
INF551



Dr. Stéphane Lengrand,

Stephane.Lengrand@Polytechnique.edu

Cours II
La notion de modèle

I. Règles de la logique des prédicats : suite et fin

Les variables et les variables libres

- $Var(x) = \{x\}$,
- $Var(f(x_1^1 ... x_{k_1}^1 t_1, ..., x_1^n ... x_{k_n}^n t_n))$
  $= Var(t_1) \cup \{x_1^1, ..., x_{k_1}^1\} \cup \cdots \cup Var(t_n) \cup \{x_n^n, ..., x_{k_n}^n\}$.

$Var(\forall x\ (x = x))$?

- $FV(x) = \{x\}$,
- $FV(f(x_1^1 ... x_{k_1}^1 t_1, ..., x_1^n ... x_{k_n}^n t_n))$
  $= (FV(t_1) \setminus \{x_1^1, ..., x_{k_1}^1\}) \cup \cdots \cup (FV(t_n) \setminus \{x_n^n, ..., x_{k_n}^n\})$

$FV(\forall x\ (x = x))$?

La classification des règles en déduction naturelle

La plupart des règles concernent un symbole (connecteur ou quantificateur) unique

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-intro}$$

classification des règles en fonction du symbole concerné

Connecteur dans conclusion ou prémisse : intro / élim

intro / élim : fabriquer / utiliser

Exceptions : axiome, tiers exclu, négation

Négation : symbole composite : $\neg A$ peut être défini comme $A \Rightarrow \bot$

Les règles une par une

axiome : la notion de contexte, raisonnement hypothético-déductif

$\top$: pas d'élim

$\bot$: pas d'intro

$\wedge$: ras

$\vee$: intros triviales, élim démonstration par cas

$\Rightarrow$: intro : la notion de contexte, raisonnement hypothético-déductif

$\neg$: lien avec $\Rightarrow$, les deux formes de raisonnement par l'absurde, forme radicale de raisonnement hypothético-déductif

Les règles une par une

$\forall$

Intro : “soit x un objet”, notion de généricité (x n’apparaît pas (libre) dans Γ),

Elim : substitution

$\exists$

Intro : substitution,

Elim : “$\exists x\ P$, appelons le y”, y générique

tiers exclu : en déduction naturelle, un cheveu sur la soupe

(mais pas dans d’autres systèmes)

La substitution

$\forall$-élim et $\exists$-intro : une opération annexe : la substitution $(t/x)u$

L'opération qui donne son sens au mot variable

(dans les langages de la logique des prédicats comme tous les autres langages)

Définition simple pour les langages sans symboles lieurs de var.

- $(t/x)(f(u_1, ..., u_n)) = f((t/x)u_1, ..., (t/x)u_n)$
- $(t/x)x = t$
- $(t/x)y = y$ si $x \neq y$

Dans les langages avec des symboles lieurs de variables

$(4/x)(\forall x\ P(x)) = \forall x\ P(4)$ ou $\forall x\ P(x)$?

Règle 1 : ne substituer que les variables libres

Première tentative :

– $\langle t/x\rangle(\forall y\ A) = \forall y\ (\langle t/x\rangle A)$ si $x \neq y$

– $\langle t/x\rangle(\forall x\ A) = \forall x\ A$

Mais ce n'est pas suffisant

$$\langle 4/y \rangle (\forall x\ P(x+y)) = \forall x\ P(x+4)$$

$$\langle z/y \rangle (\forall x\ P(x+y)) = \forall x\ P(x+z)$$

$$\langle x/y \rangle (\forall x\ P(x+y)) = \forall x\ P(x+x)$$

L'occurrence libre de x a été capturée

Règle 2 : éviter les captures de variables

$$(x/y)(\forall x\ P(x+y)) = \forall w\ P(w+x)$$

Renommer la variable liée x en w

Pourquoi w plutôt que v ?

C'est équivalent (variable liée = variable muette)

Équivalence alphabétique (α-équivalence)

α-équivalence

On définit pour ça l'échange de 2 variables sur P : $(xy)P$

partout où vous avez écrit x (lié ou libre), vous mettez y, et vice versa

$\exists x P$ est identifié avec $\exists y (xy)P$ si $y \notin FV(P)$
$\forall x P$ est identifié avec $\forall y (xy)P$ si $y \notin FV(P)$

Pourquoi "si $y \notin FV(P)$" (i.e. y est une variable fraiche) ?

