Logique

Pierre Lescanne

29 novembre 2004

Table des matières

Conventions typographiques

- ***nouveau concept ou mot clef***,
- *texte important*
- *formules*,
- règle de réduction,
- disjonction de cas dans une démonstration,
- éléments de la méta-théorie
- auteur

Les mise en formes suivantes ne sont pas destinées à être mémorisées, on se reportera à cette table lorsqu'elle seront rencontrées dans le chapitre corespondant.

Chapitre 1

Introduction

Quels sont les buts de la logique ?
Pour tous
- *Comprendre* la nature intime du raisonnement mathématique[1]
- Faire du «raisonnement» une ***théorie mathématique*** comme les autres.
- Donner un sens précis à ce que peut-être le ***vrai*** dès qu'il s'agit de raisonnement et d'argumentation.

Pour les mathématiciens
- S'assurer (se convaincre ?) que les mathématiques sont exemptes de contradictions et de paradoxes.
- *Apprendre* une branche des mathématiques.

Pour les informaticiens
- *Mécaniser* les processus de raisonnement.
- *Exhiber les liens* entre démonstrations et calculs.
- *Formaliser* les objets informatiques,
  - pour la sûreté (par exemple, la ligne 14 du métro parisien),
  - et le sécurité.

Ce que la logique n'est pas

Point de vue personnel
- Le fondement ultime auquel se réduisent les mathématiques, (point de vue réductionniste)
  Des réductions sont possibles et utiles et la logique peut aider à en faire, mais il n'y pas de réduction ultime.
- La discipline qui va faire remplacer les humains (en général) et les mathématiciens (en particulier) par des machines (point de vue mécaniste).

La logique, une théorie mathématique

La logique est une théorie mathématique[2],
- elle utilise les mathématiques comme le font les autres branches des mathématiques,
- elle *étudie des sortes particulières d'objets mathématiques* : les propositions, les théorèmes, les jugements, les démonstrations, etc.

[1] et du raisonnement non mathématique (philosophique, judiciaire) !
[2] comme les autres !

Un peu d'histoire

L'histoire montre que *tout ce qui est susceptible de se mathématiser se mathématise.*

Au début, seuls les ***entiers*** sont des êtres mathématiques.

Puis les Anciens acceptent les ***rationnels***.

Au début du dix-neuvième siècle, les ***relatifs*** et les ***complexes*** (ou imaginaires) deviennent eux-aussi des êtres mathématiques.

Au dix-neuf siècle

- les ***réels*** (Dedekind),
- puis les ***fonctions*** (en «extension»)
- et les ***ensembles*** (Cantor) deviennent des êtres mathématiques.

Au début du vingtième siècle, les ***fonctions*** (en «intention») (Church et Curry) et les ***théorèmes*** (Boole, Frege etc.) deviennent des êtres mathématiques.

Aujourd'hui, les ***démonstrations*** (Curry, de Bruijn et Howard, 1980) deviennent des êtres mathématiques.[3].

Mécaniser la logique ?

Deux positions s'affrontent.

- *Le mathématicien ne sera jamais battu par une machine* Alain Connes (le triangle de la pensée)
- *Il existe un théorème qui ne peut être prouvé que par un ordinateur* Veroff and McCune : Les algèbres de Boole peuvent être axiomatisées par l'axiome

  Axiome :

  $$((x \mid z) \mid y) \mid ((x \mid (x \mid y)) \mid x) = y$$

  où est $\mid$ est le symbole de Sheffer qui peut être interprété comme

  $$x \mid y = \neg x \wedge \neg y$$

  Est-ce un théorème profond ?

Mécaniser la logique ?

La démonstration complète du ***théorème des quatre couleurs*** vient d'être terminée par George Gonthier (septembre 2004) en utilisant l'assistant de preuve COQ.

La démonstration précédente était hybride:

- *démonstrations* et *vérifications humaines*
- et *utilisation de l'ordinateur* pour d'autres vérifications.

La démontrationde Gonthier est complètement mécanisée.

Mécaniser la logique ?

La démonstration complète de la ***conjecture de Kepler*** a suscité une polémique, car certaines parties n'ont pas pu être vérifiées par des humains.

Un programme de recherche décennal a été initié pour mener à bien une preuve complète assistée par ordinateur.

[3] Nous inisterons sur ce point de vue.

Modèles

Informellement, un ***modèle*** est une structure mathématique dans laquelle toutes les ***règles de déduction*** et les ***axiomes*** sont «***satisfaits***».

On dit qu'une formule est ***valide*** si elle est satisfaite dans tous les modèles.

Les deux niveaux de la logique

En logique, il y a deux niveaux qui interfèrent et qu'il ne faut pas confondre.

- La ***théorie***, (on dit aussi parfois la ***théorie objet***, si l'on veut être plus précis).
- La ***méta-théorie***, c'est une mathématique dans laquelle on va raisonner sur l'objet. C'est aussi un système logique !

Le ***théorie objet*** est l'objet logique que l'on étudie et que l'on souhaite donc formaliser.

En général, on accepte dans la ***méta-théorie*** toute la puissance du raisonnement traditionnel. Si elle est mécanisée, cela peut-être par un système formel plus ou moins puissant.

Dans la méta-théorie, on prouve des ***méta-théorèmes***, c-à-d des théorèmes à propos de la théorie objet.

Quelques méta-théorèmes courants sont :

- la ***correction***,
- la ***cohérence***,
- la ***complétude***.

Les concepts méta-logiques

La ***correction*** est la capacité d'un système de preuve de pouvoir prouver *seulement* des théorèmes qui sont des formules valides.

La ***cohérence*** est la capacité d'un système de preuve d'être *absent de contradiction*, on ne peut pas prouver une propriété et son contraire.

La ***complétude*** est la capacité d'un système de preuve de pouvoir *prouver toutes les formules valides.*

La cohérence

Pour prouver la cohérence, autrement dit l'absence de contradiction, on exhibe un modèle.

Les ingrédients de la logique

Les aspects preuves

En logique on trouve :

- un ***langage*** d'expressions bien formées :
  - les ***propositions*** (construites avec des ***connecteurs***),
  - les ***jugements*** ou ***séquents***
  - etc.

  On dit aussi que c'est la ***syntaxe***.
- des ***règles*** de déduction,
- des ***axiomes***.

Les ***règles de déduction*** montrent comment *construire des théorèmes à partir d'autres théorèmes.* On définit dans la méta-théorie,

- des fonctions des propositions vers les propositions (règles monadiques),

– ou des fonctions des couples de propositions vers les propositions (règles dyadiques).

Les propositions à partir desquelles ont fait la déduction dans la règle s'appelle les ***prémisses***. La proposition que l'on déduit s'appelle la ***conséquence***.

Les ***axiomes*** affirment que *certaines propositions sont des théorèmes* : on définit le prédicat unaire «être un théorème» dans la méta-théorie et on affirme que les axiomes sont des formules qui satisfont ce prédicat.

N. B. Les axiomes sont en général vus comme des règles sans prémisses.

Le but des axiomes et des règles de déduction est de former des expressions particulières, les ***théorèmes*** en construisant des objets mathématiques particuliers les ***démonstrations*** (ou ***preuves***).

Les ***preuves*** sont des ***arbres*** dont

– les ***noeuds*** sont les règles de déduction,
– les ***feuilles*** sont les axiomes
– et la ***racine*** est le théorème dont c'est la preuve.

$$\dfrac{\dfrac{\dfrac{\cdots \quad \cdots}{\cdots}\,(foo_1) \qquad \dfrac{\cdots}{\cdots}\,(bar)}{\cdots \qquad\qquad \cdots}\,(foo_2)}{\cdots \qquad\qquad\qquad\qquad \cdots}\,(foo_1)$$
$$\Gamma \vdash \Delta$$

Il y a différentes sortes d'objets : ***propositions***[4], ***théorèmes***, etc.

Dans une logique, l'appartenance d'un objet à telle ou telle sorte se décrète par un ***jugement***.

Syntaxe concrète et syntaxe abstraite

Un ordinateur a besoin qu'on lui parle de la syntaxe à un bas niveau, c'est la ***syntaxe concrète***, c-à-d les ***virgules***, les ***parenthèses***, les ***retours à la ligne***, etc.

Un humain préfère une syntaxe lisible et flexible, il a besoin de la ***syntaxe abstraite***, c-à-d plutôt la structure arborescente, donc il souhaite des ***opérateurs infixes***, l'***associativité***.

Les aspects modèles

On interprète le langage dans les ***modèles***. On parle aussi de ***sémantique***.

Les propositions qui sont «satisfaites» (dans un sens à préciser) par le modèle sont dites ***valides***.

Correction, cohérence et complétude établissent des liens entre

– les ***théorèmes*** (propositions prouvables)
– et les ***tautologies*** (propositions valides),

c'est-à-dire entre la ***prouvabilité*** et la ***validité***.

Les deux grandes branches de la logique

La partie de la logique où l'on s'intéresse plutôt aux démonstrations s'appelle la la ***théorie de la démonstration*** ou théorie de la preuve (proof theory).

La partie de la logique où l'on s'intéresse plutôt à la validité s'appelle la ***théorie des modèles***.

[4] qui ne sont pas théorèmes

Bibliographie

Deux livres de base :

R. Lalement. *Logique, Réduction, Résolution.* Études et recherches en informatique. Masson, Paris, 1990.

R.David, K.Nour, C.Raffalli *Introduction à la logique - théorie de la démonstration.* Dunod, 2001.

Ma référence :

D. van Dalen. *Logic and Structure.* Springer Verlag, 1994.

Un livre assez complet sur la logique de l'informatique en français :

P. Gochet, P. Gribomont. *Logique. Volume 1 : méthodes pour l'informatique fondamentale*. HERMES, 1990

Sur la logique épistémique :

R. Fagin, Y. Halpern, Y. Moses, and M. Y. Vardi. *Reasoning about Knowledge* The MIT Press, 1995.

Sur la théorie des ensembles

Jean-Louis Krivine *Théorie des ensembles.* Eyrolles. (1998)

Page WEB :
http://perso.ens-lyon.fr/pierre.lescanne/ENSEIGNEMENT/LOGIQUE/presentation.html
ou formation.ens-lyon.fr, groupe cours_informatiques

Le plan du cours

- L'***approche à la Hilbert*** (essentiellement axiomatique),
- La ***déduction naturelle*** (essentiellement à base de règles),
- La ***logique classique*** (une logique moins «calculatoire»),
- Le ***lambda calcul*** («la théorie des fonctions»),
- Les ***modèles*** de la logique intuitionniste,
- Le ***calcul des prédicats*** (une logique avec quantificateurs)
- La ***théorie des ensembles*** (à nouveau une théorie axiomatique),

Une progression plus didactique que linéaire ou logique.

Chapitre 2

Logique propositionnelle à la Hilbert

Les séquents

Le concept de base de la théorie de la démonstration est le ***séquent***.
Un séquent s'écrit $\Gamma \vdash \Delta$ et est constitué de regroupement de propositions.

- Si Γ est vide et Δ ne contient qu'une proposition, c'est l'***approche à la Hilbert***.
- Quand Γ est un multiensemble (une structure de données où l'ordre ne compte pas, mais où les éléments peuvent être répétés) et Δ ne contient qu'une proposition, on a affaire à la ***déduction naturelle***.
- Quand Γ et Δ sont des multiensembles de propositions, on parle de ***calcul des séquents***.
- Si Γ et Δ sont des multiensembles, mais si l'on contrôle très strictement l'emploi des duplications dans les preuves, – une proposition ne sert qu'une fois dans chaque preuve – on parle de ***logique linéaire***.
- Si les propositions déclarent le ***type d'un élément***, on parle de ***jugement de typage***.

2.1 La logique propositionnelle minimale

2.1.1 La syntaxe

La syntaxe

Il n'y a qu'un ***connecteur*** $\Rightarrow$ et des ***variables propositionnelles*** p, q, …, p_1, p_2, …

Exemple.

- p,
- $p \Rightarrow q$,
- $(p \Rightarrow q) \Rightarrow p$.

sont des propositions.

On adopte la convention d'***associativité à droite*** à savoir que

$$p_1 \Rightarrow (p_2 \Rightarrow \cdots \Rightarrow (p_{n-1} \Rightarrow p_n) \dots))$$

s'écrit $$p_1 \Rightarrow p_2 \Rightarrow \cdots \Rightarrow p_{n-1} \Rightarrow p_n$$

Les séquents de logique à la Hilbert

Les séquents sont de la forme $\vdash \varphi$ où φ est une proposition.

Ainsi on *distingue* certaines propositions des autres.

Question : Quelles sont en logique les propositions que l'on veut distinguer des autres ?

Les propositions et les théorèmes

Les propositions sont des formules constituées de variables et de l'opérateur (du connecteur) $\Rightarrow$.

Elles n'ont pas de «contenu» utilisable pour raisonner.

Les théorèmes sont acceptables pour raisonner.

Exemple. $p \Rightarrow q \Rightarrow p$ est un théorème de la logique minimale et on accepte parfaitement le raisonnement Si p alors si q alors p.

Mais toutes les propositions ne sont pas acceptables.

Exemple. $p \Rightarrow p \Rightarrow q$. Va-t-on accepter «Si p alors si p alors q ?».

Les propositions et les théorèmes dans les groupes

Dans les ***groupes***, les propositions sont de la forme $exp \equiv exp'$ où exp et exp' sont formées

- de variables
- du symbole binaire $*$,
- du symbole unaire $^{-1}$
- et de la constante e.

Les ***théorèmes*** sont dérivés à partir des axiomes bien connus des groupes et des règles de remplacement des égaux par des égaux.

$(x * x^{-1}) * y \equiv (y * x^{-1}) * x$ est un ***théorème***.

$(x*x^{-1})*y^{-1} \equiv (y*x)*x$ est une ***proposition*** qui n'est pas un ***théorème***.

Les constituants de la logique propositionnelle à la Hilbert

La ***logique propositionnelle à la Hilbert*** est une logique de presque rien :

- des séquents rudimentaires,
- une règle,
- deux axiomes.

Du coup, elle est difficile d'emploi, il va falloir s'aider d'un logiciel pour la manipuler.

La méta-théorie

Comme méta-théorie, je choisis, un système logique très puissant : le ***Calcul des Constructions Inductifs***, mécanisé dans l'*assistant de preuve* COQ[1].

A la fin du cours, on aura une meilleure idée de ce qu'est le Calcul des Constructions Inductifs

[1] Ces notes de cours vont de paire avec un script en COQ.

Un peu de «méta syntaxe»

$forall\ p, q\ : proposition$ signifie «pour tout p et tout q qui sont des ***propositions***»

$Inductive$ signifie que l'on définit un concept : ***proposition***, ***theorem*** par induction.

Le méta-prédicat theorem

En COQ, le ***méta-prédicat*** $theorem$ appliqué à p se note $(theorem\ p)$.

Mais plus tard, COQ nous permet d'utiliser le symbole de séquent $\vdash p$ qui doit se lire «p est un théorème».

2.1.2 Les axiomes et les règles

Une règle

En logique propositionnelle minimale à la Hilbert, il n'y a qu'une règle : le Modus Ponens :

$$\frac{\vdash p \Rightarrow q \qquad \vdash p}{\vdash q}\ MP$$

Le Modus Ponens

En COQ, MP est une fonction

$$theorem(p \Rightarrow q) \rightarrow theorem\ p \rightarrow theorem\ q$$

qui prend un objet du type $theorem(p \Rightarrow q)$ où $p \Rightarrow q$ est une proposition et un objet du type $theorem\ p$ où p est une proposition et fournit un objet du type $theorem\ q$.

Plus précisément, c'est une fonction qui prend quelque chose du type $p \Rightarrow q$ et rend une fonction qui à quelque chose de type p associe quelque chose de type q. *Mais c'est à peu près la même chose, à une curryfication prés !*

Deux axiomes

Il y a deux axiomes appelés K et S :

Axiome K **:** $\vdash p \Rightarrow q \Rightarrow p$

Axiome S **:** $\vdash (p \Rightarrow q \Rightarrow r) \Rightarrow (p \Rightarrow q) \Rightarrow p \Rightarrow r$

Ne me demandez pas pour l'instant pourquoi ils s'appellent K et S !

Preuve de KI

$$\mathcal{D} = \dfrac{\vdash (p \Rightarrow p) \Rightarrow q \Rightarrow p \Rightarrow p \qquad \dfrac{\mathcal{D}' \qquad \vdash p \Rightarrow p \Rightarrow p}{\vdash p \Rightarrow p}}{\vdash q \Rightarrow p \Rightarrow p}$$

où $\mathcal{D}'$ est

$$\frac{\vdash (p \Rightarrow (p \Rightarrow p) \Rightarrow p) \Rightarrow (p \Rightarrow p \Rightarrow p) \Rightarrow p \Rightarrow p \qquad \vdash p \Rightarrow (p \Rightarrow p) \Rightarrow p}{\vdash (p \Rightarrow p \Rightarrow p) \Rightarrow p \Rightarrow p}$$

$\mathcal{D}$ et $\mathcal{D}'$ sont des ***arbres de preuve.***
$\mathcal{D}$ est l'***arbre de preuve*** ou la ***preuve*** de $q \Rightarrow p \Rightarrow p$.

Exercice
Prouver le lemme

Lemme 2.1. B : $\vdash (p \Rightarrow q) \Rightarrow (r \Rightarrow p) \Rightarrow r \Rightarrow q$

Exercice
Prouver, en utilisant le lemme B, le lemme (la règle dérivée)

Lemme 2.2. L : $\vdash q \Rightarrow r \rightarrow \vdash p \Rightarrow q \rightarrow \vdash p \Rightarrow r.$

La règle Cut
La règle Cut ou ***règle de coupure*** permet d'utiliser des théorèmes intermédiaires (des lemmes !), ici q.

$$\frac{\vdash q \Rightarrow r \qquad \vdash p \Rightarrow q}{\vdash p \Rightarrow r}\ rule\_Cut$$

2.1.3 Les modèles

Le modèle $\{0, 1\}$
Une formule est ***valide classiquement*** si elle prend la valeur 1 pour l'interprétation de $\Rightarrow$ suivante :

$\Rightarrow$	0	1
0	1	1
1	0	1

et quelles que soient les valeurs prises par les variables propositionnelles.

Exercice

1. Montrer que les axiomes $Hilbert_K$ et $Hilbert_S$ sont valides classiquement.
2. Montrer que la règle MP «préserve» les propositions valides classiquement. En déduire que tous les théorèmes sont valides classiquement.
3. Montrer que la ***formule de Pierce*** $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$ est valide classiquement.

Incomplétude
La formule de Pierce n'est pas un théorème de la logique minimale. La logique minimale est ***incomplète*** pour le modèle {0, 1}.
Il faut
– soit changer de logique, ***logique classique***
– soit changer de modèles, ***modèles de Kripke***
On fera les deux ! Par exemple en ajoutant l'axiome de Pierce.

2.2 La logique propositionnelle intuitionniste (approche à la Hilbert)

La syntaxe

Il y a deux nouveaux connecteurs $\wedge$ et $\vee$.

– $\wedge$ et $\vee$ représentent la conjonction et la disjonction.

Les axiomes pour $\wedge$ et $\vee$

$$\begin{array}{rcl} Or0 & : & \vdash (p \Rightarrow r) \Rightarrow (q \Rightarrow r) \Rightarrow (p \vee q) \Rightarrow r \\ Or1 & : & \vdash p \Rightarrow (p \vee q) \\ Or2 & : & \vdash q \Rightarrow (p \vee q) \end{array}$$

Il y a six axiomes :

$$\begin{array}{rcl} And0 & : & \vdash p \Rightarrow q \Rightarrow (p \wedge q) \\ And1 & : & \vdash (p \wedge q) \Rightarrow p \\ And2 & : & \vdash (p \wedge q) \Rightarrow q \end{array}$$

Quelques conséquences

– $\vdash \quad p \vee q \;\Rightarrow\; q \vee p$
– $\vdash \quad p \vee (q \vee r) \;\Rightarrow\; (p \vee q) \vee r$
– $\vdash \quad p \vee p \;\Rightarrow\; p$
– $\vdash \quad (p \Rightarrow q) \;\Rightarrow\; (p \vee r) \;\Rightarrow\; (q \vee r)$
– $\vdash \quad p \wedge q \;\Rightarrow\; q \wedge p$
– $\vdash \quad p \wedge (q \wedge r) \;\Rightarrow\; (p \wedge q) \wedge r$
– $\vdash \quad p \wedge p \;\Rightarrow\; p$
– $\vdash \quad (p \Rightarrow q) \;\Rightarrow\; p \wedge r \;\Rightarrow\; q \wedge r$
– $\vdash \quad (p \wedge q) \vee (p \wedge r) \;\Rightarrow\; p \wedge (q \vee r)$
– $\vdash \quad p \wedge (q \vee r) \;\Rightarrow\; (p \wedge q) \vee (p \wedge r))$
– $\vdash \quad (p \vee q) \wedge (p \vee r) \;\Rightarrow\; p \vee (q \wedge r)$
– $\vdash \quad p \vee (q \wedge r) \;\Rightarrow\; (p \vee q) \wedge (p \vee r)$

Et des règles :

$$\frac{\vdash p \qquad \vdash q}{\vdash p \wedge q} \qquad \frac{\vdash p \Rightarrow q \qquad \vdash p \Rightarrow r}{\vdash p \Rightarrow q \wedge r} \qquad \frac{\vdash p1 \Rightarrow q1 \qquad \vdash p2 \Rightarrow q2}{\vdash p1 \wedge p2 \;\Rightarrow\; q1 \wedge q2}$$

Le connecteur False

Le connecteur $False$ est régi par l'axiome :

Axiome F : $\quad \vdash False \Rightarrow p$

La négation est $\quad \neg p \quad \triangleq \quad p \Rightarrow False$.

Réduire les connecteurs ?

En logique intuitionniste, *on ne peut pas réduire les connecteurs* les uns par rapport aux autres. Chaque connecteur a sa vie propre.

Il faut donc des axiomes spécifiques pour chaque connecteur.

Exercice. Prouver l'assertion précédente. Voir exercice... dans le livre de van Dalen.

La logique intuitionniste et la logique classique

En logique intuitionniste les formules suivantes ne sont pas des théorèmes.

- $\neg\neg p \Rightarrow p$
- $p \vee \neg p$
- $(\neg p \Rightarrow \neg q) \Rightarrow q \Rightarrow p$
- $(p \Rightarrow q) \vee (q \Rightarrow p)$

Le tiers exclus

Le ***tiers exclus*** est la proposition $p \vee \neg p$.

En informatique, considérons la proposition x_vaut_zero à savoir «La variable x vaut zéro»[2].

Sa négation est «La variable x ne vaut pas zero»[3].

A-t-on $x\_vaut\_zero \vee \neg\ x\_vaut\_zero$?

A-t-on une seule manière d'interpréter la négation ?

La logique intuitionniste et les preuves

En logique intuitionniste les preuves sont des *citoyens de première classe*.

Une proposition est un théorème si on peut en exhiber une preuve.

Ainsi

- d'une preuve de $\neg\neg p$ on ne peut pas exhiber une preuve de p.
- on ne peut pas construire une preuve de $p \vee \neg p$, car cet objet est devrait pouvoir être construit à partir d'une preuve de p ou d'une preuve de $\neg p$[4].

C'est comme construire une maison sur un terrain situé à Vaise *ou* à Vénissieux !

Retournons à MP.

En fait, dans

$$\vdash\ p \Rightarrow q \rightarrow\quad \vdash\ p \rightarrow\quad \vdash\ q$$

MP prend une preuve de $p \Rightarrow q$ et retourne une fonction qui prend une preuve de p et retourne une preuve de q.

Donc $\vdash\ p \Rightarrow q$ représente le ***type*** des preuves de $p \Rightarrow q$. Plutôt que l'***ensemble*** des preuves de $p \Rightarrow q$.

[2] On devrait préciser «La variable x vaut *toujours* zéro»

[3] «La variable x ne vaut *jamais* zéro»

[4] qu'on ne possède pas quand on affirme $p \vee \neg p$

Chapitre 3

Déduction naturelle

Les séquents

En ***déduction naturelle***, on raisonne avec des hypothèses.

Au lieu du séquent $\vdash \varphi$, on utilise le séquent $\Gamma \vdash \varphi$ où

- Γ est un ***ensemble de propositions*** appelés l'***antécédent***, qui sont les hypothèses
- On écrit $\Gamma, \varphi \vdash \psi$ au lieu de $\Gamma \cup \{\varphi\} \vdash \psi$et $\vdash \varphi$ quand l'ensemble des hypothèses est vide.
- $\Gamma \vdash \varphi$ se lit
  - «de Γ on déduit φ»
  - ou «Γ ***infère*** φ» ou «Γ ***induit*** φ»
  - ou «sous les hypothèses Γ on a φ».

Les théorèmes

Les ***théorèmes*** sont les séquents de la forme $\vdash \varphi$ qui peuvent être déduits des axiomes et des règles.

On les trouve donc à la ***racine*** d'un ***arbre de preuve***.

3.1 La déduction naturelle pour la logique propositionnelle minimale

L'axiome

Il n'y a qu'un seul axiome :

Axiome :

$$\Gamma, \varphi \vdash \varphi$$

Les règles

Il y a deux règles : ***introduction*** et ***élimination*** :

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \Rightarrow \psi} \Rightarrow I$$

$$\frac{\Gamma \vdash \varphi \Rightarrow \psi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \psi} \Rightarrow E$$

Preuve de Hilbert_K

$$\frac{\dfrac{\varphi, \psi \vdash \varphi}{\varphi \vdash \psi \Rightarrow \varphi} \Rightarrow I}{\vdash \varphi \Rightarrow \psi \Rightarrow \varphi} \Rightarrow I$$

Preuve de *Hilbert_S*

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(\varphi \Rightarrow \psi \Rightarrow \chi), (\varphi \Rightarrow \psi), \varphi \vdash \varphi \Rightarrow \psi \Rightarrow \chi \quad (\varphi \Rightarrow \psi \Rightarrow \chi), (\varphi \Rightarrow \psi), \varphi \vdash \varphi}{(\varphi \Rightarrow \psi \Rightarrow \chi), (\varphi \Rightarrow \psi), \varphi \vdash \psi \Rightarrow \chi} \quad \dfrac{(\varphi \Rightarrow \psi \Rightarrow \chi), (\varphi \Rightarrow \psi), \varphi \vdash \varphi \Rightarrow \psi \quad (\varphi \Rightarrow \psi \Rightarrow \chi), (\varphi \Rightarrow \psi), \varphi \vdash \varphi}{(\varphi \Rightarrow \psi \Rightarrow \chi), (\varphi \Rightarrow \psi), \varphi \vdash \psi}}{(\varphi \Rightarrow \psi \Rightarrow \chi), (\varphi \Rightarrow \psi), \varphi \vdash \chi}}{(\varphi \Rightarrow \psi \Rightarrow \chi), (\varphi \Rightarrow \psi) \vdash \varphi \Rightarrow \chi}}{(\varphi \Rightarrow \psi \Rightarrow \chi) \vdash (\varphi \Rightarrow \psi) \Rightarrow \varphi \Rightarrow \chi}}{(\varphi \Rightarrow \psi \Rightarrow \chi) \Rightarrow (\varphi \Rightarrow \psi) \Rightarrow \varphi \Rightarrow \chi}$$

Preuve de B

$$\dfrac{\dfrac{\dfrac{\dfrac{(\varphi \Rightarrow \psi),\ (\chi \Rightarrow \varphi), \chi \vdash \varphi \Rightarrow \psi \qquad \mathcal{D}}{(\varphi \Rightarrow \psi),\ (\chi \Rightarrow \varphi), \chi \vdash \psi} \Rightarrow E}{(\varphi \Rightarrow \psi),\ (\chi \Rightarrow \varphi) \vdash \chi \Rightarrow \psi}}{(\varphi \Rightarrow \psi) \vdash (\chi \Rightarrow \varphi) \Rightarrow \chi \Rightarrow \psi}}{\vdash (\varphi \Rightarrow \psi) \Rightarrow (\chi \Rightarrow \varphi) \Rightarrow \chi \Rightarrow \psi}$$

où $\mathcal{D}$ est

$$\frac{(\varphi \Rightarrow \psi),\ (\chi \Rightarrow \varphi), \chi \vdash \chi \Rightarrow \varphi \qquad (\varphi \Rightarrow \psi),\ (\chi \Rightarrow \varphi), \chi \vdash \chi}{(\varphi \Rightarrow \psi),\ (\chi \Rightarrow \varphi), \chi \vdash \varphi} \Rightarrow E$$

3.2 La présentation à la Prawitz

La présentation à la Prawitz

Prawitz donne une autre vision de la déduction naturelle.

Dans son approche, on dispose les hypothèses aux feuilles en même temps que les axiomes.

$$\dfrac{\dfrac{\dfrac{h_1 : \varphi_1 \quad \dots}{\dfrac{\dfrac{axiom_1 \quad \dots}{(foo_1)} \quad \dfrac{axiom_2 \quad \dots}{(bar)}}{(foo_2)}} \quad \dfrac{h_2 : \varphi_2 \quad \dots}{(foo_1)}}{\varphi}$$

A certains moments dans une preuve, on supprime une ou des hypothèses au moment d'utiliser une règle.

Par exemple dans $\Rightarrow$I on remplace une proposition ψ par $\varphi \Rightarrow \psi$ et on coche l'hypothèse $h : \varphi$ comme ayant été utilisée.
On dit que l'on a ***déchargé*** l'hypothèse h.

Cela donne $\not{h} : \varphi$.

Une preuve est complète quand toutes les hypothèses ont été déchargées.
L'hypothèse h_1 est barrée parce qu'elle est ***déchargée***.

$$\dfrac{\dfrac{\not{h_1} : \psi \quad \dots}{(foo_1)} \quad \dots}{\dfrac{\dfrac{\dots}{(bar)}}{\dfrac{\dots}{(foo_2)}} \quad \dots}{\dfrac{\dots}{(foo_1)}}$$
$$\dfrac{\varphi}{\psi \Rightarrow \varphi}$$

La preuve de B dans la présentation à la Prawitz

$$\dfrac{\dfrac{\dfrac{\not{h} : \varphi \Rightarrow \psi \qquad \dfrac{\not{h'} : \chi \Rightarrow \varphi \qquad \not{h''} : \chi}{\varphi}}{\psi}\, h''}{\chi \Rightarrow \psi}\, h'}{(\chi \Rightarrow \varphi) \Rightarrow \chi \Rightarrow \psi}\, h$$
$$(\varphi \Rightarrow \psi) \Rightarrow (\chi \Rightarrow \varphi) \Rightarrow \chi \Rightarrow \psi$$

J'ai noté ainsi les hypothèses quand elles sont créées et ainsi quand elles ont été déchargées.
On coche les hypothèses pour s'assurer qu'elles ont bien toutes été déchargées.

3.3 Des preuves à la Hilbert aux preuves en déduction naturelle

Pour passer d'une preuve ***à la Hilbert*** à une preuve en ***déduction naturelle***.

On remplace les invocations de $Hilbert\_K$ et $Hilbert\_S$ par leurs preuves.

Les preuves sont plus longues.

Preuve de $\psi \Rightarrow \varphi \Rightarrow \varphi$

La preuve en déduction naturelle de $\psi \Rightarrow \varphi \Rightarrow \varphi$ est

$$\dfrac{\dfrac{\psi, \varphi \vdash \varphi}{\psi \vdash \varphi \Rightarrow \varphi}}{\vdash \psi \Rightarrow \varphi \Rightarrow \varphi}$$

Alors que la preuve déduite de la preuve à la Hilbert est

$$\dfrac{\dfrac{\dfrac{(\varphi \Rightarrow \varphi), \psi, \varphi \vdash \varphi}{(\varphi \Rightarrow \varphi) \vdash \psi \Rightarrow \varphi \Rightarrow \varphi}}{\vdash (\varphi \Rightarrow \varphi) \Rightarrow \psi \Rightarrow \varphi \Rightarrow \varphi} \qquad \dfrac{\mathcal{D} \qquad \vdash \varphi \Rightarrow \varphi \Rightarrow \varphi}{\vdash \varphi \Rightarrow \varphi}}{\vdash \psi \Rightarrow \varphi \Rightarrow \varphi}$$

où $\mathcal{D}$ est

$$\dfrac{\dfrac{\mathcal{D}'}{\vdash (\varphi \Rightarrow (\varphi \Rightarrow \varphi) \Rightarrow \varphi) \Rightarrow (\varphi \Rightarrow \varphi \Rightarrow \varphi) \Rightarrow \varphi \Rightarrow \varphi} \qquad \dfrac{\dfrac{\varphi, (\varphi \Rightarrow \varphi) \vdash \varphi}{\varphi \vdash (\varphi \Rightarrow \varphi) \Rightarrow \varphi}}{\vdash \varphi \Rightarrow (\varphi \Rightarrow \varphi) \Rightarrow \varphi}}{\vdash (\varphi \Rightarrow \varphi \Rightarrow \varphi) \Rightarrow \varphi \Rightarrow \varphi}$$

et $\mathcal{D}'$ est l'arbre de la preuve de *Hilbert_S* où l'on a substitué les variables de la façon suivante:

$$\begin{array}{lcl} \varphi & := & \varphi \\ \psi & := & \varphi \Rightarrow \varphi \\ \chi & := & \varphi \end{array}$$

Exercice.
1. Dessiner l'arbre complet en déduction naturelle de la démonstration de $\psi \Rightarrow \varphi \Rightarrow \varphi$ déduite de la preuve à la Hilbert.
2. Comparer cette preuve avec la preuve «naturelle».