$(y = -1) \wedge \exists x (x \times x = y)$ n'est pas la même chose que
$(y = -1) \wedge \exists y (y \times y = x)$

Exemple : $\forall x \; P(x + w)$ et $\forall y \; P(y + w)$ sont équivalents

Désormais on ne raisonne plus que sur des classes d'expressions modulo équivalence alphabétique

La substitution (enfin ...)

Attention quand on définit $(t/x)(\forall y P)$ et $(t/x)(\exists y P)$!!!

Que se passe-t-il si $y \in FV(t)$?

Moralité :

$(t/x)(\forall y P) = \forall y (t/x)P$ et $(t/x)(\exists y P) = \exists y (t/x)P$

si $x \neq y$ et $y \notin FV(t)$

sinon, renommer y en l'échangeant avec variable fraiche z : $(yz)P$

Généraliser tout cela à la substitution simultanée $t_1/x_1, \ldots, t_n/x_n$ et à un langage quelconque

Un empilement de notions : échange $\rightarrow$ équivalence alphabétique $\rightarrow$ classes d'expressions $\rightarrow$ substitution

De nombreuses erreurs dans les livres

De nombreuses erreurs dans les systèmes de calcul symbolique (langages de programmation, systèmes de calcul formel, systèmes de traitement de démonstrations, ...)

II. Variations sur le tiers exclu

La double négation

Remplacer le tiers exclu par la règle

$$\frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}\ \text{double négation}$$

Équivalence

Dans un sens : si $\Gamma \vdash \neg\neg A$ démontrable en déduction naturelle alors $\Gamma \vdash A$ également

Dans l'autre : $\Gamma \vdash A \vee \neg A$ démontrables dans le système avec la règle *double négation*

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, \neg(A \vee \neg A), A \vdash \neg(A \vee \neg A)}\ \text{axiome} \quad \dfrac{\dfrac{}{\Gamma, \neg(A \vee \neg A), A \vdash A}\ \text{axiome}}{\Gamma, \neg(A \vee \neg A), A \vdash A \vee \neg A}\ \vee\text{-intro}}{\Gamma, \neg(A \vee \neg A), A \vdash \bot}\ \neg\text{-élim}}{\Gamma, \neg(A \vee \neg A) \vdash \neg A}\ \neg\text{-intro} \quad \dfrac{\dfrac{\dfrac{}{\Gamma, \neg(A \vee \neg A) \vdash \neg(A \vee \neg A)}\ \text{axiome} \quad \dfrac{\dfrac{}{\Gamma, \neg(A \vee \neg A) \vdash A}\ \text{axiome}}{\Gamma, \neg(A \vee \neg A) \vdash A \vee \neg A}\ \vee\text{-intro}}{\Gamma, \neg(A \vee \neg A) \vdash \bot}\ \neg\text{-élim}}{\Gamma \vdash \neg\neg(A \vee \neg A)}\ \neg\text{-intro}}{\Gamma \vdash A \vee \neg A}\ \text{double négation}$$

Les séquents à plusieurs conclusions

Au lieu de garder la négation de $A \vee \neg A$ à gauche

laissons la à droite

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, A \vdash \bot, A}\text{ axiome}}{\Gamma, A \vdash \bot, A \vee \neg A}\vee\text{-intro}}{\Gamma \vdash \neg A, A \vee \neg A}\neg\text{-intro}}{\Gamma \vdash A \vee \neg A, A \vee \neg A}\vee\text{-intro}}{\Gamma \vdash A \vee \neg A}\text{ contraction}$$

Les séquents à plusieurs conclusions

Des séquents avec plusieurs hypothèses et plusieurs conclusions

Une règle qui permet de dupliquer une conclusion

$$\frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}\ \text{contraction}$$

Intuitivement : une proposition dans les conclusions = sa négation dans les hypothèses

III. Exemples de théories

La théorie de l'égalité

c.f. PC de la semaine dernière

Reflexivité (identité) et substitutivité (Leibniz)

La théorie des classes

ι pour les objets

κ pour les classes d'objets

des symboles de fonction d'arité $(\iota, ..., \iota, \iota)$ et des symboles de prédicat d'arité $(\iota, ..., \iota)$

et un symbole de prédicat ϵ d'arité (ι, κ)

Pour chaque A

– ne contenant pas le symbole ϵ,

– dont les variables libres sont parmi y, x_1,. . .,x_n

un axiome

$$\forall x_1 ... \forall x_n \exists c \forall y \, (y \, \epsilon \, c \Leftrightarrow A)$$