3.4 La logique propositionnelle

Les règles

Les règles sont deux types :
- ***règles d'introduction*** : un connecteur qui n'était pas présent apparaît dans la proposition conséquente sous la barre d'inférence.
- ***règles d'élimination*** : la proposition conséquente sous la barre d'inférence est construite en enlevant le connecteur principal d'un des connecteurs conséquents d'un séquent au dessus de la barre.

La syntaxe

Il y a trois nouveaux connecteurs $\bot$, $\wedge$ et $\vee$.
- $\bot$ est nullaire et représente l'absurde,
- $\wedge$ et $\vee$ sont bien connus et représentent la conjonction et la disjonction.

L'axiome pour $\bot$

Il n'y a qu'une règle et c'est ***une règle d'élimination :***

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}\ \bot E$$

Les règles du $\wedge$

Il y a une règle d'***introduction*** et deux règles d'***élimination***.

$$\frac{\Gamma \vdash \varphi \qquad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}\ \wedge I$$

$$\frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi}\ \wedge E_g \qquad\qquad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}\ \wedge E_d$$

Les règles du $\vee$

Il y a deux règles d'***introduction*** et une règle d'***élimination.***

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}\ \vee I_g \qquad\qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}\ \vee I_d$$

$$\frac{\Gamma \vdash \varphi \vee \psi \qquad \Gamma, \varphi \vdash \chi \qquad \Gamma, \psi \vdash \chi}{\Gamma \vdash \chi}\ \vee E$$

Un exemple

$$\dfrac{\dfrac{\varphi \vee \psi \vdash \varphi \vee \psi \qquad \dfrac{\dfrac{\varphi \vee \psi, \varphi \vdash \varphi}{\varphi \vee \psi, \varphi \vdash \psi \vee \varphi}\ \vee I_d \qquad \dfrac{\varphi \vee \psi, \psi \vdash \psi}{\varphi \vee \psi, \varphi \vdash \psi \vee \varphi}\ \vee I_g}{\varphi \vee \psi \vdash \psi \vee \varphi}\ \vee E}{\vdash \varphi \vee \psi \Rightarrow \psi \vee \varphi}\ \Rightarrow I$$

Les hypothèses déchargées dans $\vee E$

Dans la règle

$$\frac{\Gamma \vdash \varphi \vee \psi \qquad \Gamma, h_1 : \varphi \vdash \chi \qquad \Gamma, h_2 : \psi \vdash \chi}{\Gamma \vdash \chi}\ \vee E$$

Les hypothèses $h_1 : \varphi$ et $h_2 : \psi$ sont déchargées.

$\vee$ à la Prawitz

L'utilisation de $\vee E$ et des décharges apparaissent mieux sur un exemple.

$$\dfrac{\dfrac{\not{h_1} : (\varphi \vee \psi) \vee \chi \qquad \dfrac{\not{h_2} : \varphi \vee \psi \qquad \dfrac{\not{h_3} : \varphi}{\varphi \vee (\psi \vee \chi)}\ \vee I_g \qquad \dfrac{\dfrac{\not{h_4} : \psi}{\psi \vee \chi}\ \vee I_g}{\varphi \vee (\psi \vee \chi)}\ \vee I_d}{\varphi \vee (\psi \vee \chi)}\ \vee E, h_3 \text{ et } h_4 \qquad \dfrac{\dfrac{\not{h_5} : \chi}{\psi \vee \chi}\ \vee I_d}{\varphi \vee (\psi \vee \chi)}\ \vee I_d}{\varphi \vee (\psi \vee \chi)}\ \vee E, h_2 \text{ et } h_5}{(\varphi \vee \psi) \vee \chi \Rightarrow \varphi \vee (\psi \vee \chi)}\ \Rightarrow I \text{ et } h_1$$

Exercice. Faire la même démonstration en utilisant des séquents.

Chapitre 4

Logique propositionnelle classique

En déduction naturelle

On ajoute la règle dite de ***réduction par l'absurde.***

$$\frac{\Gamma, \neg p \vdash \bot}{\Gamma \vdash p}\ RAA$$

Attention : il ne faut pas confondre cela avec

$$\frac{\Gamma, p \vdash \bot}{\Gamma \vdash \neg p}$$

qui est en fait : $$\frac{\Gamma, p \vdash \bot}{\Gamma \vdash p \Rightarrow \bot}$$

On utilise le symbole $\vdash_{NK}$ si on veut bien préciser qu'il s'agit de la déduction en logique classique.

Exercice

Prouvez

1. $\neg\neg p \Rightarrow p$
2. $p \vee \neg p$
3. $(p \Rightarrow q) \vee (q \Rightarrow p)$

Exercice 1

$$\dfrac{\dfrac{\dfrac{\neg\neg p, \neg p \vdash \neg\neg p \qquad \neg\neg p, \neg p \vdash \neg p}{\neg\neg p, \neg p \vdash \bot}\ \Rightarrow E}{\neg\neg p \vdash p}\ RAA}{\vdash \neg\neg p \Rightarrow p}\ \Rightarrow I$$

Exercice 2

$$\dfrac{\neg(p\vee\neg p)\vdash\neg(p\vee\neg p) \qquad \dfrac{\dfrac{\dfrac{\neg(p\vee\neg p),p\vdash p}{\neg(p\vee\neg p),p\vdash p\vee\neg p}\vee I}{\neg(p\vee\neg p),p\vdash\bot}\Rightarrow E}{\neg(p\vee\neg p)\vdash\neg p}\Rightarrow I}{\neg(p\vee\neg p)\vdash\bot}\vee I\ \Rightarrow E$$
$$\dfrac{\neg(p\vee\neg p)\vdash\bot}{\vdash p\vee\neg p}\,RAA$$

Exercice 3

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg p,p\vdash\neg p}\quad\dfrac{}{\neg p,p\vdash p}}{\neg p,p\vdash\bot}(\Rightarrow E)}{\neg p,p\vdash q}(\bot)}{\neg p\vdash p\Rightarrow q}(\Rightarrow I)}{\neg p\vdash(p\Rightarrow q)\vee(q\Rightarrow p)}(\vee I_g) \qquad \dfrac{\dfrac{\dfrac{}{p,q\vdash p}(\Rightarrow I)}{p\vdash q\Rightarrow p}(\vee I_d)}{p\vdash(p\Rightarrow q)\vee(q\Rightarrow p)}}{\vdash p\vee\neg p}\qquad}{\vdash(p\Rightarrow q)\vee(q\Rightarrow p)}(\vee E)$$

Correction et complétude

Interprétation : une fonction de *proposition* vers $\langle\mathbb{Z}/2\mathbb{Z};0,1,+,\cdot\rangle$,
- le support est $\{0,1\}$,
- les opérations sont la somme et le produit modulo 2.

Les connecteurs sont interprétés ainsi:
- $v(p\Rightarrow q)=1+v(p)+v(p)\cdot v(q)$
- $v(p\vee q)=v(p)+v(q)+v(p)\cdot v(q)$
- $v(p\wedge q)=v(p)\cdot v(q)$
- $v(\bot)=0$

$\Gamma\vDash_{NK}p$ signifie que si $v(q)=1$ pour tout $q\in\Gamma$ alors $v(p)=1$

La logique propositionnelle est ***correcte***, c'est-à-dire $\Gamma\vdash_{NK}p$ implique $\Gamma\vDash_{NK}p$

La logique propositionnelle est ***complète***, c'est-à-dire $\Gamma\vDash_{NK}p$ implique $\Gamma\vdash_{NK}p$

Chapitre 5

Théorie des ensembles

5.1 Le cadre formel et la syntaxe

Les objectifs

Le but est de formaliser la relation d'appartenance $\in$, c'est-à-dire de donner pour cette relation

- un ***langage***,
- des ***règles***
- et surtout dans ce cas des ***axiomes***

de façon à ce que l'on retrouve la ***théorie des ensembles*** dans le sens intuitif qu'on lui connaît.

Il faut *éviter les paradoxes*, qui ont perturbé les mathématiciens du début du 20ème siècle.

Le paradoxe de Richard

> *Le plus petit entier que l'on ne peut pas définir en moins de vingt mots.*

Le paradoxe de Russell

> L'ensemble $\mathcal{E}$ des e tels que $e \notin e$.

En effet, a-t-on $\mathcal{E} \in \mathcal{E}$ ou $\mathcal{E} \notin \mathcal{E}$?

La métathéorie

La métathéorie est le langage des mathématiques[1] avec deux symboles de relations binaires

- L'***égalité*** $=$ avec les propriétés habituelles que l'on suppose complètement axiomatisé par le calcul des prédicats du premier ordre avec égalité[2].
- L'***appartenance*** $\in$ que l'on va axiomatiser.

[1] Plus précisément le calcul des prédicats avec égalités

[2] En particulier, si $a = b$ est prouvable si et seulement si $a = b$ est valide dans $\mathcal{U}$.

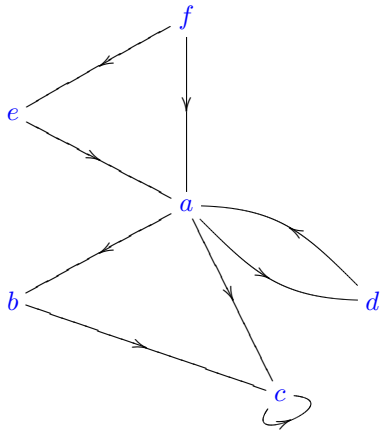
L'univers

On considère la relation $\in$ dans un ensemble $\mathcal{U}$.

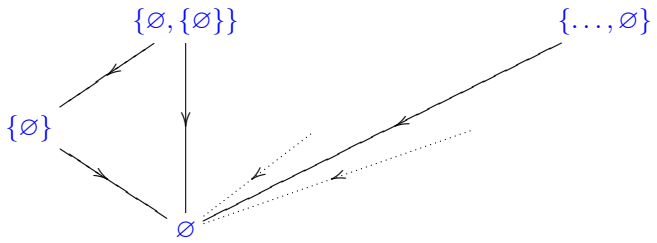
Une question sera de savoir si deux éléments qui appartiennent à $\mathcal{U}$ sont reliés par $\in$.

Des questions possibles,

- Étant donné $a \in \mathcal{U}$ et $b \in \mathcal{U}$, a-t-on $a \in b$?
- Étant donné $a \in \mathcal{U}$ et $b \in \mathcal{U}$, a-t-on $a \notin b$?
- Existe-t-il $a \in \mathcal{U}$ tel que pour tout $b \in \mathcal{U}$ on ait $a \in b$?



Un graphe d'appartenance possible.



Un graphe typique d'appartenance.

Quantificateurs, variables libres et variables liées

Les formules ou énoncés utilisent des quantificateurs $\forall$ et $\exists$.

Si une variable x apparaît dans une expression $\forall x A(x)$ (ou $\exists x A(x)$) on dit qu'elle est ***liée***.

Si une variable x apparaît dans une expression $A(x)$ sans être liée on dit qu'elle est ***libre***.

Si y variable n'apparaît pas libre dans $A(x)$, alors $\forall x A(x)$ et $\forall y A'(y)$ (où $A'(y)$ est obtenu en remplaçant toutes les occurrence de x par y) sont équivalentes.

La théorie et la métathéorie

Il y a deux notions d'ensembles,

- $\mathcal{U}$ et ses sous-ensembles, si un élément a de $\mathcal{U}$ appartient à un des sous-ensembles $\mathcal{V}$ on le note ainsi, $a \in \mathcal{V}$.

– les éléments de $\mathcal{U}$ reliés par la relation $\in$, notée ainsi.
Exemple. Pour $a \in \mathcal{U}$ et $b \in \mathcal{U}$, on peut avoir $a \in b$.
Pour les daltoniens, on a des conventions de vocabulaire.
– $\mathcal{U}$ et ses sous-ensembles sont appelés des ***«collections»***,
– et la relation $\in$ se dit ***«est dans»***.
– Les éléments de $\mathcal{U}$ sont appelés des ***«ensembles»***,
– la relation $\in$ se dit ***«appartient à»***.

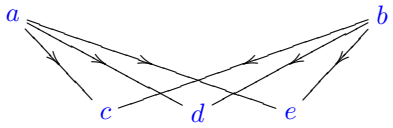
5.2 Les axiomes de Zermelo Fraenkel

L'axiome d'extensionnalité

Axiome d'extensionalité : Il n'existe pas dans $\mathcal{U}$ deux ensembles distincts qui ont les mêmes éléments.

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

On s'interdit le schéma suivant



L'axiome de la paire

Axiome de la paire : Étant donnés deux ensembles a et b, il existe un ensemble c qui contient a et b et eux seulement.

Cet ensemble c est unique d'après l'axiome d'extensionnalité.
L'axiome de la paire est conséquence d'axiomes ultérieurs, mais il est commode de l'énoncer.

$$\forall x \forall y \exists z \forall t [t \in z \Leftrightarrow (t = x \vee t = y)].$$

L'ensemble c dont les seuls éléments sont a et b est noté $\{a, b\}$.
L'axiome de la paire impose qu'il existe un seul ensemble dont le seul élément est a.
Si $a \neq b$ l'ensemble $\{a, b\}$ est appelé une ***paire***.
Si $a = b$ l'ensemble $\{a, b\}$ est appelé un ***singleton***, on le note $\{a\}$.
L'ensemble $\{\{a\}, \{a, b\}\}$ est appelé un ***couple***, on le note plutôt (a, b).

Les uples

Proposition 5.1. *Si* $(a, b) = (a', b')$ *alors* $a = a'$ *et* $b = b'$.

Démonstration. Si $a = b$ alors (a, b) n'a qu'un élément, donc (a', b'), n'a qu'un élément, donc $a' = b'$. $(a, b) = (a', b')$ signifie $\{\{a\}\} = \{\{a'\}\}$.
Si $a \neq b$ alors alors (a, b) a deux éléments, donc (a', b'), a deux éléments, comme $\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}$,

- les singletons sont égaux (soit $\{a\} = \{a'\}$)
- et les paires sont égales $\{a, b\} = \{a', b'\}$ (soit $b = b'$, puisqu'on sait déjà que $a = a'$). ■

Définition. Un ***triplet*** (a, b, c) est l'ensemble $(a, (b, c))$.

Définition. Un ***quadruplet*** (a, b, c, d) est l'ensemble $(a, (b, c, d))$.

Définition. Un n***-uplet*** $(a_1, \ldots, a_n)$ est défini par récurrence comme l'ensemble $(a_1, (a_2, \ldots, a_n))$.

Proposition 5.2. *Si* $(a, b, c) = (a', b', c')$ *alors* $a = a'$, $b = b'$ *et* $c = c'$.

Proposition 5.3. *Si* $(a_1, \ldots, a_n) = (a'_1, \ldots, a'_n)$ *alors* $a_1 = a'_1$, …, $a_n = a'_n$.

L'axiome de la somme ou de la réunion

Axiome de la réunion : Étant donné un ensemble x, il existe un ensemble dont les éléments sont les éléments des éléments x.

$$\forall x \exists u \forall z [\exists y (z \in y \wedge y \in x) \Leftrightarrow z \in u].$$

Cet ensemble est unique, on l'appelle la ***réunion*** des éléments de x et on le note :

$$\cup x \qquad \text{ou} \qquad \bigcup_{y \in x} y.$$

La réunion des éléments de $\{a, b\}$ s'appelle la ***réunion de*** a ***et de*** b on la note $a \cup b$.

Si a, b et c sont trois ensembles, il existe un ensemble dont les éléments sont a, b et c et eux seulement. C'est la réunion des éléments de $\{\{a, b\}, \{c\}\}$.

Par extensionalité, $\{a, b\} \cup \{c\}$ est unique et égale à $\{a\} \cup \{b, c\}$ et à $\{a, c\} \cup \{b\}$,

- on le note $\{a, b, c\}$
- et on l'appelle parfois un ***trio***.

En général, si on a un nombre fini d'ensembles a_1,…, a_n, il existe un ensemble et un seul noté $\{a_1, \ldots, a_n\}$ qui a comme éléments $a_1, \ldots, a_n$ et eux seulement.

L'axiome de l'ensemble des parties

L'énoncé $\forall x (x \in a \Rightarrow x \in b)$ se note $a \subseteq b$ et se lit «a ***est contenu dans*** b».

Axiome de l'ensemble des parties : Pour tout ensemble x il existe un ensemble y dont les éléments sont les ensembles qui sont contenus dans x.

$$\forall x \exists y \forall z [z \subseteq x \Leftrightarrow z \in y].$$

Il n'y a qu'un seul ensemble qui a cette propriété, on le note $\mathcal{P}(x)$.

Définir des relations

Comment peut-on définir des relations entre les éléments de $\mathcal{U}$?

On a déjà deux relations de base $\in$ et $=$.

Si on a défini une relation $n+1$-aire $R(x_1, \ldots, x_n, x_{n+1})$ et si a est un objet de $\mathcal{U}$, on a une relation n-aire $R(x_1, \ldots, x_n, a)$ qui est satisfaite par les objets b_1, ..., b_n si est seulement si $R(b_1, \ldots, b_n, a)$ est satisfaite.

Si on a défini une relation $n+1$-aire $R(x_1, \ldots, x_n, x_{n+1})$, on a une relation n-aire $R(x_1, \ldots, x_n, x_n)$ qui est satisfaite par les objets b_1, ..., b_n si est seulement si $R(b_1, \ldots, b_n, b_n)$ est satisfaite.

Si on a défini une relation n-aire $R(x_1, \ldots, x_n)$, alors on définit la relation $\neg R(x_1, \ldots, x_n)$, qui est satisfaite par les objets b_1, ..., b_n si et seulement si $R(b_1, \ldots, b_n)$ n'est pas satisfaite.

Si on a défini des relations l'une m-aire $R(x_1, \ldots, x_m)$ et l'autre n-aire $S(y_1, \ldots, y_n)$, alors on définit la relation $R(x_1, \ldots, x_m) \vee S(y_1, \ldots, y_n)$ qui est satisfaite par les objets a_1, ..., a_m et b_1, ..., b_n si et seulement si $R(a_1, \ldots, a_m)$ ou $S(b_1, \ldots, b_n)$ satisfaite.

Si on a défini une relation $n+1$-aire $R(x_1, \ldots, x_n, x_{n+1})$, on a une relation n-aire $\exists x R(x_1, \ldots, x_n, y)$ qui est satisfaite par les objets b_1, ..., b_n si est seulement si il existe un objet a tel que $R(b_1, \ldots, b_n, a)$ soit satisfaite. Une relation $R(x)$ à un argument est appelée une ***collection***.

Énoncés

Les relations qui sont construites à partir des deux relations binaires $\in$ et $=$ au moyen des règles ci-dessus sont ce qu'on appelle des ***énoncés***.

Ils sont constitués

- à la base par les symboles $\in$, $=$, $\neg$ $\vee$, $\exists$, des variables, et des objets de l'univers,
- associés entre eux pour fabriquer des énoncés composés par les règles que l'on vient de définir.

Les objets de l'univers qui interviennent dans un énoncé sont appelés ses ***paramètres***.

Relations fonctionnelles

Une relation $n+1$-aire $R(x_1, \ldots, x_n, x_{n+1})$ est une ***relation fonctionnelle à n arguments*** si on a

$$\forall x_1 \ldots \forall x_n \forall y \forall y' [R(x_1, \ldots, x_n, y) \wedge R(x_1, \ldots, x_n, y') \Rightarrow y = y'].$$

La relation $\exists y R(x_1, \ldots, x_n, y)$ est appelée le ***domaine*** de la relation fonctionnelle R.

La relation $\exists x_1 \ldots \exists x_n R(x_1, \ldots, x_n, y)$ est appelée l'***image*** de la relation fonctionnelle R.

Schéma d'axiome de substitution ou de remplacement

Axiomes de substitution : Soit $E(x, y, a_1, \ldots, a_k)$ un énoncé dont les paramètres sont $a_1, \ldots, a_k$ qui définit une relation fonctionnelle f à un argument ; soit a un ensemble quelconque.

Il existe un ensemble b dont les éléments sont exactement les images par f des éléments de a qui se trouvent dans le domaine de f.

Le ***schéma de substitution*** consiste en la liste infinie des énoncés suivants :

$$\forall x_1 \dots \forall x_k \Big(\forall x \forall y \forall y' ((E(x,y,x_1,\dots,x_k) \wedge E(x,y',x_1,\dots,x_k) \Rightarrow y = y') \Rightarrow \forall t \exists u \forall y [y \in u \Leftrightarrow \exists x (x \in t \wedge E(x,y,x_1,\dots,x_k))])\Big)$$

où $E(x,y,x_1,\dots,x_k)$ est n'importe quel énoncé sans paramètre qui a au moins deux variables libres x et y.

Schéma de compréhension

Axiomes de compréhension : Soient a un ensemble et $A(x,a_1,\dots,a_n)$ un énoncé à une variable libre dont les paramètres sont a_1,..., a_n ; alors il existe un ensemble b dont les éléments sont ceux de b qui satisfont l'énoncé A.

Le ***schéma de compréhension*** consiste donc en une liste infinie d'énoncés :

$$\forall x_1 \dots \forall x_k \ \forall x \exists y \forall z \Big[z \in y \Leftrightarrow \big(z \in x \wedge A(z,x_1,\dots,x_k)\big)\Big]$$

dans laquelle $A(x,x_1,\dots,x_n)$ est n'importe quel énoncé sans variables qui a au moins une variable libre x.

Le schéma de compréhension est un cas particulier du schéma de substitution dans le cas où $E(x,y,x_1,\dots,x_k)$ est «$y = x \wedge A(x,x_1,\dots,x_k)$» qui définit bien une relation fonctionnelle à un argument dont le domaine est la collection $A(x,x_1,\dots,x_k)$.

D'après le schéma de substitution il existe bien un ensemble b formé des éléments de a qui sont dans la collection $A(x,x_1,\dots,x_k)$.

On utilise la notation $\{x \in a \mid A(x,a_1,\dots,a_k)\}$ pour représenter l'ensemble b.

L'existence de l'ensemble vide

Proposition 5.4. *Il existe un ensemble et un seul qui n'a aucun élément.*

Démonstration. Soit a un ensemble quelconque. On applique le schéma de compréhension à a et à l'énoncé «$x \neq x$».

L'unicité est une conséquence de l'axiome d'extensionnalité. ■

L'ensemble qui n'a aucun élément est appelé l'***ensemble vide*** et on le note $\varnothing$.

L'axiome de la paire comme conséquence

En exercice.

Construire une paire «de référence» et une relation fonctionnelle injective de cette paire vers deux éléments a et b.

Les naturels

On peut représenter les naturels dans les ensembles[3].

$$\begin{aligned} 0 &\triangleq \varnothing \\ 1 &\triangleq \{\varnothing\} \\ 2 &\triangleq \{\varnothing, \{\varnothing\}\} \\ &\vdots \\ n+1 &\triangleq n \cup \{n\} \end{aligned}$$

L'axiome de l'infini

Axiome de l'infini : La collection des naturels correspond à un ensemble.

Les axiomes de Zermelo Fraenkel

- L'axiome d'extensionnalité,
- l'axiome de la somme ou axiome de la réunion,
- l'axiome de l'ensemble des parties,
- l'axiome de l'infini
- et le schéma d'axiomes de substitution

forment la ***théorie des ensembles de Zermelo-Frænkel***, en abrégé ZF.

Collections et ensembles

Une collection correspond à un ensemble si il existe un ensemble a tel que

$$\forall x[x \in a \Leftrightarrow A(x)]$$

Il y a des collections qui ne correspondent à aucun ensemble.

Exemple. La collection $x \notin x$.

En effet s'il existait a tel que $\forall x[x \in a \Leftrightarrow x \notin x]$ alors en particulier $a \in a \Leftrightarrow a \notin a$

La collection $x = x$ (c'est-à-dire l'univers $\mathcal{U}$) ne correspond pas non plus à un ensemble.

S'il existait, un ensemble a tel que $\forall x(x \in a)$, d'après le schéma de compréhension, il existerait un ensemble a tel que

$$\forall x(x \in b \Leftrightarrow x \in a \wedge x \notin x)$$

et donc $\forall x[x \in b \Leftrightarrow x \notin x]$ autrement dit $x \notin x$ correspondrait à un ensemble.

Produit de deux ensembles

Soit a et b deux ensembles et X la collection des couples (x, y) tels que $x \in a$ et $x \in b$.

Exercice. Donner la définition formelle complète de cette collection.

D'après le schéma de compréhension, la collection X est un ensemble car elle équivaut à $X(z) \ \wedge z \in \mathcal{P}(\mathcal{P}(a \cup b))$.

Cet ensemble est le ***produit*** de a et b et est noté $a \times b$.

[3] $\triangleq$ est le symbole «est égal par définition à»

Application d'un ensemble dans un ensemble

Soit a et b deux ensembles.

L'énoncé «f est une application de a dans b»

$$f \subseteq a \times b \ \wedge \ \forall x \forall y \forall y' [(x,y) \in : f \ \wedge \ (x,y') \in f \Rightarrow y = y'] \\ \wedge \forall x [x \in a \Rightarrow \exists y ((x,y) \in f)].$$

La collection A des applications de a dans b est un ensemble.

En effet, une application de a dans b appartient à $\mathcal{P}(a \times b)$ donc $A(f)$ équivaut à $A(f) \wedge f \in \mathcal{P}(a \times b)$.

C'est un ensemble d'après le schéma de compréhension.

On note cet ensemble b^a.

Réunion d'une famille d'ensembles

Soit a_i une famille d'ensembles indexée par un ensemble I.

On la note $(a_i)_{i \in I}$.

C'est une fonction a de domaine I.

La ***réunion*** de $(a_i)_{i \in I}$ notée $\bigcup_{i \in I} a_i$ est la réunion des éléments de l'image de a. C'est un ensemble et on a

$$\forall x [x \in \bigcup_{i \in I} a_i \Leftrightarrow \exists i (i \in I \wedge x \in a_i)]$$

Intersection d'une famille d'ensembles

L'***intersection*** de la famille $(a_i)_{i \in I}$ est la collection définie par $X(x) : \forall i (i \in I \Rightarrow x \in a_i)$.

Si $I = \varnothing$, X est la collection de tous les ensembles et n'est pas un ensemble.

Si $I \neq \varnothing$ on prend $i_0 \in I$.

Alors $X(x)$ est $x \in a_{i_0} \ \wedge \ \forall i (i \in I \Rightarrow x \in a_i)$.

D'après le schéma de compréhension cette collection est alors un ensemble et on la note $\bigcap_{i \in I} a_i$.

Produit d'une famille d'ensembles

Soit X la collection des applications f de I dans $\bigcup_{i \in I} a_i$ telle que $\forall i (i \in I \Rightarrow f(i) \in a_i)$.

Une telle application est un élément de l'ensemble $(\bigcup_{i \in I} a_i)^I$.

$X(f)$ est équivalent à $X(f) \ \wedge \ f \in (\bigcup_{i \in I} a_i)^I$

La collection $X(f)$ est donc un ensemble d'après le schéma de compréhension.

Cet ensemble est le ***produit*** de la famille $(a_i)_{i \in I}$ et est noté $\Pi_{i \in I} a_i$.

L'axiome du choix

Axiome du choix : Pour chaque ensemble a dont les éléments sont non vides et disjoints deux à deux, il existe un ensemble dont l'intersection avec chaque élément de a est un singleton.

$$\forall a \Big\{ \big[\forall x (x \in a \Rightarrow x \neq \varnothing) \ \wedge \ \forall x y (x \in a \wedge y \in a \ \Rightarrow \ x = y \vee x \cap y = \varnothing) \big] \\ \Rightarrow \exists b \forall x \exists u (x \in a \Rightarrow b \cap x = \{u\}) \Big\}.$$

L'axiome du choix : deux énoncés équivalents

Axiome du choix (énoncé 1) : Tout ensemble a, il existe une application h de l'ensemble des parties non vides de a dans a, telle que $h(x) \in x$ pour toute partie x non vide a.

Une telle fonction est appelée ***fonction de choix*** sur l'ensemble a.

Axiome du choix (énoncé 2) : Le produit d'une famille d'ensembles non vides est non vide.

Ensembles bien ordonnés

Un ensemble et dit ***bien ordonné*** par $\sqsubseteq$, si tous ses sous-ensembles non vides possèdent un plus petit élément pour $\sqsubseteq$.

La proposition suivante est logiquement équivalente à l'axiome du choix.

Lemme 5.5 (Zermelo). *Sur tout ensemble on peut définir un bon ordre.*

La proposition suivante est logiquement équivalente à l'axiome du choix.

Lemme 5.6 (Zorn). *Soit u un ensemble ordonné dont toute partie bien ordonnée est majorée. Alors u admet un élément maximal*[4].

[4] ***maximal*** par ***maximum***.

Chapitre 6

Lambda calcul

6.1 Introduction

> **lambda :** *adj. fam.* : moyen, quelconque. *téléspectateur lambda.*
>
> *Dictionnaire le Robert*

Les fonctions comme citoyens de première classe

On peut faire que les ***preuves*** soient citoyens de première classe, mais pourquoi pas les ***fonctions*** ?

Quelques dates

autour de 1870 un Italien[1] s'oppose à Cantor sur le point de savoir quel est le concept de base des mathématiques prétendant que ça devrait être les fonctions.

1920 Schönfinkel initie la logique combinatoire,

1925 Haskell Curry crée la logique combinatoire,

1936 Alonso Church crée le λ-calcul,

1970-... Explosion du λ-calcul due à l'informatique (Barendregt, Berry, Boehm, de Bruijn, Curien, Dezani-Ciancaglini, Girard, Hindley, Klop, Krivine, Levy, Milner, Plotkin, Scott, Statmann etc.)

Des notations différentes, un même concept

en maths	$x \mapsto x$	$f \mapsto (x \mapsto f(f(x)))$
en CAML	`fun x -> x`	`fun f -> (fun x -> (f (f x)))`
en λ-calcul	$\lambda x.x$	$\lambda f.(\lambda x.(f(fx)))$

La syntaxe

La classe Λ est la plus petite classe qui contient

1. x si x est une variable,
2. $\lambda x.M$ si $M \in \Lambda$, ***abstraction***
3. (MN) si $M \in \Lambda$ et $N \in \Lambda$. ***application***

[1] dont j'ai oublié le nom.

Qu'y a-t-il derrière la syntaxe ?

On peut voir les termes comme des abstractions des fonctions ou des programmes fonctionnels.

Dans $\lambda x.M$, on dit que M est le ***corps*** de la fonction ou du programme.

Dans (MN), on peut voir M comme une fonction que l'on ***applique*** au paramètre N. La ***valeur*** va s'obtenir par «réduction» (approche intentionnelle).

Le lambda-calcul décrit les fonctions par leur ***comportement***.

L'anecdote derrière la syntaxe ?

Au début Church voulait écrire $\hat{\mathtt{x}}$.

Mais au temps des machines à écrire on ne savait écrire que `^x`.

Ce qui a donné $\wedge$`x`, puis λx.

Exemples de termes

Exemples. $I \equiv \lambda x.x$
$K \equiv \lambda x(\lambda y.x)$
$S \equiv \lambda x.(\lambda y.(\lambda z.((xz)(yz))))$
$B \equiv \lambda x.(\lambda y.(\lambda z.(x(yz))))$

Convention

1. Au lieu de $\lambda x_1(\dots(\lambda x_n.M)\dots)$ on écrit $\lambda x_1 \dots x_n.M$.
   Exemple. $\lambda xy.x$.
2. Au lieu de $(\dots(MN_1)\dots N_p)$ on écrit $MN_1 \dots N_p$ ou $M\vec{N}$, si $\vec{N} = (N_1 \dots N_p)$.
   Exemple. $\lambda xyz.xz(yz)$ à la place de $\lambda x.(\lambda y.(\lambda z.((xz)(yz))))$.

Exemples. $((\lambda x.x)y)y$ donne $(\lambda x.x)yy$, «La fonction identité appliquée à y, puis le résultat est appliqué à y».

En revanche, $\lambda x.xyy$ correspond à $\lambda x.(xy)y$. «La fonction qui à x fait correspondre le résultat de x appliqué à y puis à y».

Les mêmes termes avec conventions

$I \equiv \lambda x.x$	I est la fonction identité
$K \equiv \lambda xy.x$	Kc est la fonction constante c
$S \equiv \lambda xyz.xz(yz)$	$Sabc$ distribue c
$B \equiv \lambda xyz.x(yz)$	B permute l'effet des parenthèses

6.1.1 Variables et substitutions

Les variables liées

$$\begin{aligned} BV(x) &= \varnothing \\ BV(\lambda x.M) &= BV(M) \cup \{x\} \\ BV(MN) &= BV(M) \cup BV(N) \end{aligned}$$

Exemple.

$$\begin{aligned} BV(\lambda x.x) &= \{x\} \\ BV(\lambda fx.f(fx)) &= \{f, x\} \\ BV(\lambda fx.f(fxy)y) &= \{f, x\} \end{aligned}$$

Les variables libres

$$\begin{array}{rcl} FV(x) & = & \{x\} \\ FV(\lambda x.M) & = & FV(M) - \{x\} \\ FV(MN) & = & FV(M) \cup FV(N) \end{array}$$

Exemple.

$$\begin{array}{rcl} FV(\lambda x.x) & = & \varnothing \\ FV(\lambda fx.f(fx)) & = & \varnothing \\ FV(\lambda fx.f(fxy)y) & = & \{y\} \\ FV(\lambda x.f(fx)) & = & \{f\} \end{array}$$

Un terme qui n'a pas de variable libre est dit ***clos*** ou ***fermé*** ou est appelé un ***combinateur***.

attention ! Une variable peut être *à la fois libre et liée* dans un terme.