Schéma de compréhension

L'arithmétique

ι pour les entiers, κ pour les classes d'entiers, 0, S, $+$, $\times$, ϵ et $=$

Axiomes de l'égalité, schéma de compréhension, plus :

$$\forall x\, \forall y\, (S(x) = S(y) \Rightarrow x = y)$$

$$\forall x\, \neg(0 = S(x))$$

$$\forall c\, (0\ \epsilon\ c \Rightarrow \forall x\, (x\ \epsilon\ c \Rightarrow S(x)\ \epsilon\ c) \Rightarrow \forall y\, y\ \epsilon\ c)$$

$$\forall y\, (0 + y = y)$$

$$\forall x\, \forall y\, (S(x) + y = S(x + y))$$

$$\forall y\, (0 \times y = 0)$$

$$\forall x\, \forall y\, (S(x) \times y = (x \times y) + y)$$

La théorie naïve des ensembles

Une seule sorte

$\in$

pour chaque A dont les variables sont parmi y, x_1,. . .,x_n, un axiome

$$\forall x_1 ... \forall x_n \exists c \forall y \, (y \in c \Leftrightarrow A)$$

En particulier

$$\exists r \forall y \, (y \in r \Leftrightarrow \neg y \in y)$$

Or $\forall y \, (y \in r \Leftrightarrow \neg y \in y) \vdash \bot$ démontrable

La théorie des classes binaires

ι pour les objets

σ pour les classes binaires

des symboles de fonction d'arité $(\iota, ..., \iota, \iota)$ et des symboles de prédicat d'arité $(\iota, ..., \iota)$

et ϵ_2 d'arité (ι, ι, σ)

le schéma de compréhension et pour chaque A ne contenant pas le symboles ϵ_2 un axiome de la forme

$$\forall x_1 ... \forall x_n \exists r \forall y \forall z \, (y, z \, \epsilon_2 \, r \Leftrightarrow A)$$

La théorie des ensembles de Zermelo-Fraenkel

Sortes ι pour les ensembles, σ pour les classes binaires

$=$, $\in$, ϵ_2

Axiomes de l'égalité, schéma de compréhension binaire

Axiome de la réunion :

$$\forall x \exists z \forall w \, (w \in z \Leftrightarrow (\exists v \, (w \in v \wedge v \in x)))$$

Informel : "$z = \bigcup x$"

Axiome des parties :

$$\forall x \exists z \forall w \, (w \in z \Leftrightarrow (\forall v \, (v \in w \Rightarrow v \in x)))$$

Informel : "$z = \wp(x)$"

La théorie des ensembles de Zermelo-Fraenkel

Axiome de remplacement :

$$\forall r\,[fonctionnelle(r) \Rightarrow \forall x \exists y \forall w\,(w \in y \Leftrightarrow \exists z\,(z \in x \wedge z, w\ \epsilon_2\ r))]$$

où $fonctionnelle(r)$ est la proposition
$\forall x \forall y \forall y'\,((x, y\ \epsilon_2\ r \wedge x, y'\ \epsilon_2\ r) \Rightarrow y = y')$.

Informel : "$y = Im(r)$"

Axiome de l'infini :

$$\exists I\,(\forall x\,(vide(x) \Rightarrow (x \in I)) \wedge \forall x \forall y\,((x \in I \wedge Succ[x, y]) \Rightarrow (y \in I)))$$

où $vide(x)$ est la proposition $\forall y\,(\neg(y \in x))$ "$x = \emptyset$"
et $Succ[x, y]$ la proposition $\forall z\,(z \in y \Leftrightarrow (z \in x \vee z = x)$ "$y = x \cup \{x\}$"

Axiome d'extensionalité :

$$\forall x \forall y\,((\forall z\,(z \in x \Leftrightarrow z \in y)) \Rightarrow x = y)$$

IV. La notion de modèle

Comment démontrer qu'une proposition n'est pas démontrable ?