Exemple. $x(\lambda x.x)$.

Le produit cartésien et la curryfication

Il n'y a pas de produit cartésien dans le λ-calcul simple.

Si on veut écrire :

$$\lambda(x,y).f(x,y) \quad \text{ou} \quad (x,y) \mapsto f(x,y)$$

on le remplace par

$$\lambda xy.fxy$$

C'est la ***curryfication*** (nommée après Haskell Curry).

Substitution

Substituer une variable par un terme ne consiste pas simplement à remplacer toutes les occurrences de la variable par ce terme, à cause du phénomène de ***capture***.

Quand on écrit $M[x := P]$ on ne remplace pas simplement les occurrences de x dans M par P.

Ainsi

$$\begin{array}{rcl} x(\lambda x.x)[x := y] & \neq & y(\lambda x.y) \\ (\lambda y.x)[x := y] & \neq & \lambda y.y \end{array}$$

donc il faut être prudent.

Substitution avec renommage

1. $x[x := P] = P$
2. $y[x := P] = y$
3. $(\lambda x.M)[x := P] = \lambda x.M$
4. $(\lambda y.M)[x := P] = \lambda y.(M[x := P])$ si $x \notin FV(M)$ ou $y \notin FV(P)$
5. $(\lambda y.M)[x := P] = \lambda z.(M[y := z][x := P])$ si $x \in FV(M)$ et $y \in FV(P)$ et z est une *nouvelle* variable
6. $(M_1 M_2)[x := P] = M_1[x := P]M_2[x := P]$

La convention de Barendregt

C'est une *convention sur les variables libres* d'un terme *dans un énoncé mathématique*.

Il n'existe aucun sous-terme dans lequel une variable apparaît à la fois libre et liée.

L'α-conversion (règles structurelles)

$$\lambda x.N \equiv_\alpha \lambda y.(N[x := y]) \qquad \text{si } y \notin FV(N) \qquad base$$

$$\frac{M_1 \equiv_\alpha N_1 \qquad M_2 \equiv_\alpha N_2}{M_1 M_2 \equiv_\alpha N_1 N_2}\ \alpha APP$$

$$\frac{M \equiv_\alpha N}{\lambda z.M \equiv_\alpha \lambda z.N}\ \alpha ABS$$

$$x \equiv_\alpha x \quad \alpha var$$

Réflexivité de l'α-conversion

Lemme 6.1. *Pour tout $M \in \Lambda$, on a $M \equiv_\alpha M$.*

Démonstration. Par induction structurelle sur M.

- M est la variable x. Dans ce cas on applique l'axiome αVar.
- M est une application $M_1 M_2$. Alors par induction on a $M_1 \equiv_\alpha M_1$ et $M_2 \equiv_\alpha M_2$ donc on peut appliquer la règle αAPP pour obtenir $M_1 M_2 \equiv_\alpha M_1 M_2$.
- M est une abstraction $\lambda x.P$. Par induction $P \equiv_\alpha P$. Donc par la règle αABS on a $\lambda x.P \equiv_\alpha \lambda x.P$.

■

L'α-conversion (règles de congruence)

$$\frac{M \equiv_\alpha N}{N \equiv_\alpha M}\ \alpha symétrie$$

$$\frac{M \equiv_\alpha N \qquad N \equiv_\alpha P}{M \equiv_\alpha P}\ \alpha transitivité$$

L'α-conversion est une ***relation d'équivalence***, stable par passage au contexte, on dit que c'est une ***congruence***.

α-conversion et convention de Barendregt

L'α-conversion ne change pas la «signification» des termes.

- On suppose que dans tout théorème que l'on énonce, on suit la convention de Barendregt.
- Si l'on a un terme qui ne satisfait pas la convention de Barendregt, on s'y ramène par α-conversion

Substitution et convention de Barendregt

Avec la convention de Barendregt, la définition des substitutions devient beaucoup plus simple.

- $x[x := P] = P$
- $y[x := P] = y$
- $(\lambda y.M)[x := P] = \lambda y.M[x := P]$
- $(M_1 M_2)[x := P] = M_1[x := P]M_2[x := P]$

6.1.2 La β-réduction et les autres réductions

La β-contraction

Les fonctions sont faites pour calculer !

Les réductions d'un terme représentent son calcul.

La β-***contraction*** en est l'étape élémentaire.

$$(\lambda x.M)P \xrightarrow[\beta]{} M[x := P]$$

bêta : *Subst. masc.* : Personne peu intelligente.

Le Trésor de la Langue française informatisé

R-contraction

On se donne un ensemble R de règles, c-à-d de paires de termes, par exemple β.

$M \xrightarrow[R]{} N$ signifie que

- M se contracte en N par R,
- ou M se réduit à N par R en une étape.

$$\frac{(M,N) \in R}{M \xrightarrow[R]{} N}\ \textit{(contraction)} \qquad \frac{M \xrightarrow[R]{} N}{\lambda x M \xrightarrow[R]{} \lambda x N}\ (\xi)$$

$$\frac{M \xrightarrow[R]{} N}{MP \xrightarrow[R]{} NP}\ \textit{(congruence gauche)}$$

$$\frac{M \xrightarrow[R]{} N}{PM \xrightarrow[R]{} PN}\ \textit{(congruence droite)}$$

$\xrightarrow[R]{}$ est alors appelée une ***contraction***.

Exercice

Réduire

- $\lambda y.(\lambda x.x)z$
- $(\lambda fx.f(fx))(\lambda x.x)$
- $(\lambda fx.f(fx))(\lambda fx.fx)$

D'autres exemples de contraction

La contraction β_v ou ***appel par valeur***
Pour toute ***abstraction*** ou toute ***variable*** $P \in \Lambda$

$$(\lambda x.M)\, P \quad \xrightarrow[\beta_v]{} \quad M[x := P]$$

La ***contraction*** η
Pour tout $M \in \Lambda$ et $x \notin FV(M)$,

$$\lambda x.Mx \quad \xrightarrow[\eta]{} \quad M.$$

L'***expansion*** η
Pour tout $M \in \Lambda$ et $x \notin FV(M)$,

$$M \quad \xrightarrow[\eta_{exp}]{} \quad \lambda x.Mx.$$

La ***contraction par*** β ***et*** η

$$\xrightarrow[\beta\eta]{} \quad = \quad \xrightarrow[\beta]{} \cup \xrightarrow[\eta]{} .$$

On s'intéresse à la $\beta\eta$***-réduction*** $\xrightarrow[\beta\eta]{}\!\!\!\!\!\rightarrow$ qui est la fermeture transitive et réflexive de $\xrightarrow[\beta\eta]{}$.

Fermeture transitive et réflexive

$$\frac{M \xrightarrow[R]{} N}{M \xrightarrow[R]{}\!\!\!\!\!\rightarrow N}\ \textit{(cas de base)} \qquad \frac{}{M \xrightarrow[R]{}\!\!\!\!\!\rightarrow M}\ \textit{(réflexivité)}$$

$$\frac{M \xrightarrow[R]{}\!\!\!\!\!\rightarrow N \qquad N \xrightarrow[R]{}\!\!\!\!\!\rightarrow L}{M \xrightarrow[R]{}\!\!\!\!\!\rightarrow L}\ \textit{(transitivité)}$$

Proposition 6.2. *Préservation de* $\xrightarrow[\beta]{}\!\!\!\!\!\rightarrow$ *par abstraction et application.*

$$\frac{M \xrightarrow[\beta]{}\!\!\!\!\!\rightarrow N}{\lambda x.M \xrightarrow[\beta]{}\!\!\!\!\!\rightarrow \lambda x.N}$$

$$\frac{M \xrightarrow[\beta]{}\!\!\!\!\!\rightarrow N \qquad P \xrightarrow[\beta]{}\!\!\!\!\!\rightarrow Q}{MP \xrightarrow[\beta]{}\!\!\!\!\!\rightarrow NQ}$$

Preuve

Cas $\dfrac{M \underset{\beta}{\longrightarrow\!\!\!\!\!\rightarrow} N}{\lambda x.M \underset{\beta}{\longrightarrow\!\!\!\!\!\rightarrow} \lambda x.N}$

On doit montrer que
- sous l'***hypothèse*** $M \underset{\beta}{\longrightarrow\!\!\!\!\!\rightarrow} N$
- on a la ***conclusion*** $\lambda x.M \underset{\beta}{\longrightarrow\!\!\!\!\!\rightarrow} \lambda x.N$.

La démonstration est par ***induction*** sur la taille de l'arbre de preuve de $M \underset{\beta}{\longrightarrow\!\!\!\!\!\rightarrow} N$.

Elle utilise les règles de la définition de $\underset{\beta}{\longrightarrow\!\!\!\!\!\rightarrow}$ et celle de $\underset{\beta}{\longrightarrow}$.

Trois cas se présentent :

1. $M \underset{\beta}{\longrightarrow} N$, on a utilisé le «cas de base», alors par (ξ), $\lambda x.M \underset{\beta}{\longrightarrow} \lambda x.N$ et on conclut par le «cas de base».
2. $M \equiv N$, alors $\lambda x.M \equiv \lambda x.N$ et conclut par «réflexivité».
3. Il existe P tel que $M \underset{\beta}{\longrightarrow\!\!\!\!\!\rightarrow} P$ et $P \underset{\beta}{\longrightarrow\!\!\!\!\!\rightarrow} N$. Par induction, on tire,
   - $\lambda x.M \underset{\beta}{\longrightarrow\!\!\!\!\!\rightarrow} \lambda x.P$
   - et $\lambda x.P \underset{\beta}{\longrightarrow\!\!\!\!\!\rightarrow} \lambda x.N$,

   et par «transitivité» $\lambda x.M \underset{\beta}{\longrightarrow\!\!\!\!\!\rightarrow} \lambda x.N$.

Fermeture transitive, réflexive et symétrique

Avec les règles

$$\frac{M \underset{R}{\longrightarrow} N}{M \underset{R}{\longleftrightarrow\!\!\!\!\!\rightarrow} N}\ \textit{(cas de base)} \qquad \frac{}{M \underset{R}{\longleftrightarrow\!\!\!\!\!\rightarrow} M}\ \textit{(réflexivité)}$$

$$\frac{M \underset{R}{\longleftrightarrow\!\!\!\!\!\rightarrow} N \qquad N \underset{R}{\longleftrightarrow\!\!\!\!\!\rightarrow} L}{M \underset{R}{\longleftrightarrow\!\!\!\!\!\rightarrow} L}\ \textit{(transitivité)} \qquad \frac{M \underset{R}{\longleftrightarrow\!\!\!\!\!\rightarrow} N}{N \underset{R}{\longleftrightarrow\!\!\!\!\!\rightarrow} M}\ \textit{(symétrie)}$$

on obtient la fermeture transitive, réflexive et symétrique de $\underset{R}{\longrightarrow}$ dite aussi ***R-conversion***.
- La R-conversion s'écrit $\underset{R}{\longleftrightarrow\!\!\!\!\!\rightarrow}$ ou $=_R$ ou $\overset{*}{\underset{R}{\longleftrightarrow}}$
- $M \underset{R}{\longleftrightarrow\!\!\!\!\!\rightarrow} P$ se dit
  - M est R***-égal*** à P
  - ou M est R***-convertible*** à P.

6.1.3 Quelques résultats de stabilité

Contexte

Un ***contexte*** $C[\,]$ est défini ainsi

1. $[\,]$ est un contexte,
2. si $M \in \Lambda$ et si $C[\,]$ est un contexte alors $MC[\,]$ et $C[\,]M$ sont des contextes,
3. si $C[\,]$ est un contexte alors $\lambda x.C[\,]$ est un contexte.

Définition. Si $C[\,]$ est un contexte et $A \in \Lambda$ alors $C[A]$ est défini par induction sur $C[\,]$.

- $[A] = A$,
- si $C[\,] = \lambda x.D[\,]$ alors $C[A] = \lambda x.D[A]$,
- si $C[\,] = MD[\,]$ alors $C[A] = MD[A]$,
- si $C[\,] = D[\,]M$ alors $C[A] = D[A]M$,

Stabilité

Un relation $\xrightarrow[R]{}$ est ***stable par contexte*** si $M \xrightarrow[R]{} N$ alors $C[M] \xrightarrow[R]{} C[N]$.

Un relation $\xrightarrow[R]{}$ est ***stable par substitution*** si $M \xrightarrow[R]{} N$ alors $P[x := M] \xrightarrow[R]{} P[x := N]$.

Proposition 6.3. *Soit* $\xrightarrow[R]{}$ *une contraction.*

$\xrightarrow[R]{}$, $\xrightarrow[R]{}$ *et* $\xleftrightarrow[R]{}$ *sont stables par contexte.*

$\xrightarrow[R]{}$ *et* $\xleftrightarrow[R]{}$ *sont stables par substitutions.*

Proposition 6.4. $\xrightarrow[R]{}$ *est stable par contexte.*

Démonstration. Si $M \xrightarrow[R]{} N$ alors $C[M] \xrightarrow[R]{} C[N]$

Par induction sur la structure de $C[\,]$, sachant que $M \xrightarrow[R]{} N$.

1. $C[\,] = [\,]$ alors $C[M] = M$ et $C[N] = N$, évident.
2. $C[\,] = AD[\,]$,
   - par induction $D[M] \xrightarrow[R]{} D[N]$,
   - d'autre part, $C[M] = AD[M]$ et $C[N] = AD[N]$,
   - donc par congruence à droite $C[M] \xrightarrow[R]{} C[N]$.
3. $C[\,] = D[\,]A$, comme 2 en changeant «droite» en «gauche».
4. $C[\,] = \lambda x.D[\,]$, par induction $D[M] \xrightarrow[R]{} D[N]$, d'où la conclusion par (ξ). ■

Stabilité par substitution

Proposition 6.5. $M \xrightarrow[R]{} N$ *implique* $A[x := M] \xrightarrow[R]{} A[x := N]$.

Démonstration.

L'hypothèse est $M \xrightarrow[R]{} N$. La démonstration se fait par induction sur A.

- $A \equiv x$, alors $A[x := M] \equiv M \xrightarrow[R]{} N \equiv A[x := N]$.
- $A \equiv y$, alors $A[x := M] \equiv y \xrightarrow[R]{} y \equiv A[x := N]$ par réflexivité.
- $A \equiv \lambda y.B$, par induction $B[x := M] \xrightarrow[R]{} B[x := N]$, donc $A[x := M] \equiv \lambda y.B[x := M]$ et $A[x := N] \equiv \lambda y.B[x := N]$, par (ξ) pour $\xrightarrow[R]{}$, on a $\lambda y.B[x := M] \xrightarrow[R]{} \lambda y.B[x := N]$.

– $A \equiv BB'$ par induction

$$\begin{array}{ccc} B[x := M] & \xrightarrow[R]{} & B[x := N] \\ B'[x := M] & \xrightarrow[R]{} & B'[x := N] \end{array}$$

par définition de la substitution

$$\begin{array}{rcl} A[x := M] & \equiv & B[x := M]\ B'[x := M] \\ A[x := N] & \equiv & B[x := N]\ B'[x := N] \end{array}$$

par congruence et transitivité de $\xrightarrow[R]{}$ on a

$$\frac{B[x := M] \twoheadrightarrow B[x := N] \qquad B'[x := M] \twoheadrightarrow B'[x := N]}{\begin{array}{cc} B[x := M]B'[x := M] & B[x := N]B'[x := M] \\ \twoheadrightarrow & \twoheadrightarrow \\ B[x := N]B'[x := M] & B[x := N]B'[x := N] \end{array}}{B[x := M]B'[x := M] \twoheadrightarrow B[x := N]B'[x := N]}$$

■

Exercice

Montrez que ça ne peut pas marcher pour $\xrightarrow[R]{}$, c'est-à-dire qu'*on n'a pas* :

$M \xrightarrow[R]{} N$ implique $A[x := M] \xrightarrow[R]{} A[x := N]$.

6.1.4 Redex et formes normales

Quelques définitions

– Un R-***redex*** est un terme M tel que $(M, N) \in R$.
– N et le R-contracté de M.
– Un terme M est R-***irréductible*** si M ne contient aucun R-redex.

Quelques exemples de redex

Les β-redex sont de la forme $(\lambda x.M)N$.
Les η-redex sont de la forme $\lambda x.(Mx)$ si x *n'est pas libre dans* M.
Tout terme est un redex pour l'expansion η.

Formes normales

Un terme N est une ***forme normale*** de M, si N est R-irréductible et si $M \xrightarrow[R]{\twoheadrightarrow} N$.

On n'affirme

– *ni l'existence* cf le terme $(\lambda x.xx)\ (\lambda x.xx)$,
– *ni l'unicité*, il y a unicité pour β, mais il faut le prouver.
La forme β-normale de M si elle existe (et si on a prouvé l'unicité) est la valeur intentionnelle de M.

Exercice

Lesquels de ces termes sont des formes normales ?
$(\lambda x.x)$
$((\lambda xy.x)v)w$
$(\lambda xy.xv)w$
$\lambda xy.xvw$
$(\lambda x.xx)\ (\lambda x.xx)$
$(\lambda xy.y)((\lambda x.xx)\ (\lambda x.xx))$

6.1.5 Des termes

Ω et les autres

$\omega \equiv \lambda x.xx$
$\Omega \equiv (\lambda x.xx)(\lambda x.xx)$
$\mathsf{Y} \equiv \lambda f.(\lambda x.f(xx))(\lambda x.f(xx))$
$\mathsf{W}_F \equiv (\lambda x.F(xx))$

Exercices

Montrez que Ω se récrit vers un unique terme. Lequel ?

Plus précisément, montrez qu'il existe un terme unique $M \in \Lambda$ tel que $\Omega \xrightarrow[\beta]{} M$.

Ω n'a pas de forme normale.

1. Montrez que $\mathsf{Y}F \xrightarrow[\beta]{} F(\mathsf{W}_F\mathsf{W}_F)$.
2. Montrez que $F(\mathsf{Y}F) \xrightarrow[\beta]{} F(\mathsf{W}_F\mathsf{W}_F)$.
3. Conclure que $\mathsf{Y}F \xleftrightarrow[\beta]{} F(\mathsf{Y}F)$.

Y est appelé le combinateur de ***point de fixe***.
Y et $\mathsf{Y}F$ n'ont pas de formes normales.

6.1.6 Les entiers de Church

Entiers de Church

- $(\lambda fx.f(fx)) \equiv \mathbf{2}$ correspond au nombre entier *deux*.
- $(\lambda fx.x) \equiv T$ correspond à *zéro*.
- $(\lambda fx.fx) \equiv \mathbf{1}$ correspond à *un*.
- Plus généralement l'entier $\mathbf{n}$ est le terme $(\lambda fx.f^n x)$.

Exercice

1. Montrez que
$$\mathbf{1} \xrightarrow[\eta]{} I \equiv \lambda x.x.$$
2. Écrivez l'opération «successeur».
3. Écrivez les opérations d'«addition» et de «multiplication».
4. Calculez
   - $\mathbf{12}$,
   - $\mathbf{21}$,

– **22**,

5. A quoi correspond **mn** ?

Corrigé

En effet,

$$\begin{array}{rcl} \mathbf{1} & \equiv & \lambda fx.fx \\ & \xrightarrow[\eta]{} & \lambda f.f \quad \equiv \quad I. \end{array}$$

Le ***successeur*** est $\mathbf{succ} \equiv \lambda nfx.n\ f\ (f\ x)$,
l'***addition*** est $\mathbf{add} \equiv \lambda mnfx.\ m\ f\ (n\ f\ x)$,
tandis que la ***multiplication*** est $\mathbf{mult} \equiv \lambda mnf.\ m\ (n\ f)$.

$$\begin{array}{rcl} \mathbf{22} & \equiv & (\lambda fx.f(f\ x))\ (\lambda gy.g(g\ y)) \\ & \longrightarrow & \lambda x.(\lambda gy.g(g\ y))\ ((\lambda hz.h(h\ z))\ x) \\ & \longrightarrow & \lambda x.(\lambda gy.g(g\ y))\ (\lambda z.x(x\ z)) \\ & \longrightarrow & \lambda xy.(\lambda z.x(x\ z))\ ((\lambda w.x(x\ w))y) \\ & \longrightarrow & \lambda xy.(\lambda z.x(x\ z))\ (x\ (x\ y)) \\ & \longrightarrow & \lambda xy.x(x\ (x\ (x\ y))) \\ & \equiv & \lambda fx.f(f\ (f\ (f\ x))) \quad \equiv \quad \mathbf{4} \end{array}$$

Appelons $\mathbf{p} \equiv \lambda mn.m\ n$ cette opération.
Autrement dit $\mathbf{p\ m\ n} = \mathbf{m\ n}$.
On remarque que

$$\begin{array}{rcl} \mathbf{p\ 0\ n} & \xrightarrow[\beta]{} & (\lambda fx.x)\ \mathbf{n} \\ & \xrightarrow[\beta]{} & \lambda x.x \\ & \xleftarrow[\eta]{} & \mathbf{1} \end{array}$$

et que

$$\begin{array}{rcll} \mathbf{p\ (succ\ m)\ n}\ x & \triangleq & \mathbf{succ\ m\ n}\ x & \text{Définition de } \mathbf{p} \\ & \xrightarrow[\beta]{} & (\mathbf{m\ n})\ (\mathbf{n}\ x) & \text{Définition de } \mathbf{succ} \\ & \xleftarrow[\beta]{} & \mathbf{mult\ (m\ n)\ n}\ x & \text{Définition de } \mathbf{mult} \\ & \triangleq & \mathbf{mult\ (p\ m\ n)\ n}\ x & \text{Définition de } \mathbf{p}. \end{array}$$

On a donc

$$\begin{array}{rcl} \mathbf{p\ 0\ n} & =_{\beta\eta} & \mathbf{1} \\ \mathbf{p\ (succ\ m)\ n} & =_{\beta\eta} & \mathbf{mult\ (p\ m\ n)\ n} \end{array}$$

Or on a

$$\begin{array}{rcl} n^0 & = & 1 \\ n^{m+1} & = & n^m \cdot n. \end{array}$$

p est un bon candidat pour représenter l'***exponentielle***. Il y a simplement un problème : *on «applique» un entier à un entier.*

6.1.7 Lambda calcul et cohérence

Le lambda calcul est maximalement cohérent

Un théorie $\mathcal{T}$ est ***maximalement cohérente*** (on dit aussi qu'elle est ***complète au sens de Hilbert***) si pour tout φ

– ou bien $\vdash \varphi$,
– $\mathcal{T} + \varphi$ est incohérente.

La $\beta\eta$-calcul est maximalement cohérent, autrement dit pour tout M et N,
– ou bien $\vdash M \underset{\beta\eta}{\twoheadleftarrow\!\!\!\twoheadrightarrow} N$,
– $\beta\eta + (M \underset{}{\twoheadleftarrow\!\!\!\twoheadrightarrow} N)$ est incohérent, autrement dit pour tout $P, Q \in \Lambda$, on a $\beta\eta + (M \underset{}{\twoheadleftarrow\!\!\!\twoheadrightarrow} N) \quad \vdash \quad P \underset{}{\twoheadleftarrow\!\!\!\twoheadrightarrow} Q$.
On va considérer un cas assez spécifique
Supposons que l'on ajoute au lambda calcul l'identité $\mathbf{S} = \mathbf{K}$.
Notons que d'une part

$$\begin{aligned} \mathbf{S}\ \mathbf{I}\ (\mathbf{K}\ P)\ \mathbf{I} &\xrightarrow[\beta]{} \mathbf{I}\ (\mathbf{K}\ P)\ \mathbf{I} \\ &\xrightarrow[\beta]{} \mathbf{K}\ P\ \mathbf{I} \\ &\xrightarrow[\beta]{} P \end{aligned}$$

et d'autre part

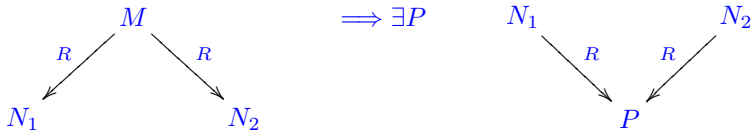
$$\begin{aligned} \mathbf{K}\ \mathbf{I}\ (\mathbf{K}\ P)\ \mathbf{I} &\xrightarrow[\beta]{} \mathbf{I}\ \mathbf{I} \\ &\xrightarrow[\beta]{} \mathbf{I} \end{aligned}$$

Donc de $\mathbf{S} = \mathbf{K}$ on déduit que pour tout terme P on a $P = \mathbf{I}$.

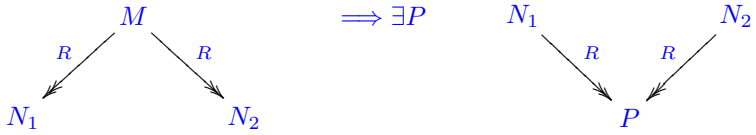
Autrement dit, si on ajoute au lambda calcul l'unique égalité $\mathbf{S} = \mathbf{K}$, on le rend incohérent en autorisant tous les termes à être égaux.

6.2 Confluence

Propriété du losange

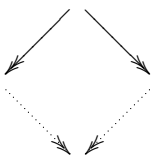


Confluence



Remarques

1. $\underset{R}{\longrightarrow}$ est confluente si $\underset{R}{\twoheadrightarrow}$ a la propriété du losange.
2. Parfois on note la confluence :



où $\cdots\!\!\twoheadrightarrow$ est un flèche existentielle.

Confluence et convertibilité

Théorème 6.6 (Church-Rosser). *Si R est confluente alors* $M \underset{R}{\twoheadleftarrow\!\!\twoheadrightarrow} N \iff \exists P(M \underset{R}{\twoheadrightarrow} P \wedge N \underset{R}{\twoheadrightarrow} P)$.

Démonstration.

- $\Leftarrow$ est évident car $\underset{R}{\twoheadrightarrow} \subseteq \underset{R}{\twoheadleftarrow\!\!\twoheadrightarrow}$ et $\underset{R}{\twoheadleftarrow\!\!\twoheadrightarrow}$ est symétrique et transitive.
- $\Rightarrow$ Par induction sur le nombre de «pics» dans $M \underset{R}{\twoheadleftarrow\!\!\twoheadrightarrow} N$. Soit

  $M \overset{+}{\underset{R}{\twoheadleftarrow}} M_1 \overset{+}{\underset{R}{\twoheadrightarrow}} N_1 \ldots \overset{+}{\underset{R}{\twoheadleftarrow}} M_i \overset{+}{\underset{R}{\twoheadrightarrow}} N_1 \ldots$

  $\ldots N_{n-1} \overset{+}{\underset{R}{\twoheadleftarrow}} M_n \overset{+}{\underset{R}{\twoheadrightarrow}} N_n \underset{R}{\twoheadleftarrow} N$
  - si $n = 0$ alors $M \underset{R}{\twoheadleftarrow} N$ ou $M \underset{R}{\twoheadrightarrow} N$.
  - si $n \neq 0$, par confluence, dans

    $M \overset{+}{\underset{R}{\twoheadleftarrow}} M_1 \overset{+}{\underset{R}{\twoheadrightarrow}} N_1 \ldots N_{n-1} \overset{+}{\underset{R}{\twoheadleftarrow}} M_n \overset{+}{\underset{R}{\twoheadrightarrow}} N_n \underset{R}{\twoheadleftarrow} N$

    il existe M'_n tel que $N_{n-1} \overset{+}{\underset{R}{\twoheadrightarrow}} M'_n \overset{+}{\underset{R}{\twoheadleftarrow}} N_n \underset{R}{\twoheadleftarrow} N$

    et $M \overset{+}{\underset{R}{\twoheadleftarrow}} M_1 \overset{+}{\underset{R}{\twoheadrightarrow}} N_1 \ldots \overset{+}{\underset{R}{\twoheadleftarrow}} M_i \overset{+}{\underset{R}{\twoheadrightarrow}} N_1 \ldots$

    $\ldots N_{n-1} \overset{+}{\underset{R}{\twoheadrightarrow}} M'_n \overset{+}{\underset{R}{\twoheadleftarrow}} N_n \underset{R}{\twoheadleftarrow} N$

    a un pic de moins, donc on a le résultat par induction. ■

Confluence et convertibilité

Corollaire 1. *Si R est confluente*

1. *Si N est une forme normale de M alors* $M \underset{R}{\twoheadrightarrow} N$.
2. *Un terme a au plus une forme normale.*

Confluence de $\rightarrow_\beta$

Théorème 6.7. $\underset{\beta}{\longrightarrow}$ *est confluent*

Remarques préliminaires

- Si $\underset{R}{\longrightarrow}$ a la propriété du losange, alors $\underset{R}{\twoheadrightarrow}$ a la propriété du losange.
- $\underset{\beta}{\longrightarrow}$ n'a pas la propriété du losange. Pourquoi ?
- Il faut donc trouver une relation $\underset{}{\dashrightarrow}$ telle que
  - $\underset{}{\dashrightarrow}$ a la propriété du losange,
  - $\underset{}{\dashrightarrow\!\!\twoheadrightarrow} = \underset{\beta}{\twoheadrightarrow}$,
    - donc $\underset{\beta}{\twoheadrightarrow}$ a la propriété du losange,
    - ce qui signifie que $\underset{\beta}{\longrightarrow}$ est confluente.

Lemme de substitution

Lemme 6.8. *Si* $x \notin FV(L)$ *alors* $M[x := N][y := L] \equiv M[y := L][x := N[y := L]]$

Démonstration. Par induction sur la structure de M.

– M est la variable x : Alors $M[x := N][y := L] \equiv$

$$\begin{aligned} &\equiv x[x := N][y := L] \\ &\equiv N[y := L] \\ &\equiv x[x := N[y := L]] \\ &\equiv x[y := L][x := N[y := L]] \end{aligned}$$

– M est la variable y : Alors $M[x := N][y := L] \equiv$

$$\begin{aligned} &\equiv y[x := N][y := L] \\ &\equiv y[y := L] \\ &\equiv L \\ &\equiv L[x := N[y := L]] \quad (\text{par } x \notin FV(L)) \\ &\equiv (y[y := L])[x := N[y := L]] \end{aligned}$$

– M est la variable z : Alors $M[x := N][y := L] \equiv$

$$\begin{aligned} &\equiv z[x := N][y := L] \\ &\equiv z[y := L] \\ &\equiv z \\ &\equiv z[x := N[y := L]] \\ &\equiv z[y := L][x := N[y := L]] \end{aligned}$$

– M est une abstraction : $M \equiv \lambda z.M_1$. Alors $M[x := N][y := L] \equiv$

$$\begin{aligned} &\equiv (\lambda z.M_1)[x := N][y := L] \\ &\equiv \lambda z.(M_1[x := N][y := L]) \quad (\text{par définition}) \\ &\equiv \lambda z.(M_1[y := L][x := N[y := L]]) \quad (\text{par induction}) \\ &\equiv (\lambda z.M_1)[y := L][x := N[y := L]] \quad (\text{par définition}) \end{aligned}$$

– M est une application : facile. ∎

Définition de la réduction parallèle

$$\frac{}{M \twoheadrightarrow M} \text{ (réflexivité)}$$

$$\frac{M \twoheadrightarrow M' \qquad N \twoheadrightarrow N'}{MN \twoheadrightarrow M'N'} \text{ (APP-congruence)}$$

$$\frac{M \twoheadrightarrow M'}{\lambda x.M \twoheadrightarrow \lambda x.M'} \text{ (ABS-congruence)}$$

$$\frac{M \twoheadrightarrow M' \qquad N \twoheadrightarrow N'}{(\lambda x.M)N \twoheadrightarrow M'[x := N']} \text{ (β-parallèle)}$$

Trois résultats

1. Si $M \xrightarrow[\beta]{} M'$ alors $M \twoheadrightarrow M'$ c'est-à-dire $\xrightarrow[\beta]{} \subseteq \twoheadrightarrow$
2. Si $M \twoheadrightarrow M'$ alors $M \xrightarrow[\beta]{}\!\!\!\!\twoheadrightarrow M'$ c'est-à-dire $\twoheadrightarrow \subseteq \xrightarrow[\beta]{}\!\!\!\!\twoheadrightarrow$
3. Si $M \twoheadrightarrow M'$ et $N \twoheadrightarrow N'$ alors $M[x := N] \twoheadrightarrow M'[x := N']$

   En exercice.

Une propriété plus forte

On prouve une propriété plus forte que la propriété du losange pour $\twoheadrightarrow$:

$$M \twoheadrightarrow N \Longrightarrow N \twoheadrightarrow M^* \tag{6.1}$$

où M^* est un terme déterminé par M mais *indépendant* de N.

Intuitivement, M^* est le terme obtenu à partir de M en contractant tous ses redex simultanément.