La notion de modèle

Un langage $\mathcal{L} = (\mathcal{S}, \mathcal{F}, \mathcal{P})$

Un modèle de ce langage est formé de

– pour chaque s, un ensemble non vide $\mathcal{M}_s$

– un ensemble non vide $\mathcal{B}$, un sous-ensemble $\mathcal{B}^+$

– pour chaque f d'arité $(s_1, ..., s_n, s')$, une fonction $\hat{f}$ de $\mathcal{M}_{s_1} \times ... \times \mathcal{M}_{s_n}$ dans $\mathcal{M}_{s'}$

– pour chaque P d'arité $(s_1, ..., s_n)$, une fonction $\hat{P}$ de $\mathcal{M}_{s_1} \times ... \times \mathcal{M}_{s_n}$ dans $\mathcal{B}$

– $\hat{\top}$, $\hat{\bot}$, $\hat{\neg}$, $\hat{\wedge}$, $\hat{\vee}$, $\hat{\Rightarrow}$, $\hat{\forall}$, $\hat{\exists}$

Un langage et un modèle de ce langage

Une fonction $[\![\ ]\!]$ qui associe

– à chaque terme t un élément $[\![t]\!]$ de $\mathcal{M}_s$ (s sorte de t)

– à chaque proposition A, un élément $[\![A]\!]$ de $\mathcal{B}$

Morphisme :

$$[\![f(t_1, ..., t_n)]\!] = \hat{f}([\![t_1]\!], ..., [\![t_n]\!])$$

$$[\![P(t_1, ..., t_n)]\!] = \hat{P}([\![t_1]\!], ..., [\![t_n]\!])$$

$$[\![A \wedge B]\!] = \hat{\wedge}([\![A]\!], [\![B]\!]) \ ...$$

Combien de fonctions possibles ?

Combien de fonctions possibles ?

Une seule si on se limite aux termes et propositions sans variables

Mais plusieurs si on a des variables

La fonction $[\![\ ]\!]$ complètement définie par sa valeur sur les variables

(idem morphisme d'e.v. défini par son image sur une base)

Valuation : fonction de domaine fini qui associe aux variables $x_1, ..., x_n$ de sortes $s_1, ..., s_n$ des éléments $a_1, ..., a_n$ de $\mathcal{M}_{s_1}, ..., \mathcal{M}_{s_n}$

$\phi = (x_1 = a_1, ..., x_n = a_n)$

$[\![\ ]\!]_\phi$

$[\![x]\!]_\phi = \phi(x),$

$[\![f(t_1, ..., t_n)]\!]_\phi = \hat{f}([\![t_1]\!]_\phi, ..., [\![t_n]\!]_\phi), ...$

Toutes les expressions dont les variables sont dans le domaine de ϕ

$[\![\forall x\ A]\!]_\phi$?

$$[\![\forall x\ A]\!]_\phi = \hat{\forall}([\![A]\!]_\phi)$$

$$FV(A) \subseteq FV(\forall x\ A) \cup \{x\}$$

On considère l'ensemble de toutes les valeurs $[\![A]\!]_{\phi,x=a}$,

i.e. $\{[\![A]\!]_{\phi,x=a} \in \mathcal{B} \mid a \in \mathcal{M}_s\}$ $\quad (\subseteq \mathcal{B})$

Et c'est à cet ensemble qu'on applique $\hat{\forall}$ ou $\tilde{\exists}$

Fonctions de $\wp^+(\mathcal{B})$ dans $\mathcal{B}$

Pour une proposition A sans variables $[\![A]\!]_\phi$ indépendant de ϕ

La notion de valuation inutile

Pour une proposition A close également

Mais la notion de valuation nécessaire pour les sous-expressions

À quoi sert $\mathcal{B}^+$?

Un langage $\mathcal{L} = (\mathcal{S}, \mathcal{F}, \mathcal{P})$

Un modèle de ce langage est formé de

– pour chaque s, un ensemble non vide $\mathcal{M}_s$

– un ensemble non vide $\mathcal{B}$, un sous-ensemble $\mathcal{B}^+$

– pour chaque f d'arité $(s_1, ..., s_n, s')$, une fonction $\hat{f}$ de $\mathcal{M}_{s_1} \times ... \times \mathcal{M}_{s_n}$ dans $\mathcal{M}_{s'}$

– pour chaque P d'arité $(s_1, ..., s_n)$, une fonction $\hat{P}$ de $\mathcal{M}_{s_1} \times ... \times \mathcal{M}_{s_n}$ dans $\mathcal{B}$

– $\hat{\top}$, $\hat{\bot}$, $\hat{\neg}$, $\hat{\wedge}$ $\hat{\vee}$, $\hat{\Rightarrow}$, $\hat{\forall}$, $\hat{\exists}$

À quoi sert $\mathcal{B}^+$?