Le définition de M^*

1. $x^* \equiv x$
2. $(\lambda x.M)^* \equiv \lambda x.M^*$
3. $(M_1 M_2)^* \equiv M_1^* M_2^*$ si $M_1 M_2$ n'est pas un redex.
4. $((\lambda x.M_1)M_2)^* \equiv M_1^*[x := M_2^*]$

Exercices

Calculer

1. $((\lambda x.x)\ ((\lambda yzu.y\ (z\ u))\ abc))^*$
2. $((\lambda x.x\ x)\ (\lambda y.y\ y))^*$

Proposition 6.9. $M \twoheadrightarrow N \Longrightarrow N \twoheadrightarrow M^*$

Démonstration. Les cas correspondant aux parties 1., 2. et 3. de la définition M^* sont laissés en exercice.

Si $M \equiv ((\lambda x.M_1)M_2) \twoheadrightarrow N$, alors deux cas pour N,

- $N \equiv (\lambda x.N_1)N_2$
- $N \equiv N_1[x := N_2]$

dans les deux cas, il y a des N_i (i=1 ou i=2) tels que $M_i \twoheadrightarrow N_i$.

Par induction, $N_i \twoheadrightarrow M_i^*$.

Pour chaque cas :

- Si $N \equiv (\lambda x.N_1)N_2$ alors $N \twoheadrightarrow M_1^*[x := M_2^*] \equiv M^*$.
- Si $N \equiv N_1[x := N_2]$, alors nous avons $N \twoheadrightarrow M_1^*[x := M_2^*] \equiv M^*$, préservation de $\twoheadrightarrow$ par substitution. ∎

Résumons

De la propriété 6.1 pour $\twoheadrightarrow$ on déduit la propriété du losange pour $\twoheadrightarrow$ de laquelle on déduit la propriété du losange pour $\twoheadrightarrow$ de laquelle on déduit la propriété du losange pour $\xrightarrow[\beta]{}$ parce que $\xrightarrow[\beta]{} = \twoheadrightarrow$, qui est la confluence de $\xrightarrow[\beta]{}$.

Donc $\xrightarrow[\beta]{}$ est confluent. ■

6.3 Lambda calcul simplement typé

Le paradoxe du barbier

$\Omega \equiv (\lambda x.xx)(\lambda x.xx)$ et $\mathsf{Y} \equiv \lambda f.(\lambda x f(xx))\ (\lambda x f(xx))$ contiennent des termes qui s'appliquent à eux-mêmes.

Le ***paradoxe du barbier*** est :

> Le barbier rase tous ceux qui ne se rasent pas eux-mêmes. Qui rase le barbier ?

Pour éviter les paradoxes, on cherche à éviter de tels termes.

On va donc ***typer*** les termes.

Typer est aussi bien pour la programmation.

Les objectifs du typage

Le typage a donc deux objectifs :

- préserver la correction, *rien de mauvais ne peut arriver*,
- préserver la terminaison, *toutes les réductions se terminent.*

En λ-calcul la ***terminaison*** s'appelle la ***normalisation forte***.

6.3.1 Les types à la Church

Types, annotations des variables

Les ***types*** sont

- soit des types de base o,
- soit des types applications $\sigma \to \tau$.

Dans l'approche dite ***à la Church***, les variables associées à un λ sont annotées par un type.

$$M, N \quad ::= \quad x \mid \lambda x^{\sigma}.M \mid M\ N$$

Soit Γ un ensemble de variables (toutes différentes) annotées par leurs types.

$$\Gamma \quad = \quad \{x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}\}.$$

Jugements et règles

Un jugement de typage à la Church est une déclaration de la forme $\Gamma \vdash M : \sigma$.

On a alors les règles de typage suivante.

$$\frac{}{\Gamma \vdash x : \sigma \quad \text{si } x^{\sigma} \in \Gamma} \qquad \frac{\Gamma \cup \{x^{\sigma}\} \vdash M : \tau}{\Gamma \vdash \lambda x^{\sigma}.M : \sigma \to \tau.}$$

$$\frac{\Gamma \vdash M : \sigma \to \tau \quad \Gamma \vdash N : \sigma}{\Gamma \vdash M\ N : \tau}$$

Un exemple

À la Church on écrirait :

$$(\lambda f^{(o\to o)\to(o\to o)} x^{o\to o}.f(fx))\ (\lambda f^{o\to o} x^{o}.f(fx))$$

6.3.2 Les types à la Curry

Les environnements

Dans l'approche ***à la Curry***, on traite des termes usuels du lambda-calcul.

Il faut typer les variables libres, il faut donc faire des hypothèses sur les types de ces variables.

D'où la notion d'***environnement***.

Un environnement est un ensemble d'association de types à des variables.

$$\Gamma \equiv x_1 : \sigma_1, \ldots, x_n : \sigma_n$$

Les types

Un ***jugement*** est l'affirmation du type σ d'un terme M sous un certain environnement Γ :

$$\Gamma \vdash M : \sigma$$

Les règles

$$\frac{}{\Gamma, x : \sigma \vdash x : \sigma}\ (Var)$$

$$\frac{\Gamma, x : \sigma \vdash M : \tau}{\Gamma \vdash \lambda x.M : \sigma \to \tau}\ (Abs)$$

$$\frac{\Gamma \vdash M : \sigma \to \tau \qquad \Gamma \vdash N : \sigma}{\Gamma \vdash MN : \tau}\ (App)$$

Exercices

Typez les termes
$B \equiv \lambda xyz.x(yz)$,
$I \equiv \lambda x.x$,
$C \equiv \lambda xyz.xzy$,
$K \equiv \lambda xy.x$,
$S \equiv \lambda xyz.xz(yz)$,
$\mathbf{p\ 2\ 2} \equiv (\lambda mn.m\ n)\ (\lambda fx.f(fx))\ (\lambda fx.f(fx))$

1. Typez $II \equiv (\lambda x.x)(\lambda x.x)$.

2. Typez $\mathbf{2}\ \mathbf{2} \equiv (\lambda fx.f(fx))(\lambda fx.f(fx))$.
3. A-t-on le même type pour I (resp. $\mathbf{2}$) dans chaque cas ?

Conclusion : Le système de ***types simples*** n'est pas assez général. Il ne permet pas d'affecter un type unique à chaque terme.

Le type d'un même terme peut dépendre de son contexte.

Préservation du typage par substitution

Proposition 6.10. *Si* $\Gamma, x : \sigma \vdash M : \tau$ *et* $\Gamma \vdash N : \sigma$ *alors* $\Gamma \vdash M[x := N] : \tau$

Démonstration. Par induction sur M.

- Si $M \equiv y$ alors Γ contient $y : \tau$ et $M[x := N] \equiv M \equiv y$ donc le résultat qui est $\Gamma \vdash y : \tau$ est clair.
- Si $M \equiv x$ alors $\tau = \sigma$ et $M[x := N] \equiv N$ et le résultat est l'une des hypothèses.
- Si $M \equiv P\ Q$ alors par (App) pour un certain τ', on a
  - $\Gamma, x : \sigma \vdash P : \tau' \to \tau$ duquel on tire par induction $\Gamma \vdash P[x := N] : \tau' \to \tau$
  - et $\Gamma, x : \sigma \vdash Q : \tau'$ duquel on tire par induction $\Gamma \vdash Q[x := N] : \tau'$.

  Donc par (App) $\Gamma \vdash (P\ Q)[x := N] : \tau$ puisque $(P\ Q)[x := N] \equiv P[x := N]\ Q[x := N]$.
- Le cas $M \equiv \lambda x.P$ est similaire. ■

Réduction du sujet

Lemme 6.11 (Réduction du sujet). *La β-réduction préserve le type.*
Si $\Gamma \vdash M : \sigma$ *et si* $M \xrightarrow[\beta]{} N$ *alors* $\Gamma \vdash N : \sigma$.

Démonstration. Par induction sur la définition de $M \xrightarrow[\beta]{} N$.

- Cas $M \equiv (\lambda x.M_1)M_2$. $\Gamma \vdash (\lambda x.M_1)M_2 : \sigma$ vient de $\Gamma, x : \tau \vdash M_1 : \sigma$ et de $\Gamma \vdash M_2 : \tau$. D'autre part $N \equiv M_1[x := M_2]$ or d'après le lemme $\Gamma \vdash M_1[x := M_2] : \sigma$.
- Cas $M \equiv M_1M_2$ avec $N \equiv N_1M_2$ et $M_1 \xrightarrow[\beta]{} N_1$. $\Gamma \vdash M : \sigma$ vient de $\Gamma \vdash M_1 : \tau \to \sigma$ et $\Gamma \vdash M_2 : \tau$, par induction $\Gamma \vdash N_1 : \tau \to \sigma$ et donc $\Gamma \vdash N_1M_2 : \sigma$.
- Les autres cas sont similaires. ■

Commentaires

- Si un terme est d'un certain type, *il n'en sortira pas* par β-réduction.
- Si un terme a une forme normale et s'il a un type, alors *sa forme normale a ce type.*

6.3.3 La correspondance de Curry-Howard

> La mathématique c'est l'art de donner le même nom à des choses différentes.
>
> Henri Poincaré

La correspondance de Curry-Howard

$$\frac{}{\Gamma, x:\sigma \vdash x:\sigma}\,(Var) \qquad \frac{\Gamma, x:\sigma \vdash M:\tau}{\Gamma \vdash \lambda x.M : \sigma \to \tau}\,(Abs) \qquad \frac{\Gamma \vdash M:\sigma \to \tau \qquad \Gamma \vdash N:\sigma}{\Gamma \vdash MN : \tau}\,(App)$$

$$\frac{}{\Gamma, p \vdash p} \qquad \frac{\Gamma, p \vdash q}{\Gamma \vdash p \Rightarrow q} \Rightarrow I \qquad \frac{\Gamma \vdash p \Rightarrow q \qquad \Gamma \vdash p}{\Gamma \vdash q} \Rightarrow E$$

Dans $\Gamma \vdash M : \sigma$,
- M: est une ***annotation*** qui est le ***«terme de preuve»***,
- σ peut-être vu comme un ***type*** ou comme une ***proposition***.

La preuve de B

$$\dfrac{\dfrac{\dfrac{\dfrac{(p \Rightarrow q),\ (r \Rightarrow p), r \vdash p \Rightarrow q \qquad \mathcal{D}}{(p \Rightarrow q),\ (r \Rightarrow p), r \vdash q} \Rightarrow E}{(p \Rightarrow q),\ (r \Rightarrow p) \vdash r \Rightarrow q}}{(p \Rightarrow q) \vdash (r \Rightarrow p) \Rightarrow r \Rightarrow q}}{\vdash (p \Rightarrow q) \Rightarrow (r \Rightarrow p) \Rightarrow r \Rightarrow q}$$

où $\mathcal{D}$ est

$$\frac{(p \Rightarrow q),\ (r \Rightarrow p), r \vdash r \Rightarrow p \qquad (p \Rightarrow q),\ (r \Rightarrow p), r \vdash r}{(p \Rightarrow q),\ (r \Rightarrow p), r \vdash p} \Rightarrow E$$

La preuve de B annotée

$$\dfrac{\dfrac{\dfrac{\dfrac{x:(p \Rightarrow q),\ y:(r \Rightarrow p), z:r \vdash x : p \Rightarrow q \qquad \dfrac{\mathcal{D}_1 \qquad \mathcal{D}_2}{\mathcal{D}_3} \Rightarrow E}{x:(p \Rightarrow q),\ y:(r \Rightarrow p), z:r \vdash x\ (y\ z) : q} \Rightarrow E}{x:(p \Rightarrow q),\ y:(r \Rightarrow p) \vdash \lambda z.x\ (y\ z) : r \Rightarrow q}}{x:(p \Rightarrow q) \vdash \lambda yz.x\ (y\ z) : (r \Rightarrow p) \Rightarrow r \Rightarrow q}}{\vdash \lambda xyz.x\ (y\ z) : (p \Rightarrow q) \Rightarrow (r \Rightarrow p) \Rightarrow r \Rightarrow q}$$

où
$$\begin{aligned} \mathcal{D}_1 &= x:(p \Rightarrow q),\ y:(r \Rightarrow p), z:r \vdash y : r \Rightarrow p \\ \mathcal{D}_2 &= x:(p \Rightarrow q),\ y:(r \Rightarrow p), z:r \vdash z : r \\ \mathcal{D}_3 &= x:(p \Rightarrow q),\ y:(r \Rightarrow p), z:r \vdash y\ z : p \end{aligned}$$

La preuve du lemme B est le terme B !

Simplification de preuves

La preuve

$$\dfrac{\dfrac{\dfrac{\dfrac{(p \Rightarrow p), q \vdash p \Rightarrow p}{(p \Rightarrow p) \vdash q \Rightarrow p \Rightarrow p}\,(\Rightarrow I)}{\vdash (p \Rightarrow p) \Rightarrow q \Rightarrow p \Rightarrow p}\,(\Rightarrow I) \qquad \dfrac{\dfrac{p \vdash p}{\vdash p \Rightarrow p}\,(\Rightarrow I)}{\vdash q \Rightarrow p \Rightarrow p}\,(\Rightarrow E)}$$

peut être réduite
En effet, on fait une introduction immédiatement suivie d'une élimination :

$$\dfrac{\dfrac{\dfrac{(p \Rightarrow p), q \vdash p \Rightarrow p}{(p \Rightarrow p) \vdash q \Rightarrow p \Rightarrow p}(\Rightarrow I)}{\vdash (p \Rightarrow p) \Rightarrow q \Rightarrow p \Rightarrow p}(\Rightarrow I) \qquad \dfrac{p \vdash p}{\vdash p \Rightarrow p}(\Rightarrow I)}{\vdash q \Rightarrow p \Rightarrow p}(\Rightarrow E)$$

On peut obtenir une preuve de $\vdash q \Rightarrow p \Rightarrow p$ à partir de la preuve de $(p \Rightarrow p) \vdash q \Rightarrow p \Rightarrow p$.
Pour cela, il suffit de remplacer chaque occurrence de l'utilisation de l'hypothèse $(p \Rightarrow p)$ par sa preuve.
En utilisant cette remarque,

$$\dfrac{\dfrac{\dfrac{(p \Rightarrow p), q \vdash p \Rightarrow p}{(p \Rightarrow p) \vdash q \Rightarrow p \Rightarrow p}(\Rightarrow I)}{\vdash (p \Rightarrow p) \Rightarrow q \Rightarrow p \Rightarrow p}(\Rightarrow I) \qquad \dfrac{p \vdash p}{\vdash p \Rightarrow p}(\Rightarrow I)}{\vdash q \Rightarrow p \Rightarrow p}(\Rightarrow E)$$

donne

$$\dfrac{\dfrac{q, p \vdash p}{q \vdash p \Rightarrow p}(\Rightarrow I)}{\vdash q \Rightarrow p \Rightarrow p}(\Rightarrow I)$$

Donc avec les annotations par les termes de preuve

$$\dfrac{\dfrac{\dfrac{x : (p \Rightarrow p), y : q \vdash x : p \Rightarrow p}{x : (p \Rightarrow p) \vdash \lambda y.x : q \Rightarrow p \Rightarrow p}(Abs)}{\vdash \lambda xy.x : (p \Rightarrow p) \Rightarrow q \Rightarrow p \Rightarrow p}(Abs) \qquad \dfrac{z : p \vdash z : p}{\vdash \lambda z.z : p \Rightarrow p}(Abs)}{\vdash (\lambda xy.x)\ (\lambda z.z) : q \Rightarrow p \Rightarrow p}(App)$$

donne

$$\dfrac{\dfrac{y : q, z : p \vdash z : p}{y : q \vdash \lambda z.z : p \Rightarrow p}(Abs)}{\vdash (\lambda y.x)[x := \lambda z.z] \equiv \lambda yz.z : q \Rightarrow p \Rightarrow p}(Abs)$$

La β-réduction correspond à la simplification des preuves.

$$\dfrac{\dfrac{\dfrac{\mathcal{D}}{\varphi, \Gamma \vdash \psi}}{\Gamma \vdash \varphi \Rightarrow \psi}(\Rightarrow I) \qquad \dfrac{\mathcal{D}'}{\Gamma \vdash \varphi}}{\Gamma \vdash \psi}(\Rightarrow E)$$

se transforme en

$$\frac{\mathcal{D}''}{\Gamma \vdash \psi}$$

$\mathcal{D}''$ est la preuve $\mathcal{D}$ dans laquelle toutes les utilisations de l'hypothèse φ sont remplacées par la preuve $\mathcal{D}$ de φ.

$$\frac{\dfrac{\dfrac{\mathcal{D}}{x : \varphi, \Gamma \vdash M : \psi}}{\Gamma \vdash (\lambda x.M) : \varphi \Rightarrow \psi}\,(Abs) \qquad \dfrac{\mathcal{D}'}{\Gamma \vdash N : \varphi}}{\Gamma \vdash (\lambda x.M)\ N : \psi}\,(App)$$

se transforme en

$$\frac{\mathcal{D}''}{\Gamma \vdash M[x := N] : \psi}$$

$\mathcal{D}''$ (qui se note $M[x := N]$) est la preuve $\mathcal{D}$ (qui se note M) dans laquelle toutes les utilisations de l'hypothèse $x : \varphi$ sont remplacées par la preuve $\mathcal{D}$ de φ (qui se note N).