Une proposition close A est valide dans un modèle si $[\![A]\!] \in \mathcal{B}^+$

Une proposition A qui a des variables libres $x_1, ..., x_n$ est valide si $\forall x_1 \ ... \ \forall x_n \ A$ est valide

Un séquent $A_1, ..., A_n \vdash B_1, ..., B_m$ est valide si la proposition $(A_1 \wedge ... \wedge A_n) \Rightarrow (B_1 \vee ... \vee B_m)$ est valide

Un cas particulier : les modèles bivalués

$\mathcal{B} = \{0, 1\}$

$\mathcal{B}^+ = \{1\}$

$\hat{\top} = 1, \hat{\bot} = 0, \hat{\neg}, \hat{\wedge}, \hat{\vee}, \hat{\Rightarrow}$ ...

Que sont $\hat{\forall}$ et $\hat{\exists}$?

Désormais : tous les modèles sont bivalués

Un exemple

Langage : une seule sorte, une constante c, deux prédicats unaires P et Q

$\mathcal{M} = \{\pi, e\}$

$\hat{c} = \pi,$

$\hat{P}$ est la fonction qui associe 0 à π et 1 à e

$\hat{Q}$ est la fonction qui associe 1 à π et 1 à e

Est-ce que $P(c)$ est valide ? $Q(c)$? $P(c) \vee Q(c)$? $\forall x\ P(x)$? $\exists x\ P(x)$?
$\forall x\ Q(x)$? $\exists x\ Q(x)$?

Un autre exemple

Langage : une sorte, symbole de fonction binaire $+$, symbole de prédicat binaire $=$

($\mathbb{N}$, addition sur $\mathbb{N}$, égalité sur $\mathbb{N}$) $\forall x \forall y \exists z \, (x + z = y)$ est-elle valide ?

Même question pour $\mathbb{Z}$ muni de l'addition et de l'égalité sur $\mathbb{Z}$?

La proposition $\forall x \forall y \, (x + y = y + x)$ est-elle valide dans ces modèles ? Un modèle dans lequel elle n'est pas valide ?

Quel rapport avec la question du jour :

“comment démontrer qu’une proposition n’est pas démontrable” ?

V. Le théorème de correction et la notion d'indépendance

Le théorème de correction

Si un séquent est démontrable, alors il est valide dans tous les modèles

Le théorème de correction

Simple récurrence sur la structure d'une démonstration

$$\frac{\dfrac{\pi_1}{\Gamma \vdash B} \quad \dfrac{\pi_2}{\Gamma \vdash C}}{\Gamma \vdash B \wedge C}$$

Par hypothèse de récurrence $\Gamma \vdash A$ est valide et $\Gamma \vdash B$ sont valides dans tous les modèles

Soit $A_1, ..., A_n$ les propositions de Γ et $A = A_1 \wedge .... \wedge A_n$

Les propositions $A \Rightarrow B$ et $A \Rightarrow C$ sont valides dans tous les modèles donc

$A \Rightarrow (B \wedge C)$ est valide dans tous les modèles

idem pour les autres règles

Un corollaire

Soit

– $\mathcal{T}$ une théorie et

– $\mathcal{M}$ un modèle dans lequel tous les axiomes de $\mathcal{T}$ sont valides

– A une proposition

Si A est démontrable dans $\mathcal{T}$, alors A est valide dans $\mathcal{M}$

Il existe un sous-ensemble fini Γ de $\mathcal{T}$ tel que $\Gamma \vdash A$ démontrable

$\Gamma \vdash A$ valide dans $\mathcal{M}$ donc A valide dans $\mathcal{M}$

On contrapose

Soit

– $\mathcal{T}$ une théorie et

– $\mathcal{M}$ un modèle dans lequel tous les axiomes de $\mathcal{T}$ sont valides

– A une proposition

Si A n'est pas valide dans $\mathcal{M}$ alors A est n'est pas démontrable dans $\mathcal{T}$

Une méthode pour montrer que A n'est pas démontrable dans $\mathcal{T}$

Trouver un modèle $\mathcal{M}$

dans lequel tous les axiomes de $\mathcal{T}$ sont valides

dans lequel A n'est pas valide

Un exemple

Soit la théorie $\mathcal{T}$ formée de l'axiome $P(c) \vee Q(c)$

Montrer que $P(c)$ n'est pas démontrable dans $\mathcal{T}$

Montrer que $Q(c)$ n'est pas démontrable dans $\mathcal{T}$

La suite

En PC : des exemples de démonstration en théorie des ensembles

La prochaine fois : le théorème de complétude

Questions?