La correspondance complète de Curry-Howard

On obtient le tableau de correspondance :

types	***propositions***
termes	***preuves***
réduction	***simplification des preuves***

6.3.4 Forte normalisation

Terminaison de la simplification ?

Est-ce que le processus de simplification de preuves se ***termine*** ?

Autrement dit est-ce que ce processus est vraiment un processus de simplification.

Normalisation forte

Définition. Un terme M est ***fortement normalisable*** si toute suite de réductions $M \xrightarrow[\beta]{} M_1 \xrightarrow[\beta]{} \dots \xrightarrow[\beta]{} M_n \dots$ est finie.

Théorème 6.12. *Si $\Gamma \vdash M : \tau$ alors M est fortement normalisable.*

La démonstration repose sur deux lemmes.

Démonstration : premier lemme

Lemme 6.13. *Si A, B et $\vec{C}$ sont fortement normalisables et $AB\vec{C}$ n'est pas fortement normalisable alors il y a un D tel que*

1. $A \xrightarrow[\beta]{}\!\!\!\!\!\rightarrow \lambda x.D$
2. $D[x := B]\vec{C}$ *n'est pas fortement normalisable.*

Démonstration. Puisque A, B et $\vec{C}$ sont fortement normalisables, la réduction infinie qui part de $AB\vec{C}$ est de la forme

$$AB\vec{C} \underset{\beta}{\twoheadrightarrow} (\lambda x.D)B_1\vec{C_1} \underset{\beta}{\rightarrow} D[x := B_1]\vec{C_1} \underset{\beta}{\twoheadrightarrow} \dots$$

Mézalors le résultat vient immédiatement du fait que

$$D[x := B]\vec{C} \underset{\beta}{\twoheadrightarrow} D[x := B_1]\vec{C_1}.$$

■

Remettons le lemme à l'endroit.

Lemme 6.14. *Si A, B et $\vec{C}$ sont fortement normalisables et si D est le premier tel que*

1. $A \underset{\beta}{\twoheadrightarrow} \lambda x.D$
2. $D[x := B]\vec{C}$ *est fortement normalisable.*

alors $AB\vec{C}$ est fortement normalisable

Démonstration : second lemme

Lemme 6.15. *Si M et P sont typés et si M et P sont fortement normalisables, alors $M[x := P]$ est fortement normalisable.*

Démonstration. Par induction sur le triplet $(type(P), h(M), taille(M))$, où
- $type(P)$ est la complexité du type de P,
- $h(M)$ (ou hauteur) est la longueur de la plus longue réduction qui commence en M,
- $taille(M)$ est la taille de M (le nombre de symboles).

Examinons les cas possibles...
- $M = \lambda y.N$, clairement $h(M) = h(N)$, mais $taille(M) > taille(N)$. On applique l'induction.
  Donc $N[x := P]$ est fortement normalisable, donc $M[x := P] \equiv \lambda y.N[x := P]$ est fortement normalisable.
- $M = y\vec{R}$, les réductions ont lieu dans les R_i, donc clairement $h(M) \geqslant h(R_i)$, et $taille(M) > taille(R_i)$.
  On applique l'induction à chacun des R_i, on conclut que chaque $R_i[x := P]$ est fortement normalisable, donc $y \dots R_i[x := P] \dots$ est fortement normalisable, mais comme

  $$y \dots R_i[x := P] \dots \equiv (y\vec{R})[x := P].$$

  Par conséquent, $(y\vec{R})[x := P]$ est aussi fortement normalisable
- $M = (\lambda y.L)Q\vec{R}$
  Par induction, $L[x := P]$, $Q[x := P]$ et $\vec{R}[x := P]$ sont fortement normalisables.
  Posons $D \equiv L[y := Q]\ \vec{R}$.
  Si on veut utiliser le lemme précédent, il suffit de montrer que $L[x := P][y := Q[x := P]]\ \vec{R}[x := P] \equiv D[x := P]$ est fortement normalisable.

Or $h(M) > h(D)$ donc par induction $D[x := P]$ est fortement normalisable. On peut donc appliquer le 1er lemme.
Et donc par le lemme, $M[x := P]$ est fortement normalisable.

– $M = xL\vec{Q}$
On veut démontrer que $P\ L[x := P]\ \vec{Q}[x := P]$ est fortement normalisable.
Notons que
– $h(M) \geqslant h(L)$ et $taille(M) > taille(L)$
– et $h(M) \geqslant h(Q_i)$ et $taille(M) > taille(Q_i)$.
Donc, par induction, $L' \equiv L[x := P]$ et $\vec{Q'} \equiv \vec{Q}[x := P]$ sont fortement normalisables. Si on veut utiliser le lemme précédent, il suffit de montrer que si P_1 est le premier tel que $P \xrightarrow[\beta]{}\!\!\!\!\!\rightarrow \lambda y.P_1$ alors $M' \equiv P_1[y := L']\vec{Q'}$ est fortement normalisable.
Remarquons
– que $type(x) = type(P) = type(\lambda y.P_1) = \sigma \to \tau$,
– que $type(L) = type(L') = \sigma < type(P)$.
– et que $type(P_1[y := L']) = \tau < type(P)$
On peut appliquer l'hypothèse d'induction et donc $P_1[y := L']$ est fortement normalisable.
Parce que $type(P_1[y := L']) < type(P)$, on conclut par induction, que $M' \equiv (z\vec{Q'})[z := P_1[y := L']]$ est fortement normalisable. Ainsi on peut appliquer l'hypothèse d'induction et conclure que $M[x := P]$ est fortement normalisable. ■

Démonstration : conclusion

Théorème 6.16. *Si $\Gamma \vdash M : \tau$ alors M est fortement normalisable.*

Démonstration. Le théorème est prouvé par induction structurelle sur le terme dont on cherche à prouver la normalisation forte.

– Le terme est une variable ou une abstraction c'est clair.
– Le terme est une application $P\ Q$ alors on utilise la même astuce que dans le lemme en disant que

$$P\ Q \quad \equiv \quad (zQ)[z := P]$$

ça devient évident par le 2^{e} lemme dont les hypothèses proviennent de l'induction structurelle.
(En effet si Q est fortement normalisable alors $z\ Q$ est fortement normalisable.) ■

6.3.5 Une autre démonstration

Réductibles

Soit $\mathcal{R}^\sigma$ des ensembles de termes

$$\begin{array}{rcl} \mathcal{R}^o & = & \mathcal{SN} = \{\text{l'ensemble de fortement normalisables}\} \\ \mathcal{R}^{\sigma\to\tau} & = & \{M \mid (\forall N \in \mathcal{R}^\sigma)\ M\ N \in \mathcal{R}^\tau\} \end{array}$$

Les réductibles sont fortement normalisables

Lemme 6.17. *Pour tout* σ
- *pour tous* $M_1 \in \mathcal{SN}, \ldots, M_p \in \mathcal{SN}$ *on a* $x\ M_1 \ldots M_p \in \mathcal{R}^\sigma$,
- $\mathcal{R}^\sigma \subseteq \mathcal{SN}$.

Démonstration. Par induction sur les types.
- Si le type est o, alors clairement $x\ M_1 \ldots M_p \in \mathcal{R}^o = \mathcal{SN}$ et $\mathcal{R}^o \subseteq \mathcal{SN}$.
- Si le type est $\sigma \to \tau$, alors
  - Pour montrer que $x\ M_1 \ldots M_p \in \mathcal{R}^{\sigma\to\tau}$, il faut montrer que pour tout $N \in \mathcal{R}^\sigma$, on a $x\ M_1 \ldots M_p\ N \in \mathcal{R}^\tau$;or par induction $\mathcal{R}^\sigma \subseteq \mathcal{SN}$et donc aussi par induction $x\ M_1 \ldots M_p\ N \in \mathcal{R}^\tau$;
  - Soit $M \in \mathcal{R}^{\sigma\to\tau}$, on sait que pour tout $N \in \mathcal{R}^\sigma$ on a $M\ N \in \mathcal{R}^\tau \subseteq \mathcal{SN}$on sait que $x \in \mathcal{R}^\sigma$, donc en particulier $M\ x \in \mathcal{R}^\tau \subseteq \mathcal{SN}$, et donc $M \in \mathcal{SN}$. ■

Lemme de saturation

Lemme 6.18. *Si* $M[x := P] \in \mathcal{R}^\sigma$ *et si* $P \in \mathcal{R}^\tau$ *alors* $(\lambda x.M)\ P \in \mathcal{R}^\sigma$.

Démonstration. On voit que si $\sigma \equiv \sigma_n \to \ldots \to o$, alors

$$M \in \mathcal{R}^\sigma \quad \Leftrightarrow \quad \forall N_n \in \mathcal{R}^{\sigma_n} \ldots \forall N_1 \in \mathcal{R}^{\sigma_1}\ M\ N_n \ldots N_1 \in \mathcal{SN}.$$

Il faut donc montrer que $(\lambda x.M)\ P\ N_n \ldots N_1 \in \mathcal{SN}$ sachant que $M[x := P]\ N_n \ldots N_1 \in \mathcal{SN}$ et que $N_n \in \mathcal{R}^{\sigma_n}, \ldots, N_1 \in \mathcal{R}^{\sigma_1}, P \in \mathcal{R}^\tau$.

On raisonne par induction sur $red(P)+red(M[x := P]\ N_n \ldots N_1)$. où $red(Q)$ est la somme des longueurs de toutes les réductions qui commencent en Q. Il faut montrer que toutes les réductions de $(\lambda x.M)\ P\ N_n \ldots N_1$ sont fortement normalisables.
- Si on contracte le redex $(\lambda x.M)\ P$ alors $M[x := P]\ N_n \ldots N_1 \in \mathcal{SN}$ par hypothèse.
- Si on contracte en M' un redex dans M, on sait que $M[x := P]\ N_n \ldots N_1 \xrightarrow[\beta]{} M'[x := P]\ N_n \ldots N_1$ donc $M'[x := P]\ N_n \ldots N_1 \in \mathcal{SN}$ et de plus $red(M'[x := P]\ N_n \ldots N_1) < red(M[x := P]\ N_n \ldots N_1)$ donc par induction $(\lambda x.M')\ P\ N_n \ldots N_1 \in \mathcal{SN}$
- Même démonstration si on contracte un redex dans N_i.
- Si on contracte le redex P en P', alors $red(P') < red(P)$. $M[x := P]\ N_n \ldots N_1 \xrightarrow[\beta]{}\!\!\!\!\!\rightarrow M[x := P']\ N_n \ldots N_1$

donc $M[x := P']\ N_n \ldots N_1 \in \mathcal{SN}$, et $red(M[x := P']\ N_n \ldots N_1) \leqslant red(M[x := P]\ N_n \ldots N_1)$ par induction $(\lambda x.M)\ P'\ N_n \ldots N_1 \in \mathcal{SN}$.

Lemme d'adéquation

Lemme 6.19. *Si* $x_1 : \sigma_1, \ldots, x_n : \sigma_n \vdash M : \sigma$ *et si* $N_i \in \mathcal{R}^{\sigma_i}$ *alors* $M[x_1 := N_1, \ldots, x_n := N_n] \in \mathcal{R}^\sigma$.

Démonstration. Par induction sur M.
- Si $M = y$ avec $y \neq x_i$, alors $M[x_1 := N_1, \ldots, x_n := N_n] = y \in \mathcal{R}^\sigma$ par le lemme.
- Si $M = x_i$ alors $M[x_1 := N_1, \ldots, x_n := N_n] = N_i \in \mathcal{R}^\sigma$ par hypothèse.

– Si $M = \lambda x.M'$ et $x_1 : \sigma_1, \ldots, x_n : \sigma_n \vdash \lambda x.M' : \sigma \to \tau$ alors $x_1 : \sigma_1, \ldots, x_n : \sigma_n, x : \sigma \vdash M' : \tau$. Il faut montrer que pour tout $N \in \mathcal{R}^\sigma$, on a $(\lambda x.M')[x_1 := N_1, \ldots, x_n := N_n]\ N \in \mathcal{R}^\tau$.
D'après le lemme de saturation, il faut montrer que $M'[x_1 := N_1, \ldots, x_n := N_n, x := N] \in \mathcal{R}^\tau$.
Ce qui vient par hypothèse d'induction.
– Si $M = P\ Q$ alors
– $x_1 : \sigma_1, \ldots, x_n : \sigma_n \vdash P : \tau \to \sigma$
– et $x_1 : \sigma_1, \ldots, x_n : \sigma_n \vdash Q : \tau$,
par induction
– $P[x_1 := N_1, \ldots, x_n := N_n] \in \mathcal{R}^{\tau \to \sigma}$
– et $Q[x_1 := N_1, \ldots, x_n := N_n] \in \mathcal{R}^\tau$.
Donc $P\ Q[x_1 := N_1, \ldots, x_n := N_n] = P[x_1 := N_1, \ldots, x_n := N_n]\ Q[x_1 := N_1, \ldots, x_n := N_n] \in \mathcal{R}^\sigma$. ■

Théorème de forte normalisation

Théorème 6.20. *Si* $x_1 : \sigma_1, \ldots, x_n : \sigma_n \vdash M : \sigma$ *alors* $M \in \mathcal{SN}$.

On applique le lemme d'adéquation avec $N_i = x_i$ et on obtient $M \in \mathcal{R}^\sigma$ donc $M \in \mathcal{SN}$ puisque $\mathcal{R}^\sigma \subseteq \mathcal{SN}$.

6.3.6 Les autres connecteurs

Le $\wedge$ et le produit cartésien

Le $\wedge$ s'interprète bien calculatoirement en ajoutant des opérateurs de ***produit cartésien***.

Le ***constructeur de paires*** $\langle \_, \_ \rangle$,

Les ***destructeurs ou projections*** π^1 et π^2.

En fait, le connecteur $\wedge$ en logique correspond au produit de type $\times$.

Les règles de typage

$$\frac{\Gamma \vdash M : \sigma \times \tau}{\Gamma \vdash \pi^1\ M : \sigma} \qquad \frac{\Gamma \vdash M : \sigma \times \tau}{\Gamma \vdash \pi^2\ M : \tau}$$

$$\frac{\Gamma \vdash M : \sigma \qquad \Gamma \vdash N : \tau}{\Gamma \vdash \langle M, N \rangle : \sigma \times \tau}$$

correspondent clairement
– aux deux règles d'éliminations du $\wedge$
– et à la règle d'introduction du $\wedge$.

On a deux règles de réduction

$$\begin{array}{lcl} \pi^1\ \langle M, N \rangle & \to & M \\ \pi^2\ \langle M, N \rangle & \to & N \end{array}$$

qui correspondent à la simplification de preuve :

$$\frac{\dfrac{\mathcal{D}}{\Gamma \vdash M : \sigma} \qquad \Gamma \vdash N : \tau}{\dfrac{\Gamma \vdash \langle M, N \rangle : \sigma \times \tau}{\Gamma \vdash \pi^1 \langle M, N \rangle : \sigma}} \quad \to \quad \frac{\mathcal{D}}{\Gamma \vdash M : \sigma}$$

et la simplification symétrique.

Le $\vee$ et la somme

Le $\vee$ s'interprète comme la structure de données ***somme*** souvent notée $+$.

Les deux ***constructeurs*** in_1 et in_2,

Le ***destructeur*** ou ***discriminateur*** $case \quad of \quad in \quad | \quad$. un peu le `match` de CAML.

Les règles de typage sont

$$\frac{\Gamma \vdash M : \sigma}{\Gamma \vdash \mathsf{in}_1\ M : \sigma + \tau} \qquad \frac{\Gamma \vdash M : \tau}{\Gamma \vdash \mathsf{in}_2\ M : \sigma + \tau}$$

$$\frac{\Gamma \vdash M : \sigma + \tau \qquad \Gamma, x : \sigma \vdash P : \rho \qquad \Gamma, x : \tau \vdash Q : \rho}{\Gamma \vdash case\ M\ of\ x\ in\ P\ \mid\ Q : \rho}$$

Elles correspondent

- aux ***règles d'introduction*** du $\vee$
- et à la ***règle d'élimination*** du $\vee$.

On a les règles de réduction

$$\begin{array}{rcl} case\ (\mathsf{in}_1\ M)\ of\ x\ in\ P\ \mid\ Q & \rightarrow & P[x := M] \\ case\ (\mathsf{in}_2\ M)\ of\ x\ in\ P\ \mid\ Q & \rightarrow & Q[x := M] \end{array}$$

qui correspond à la simplification de preuve.

$$\frac{\dfrac{\dfrac{\mathcal{D}'}{\Gamma \vdash M : \sigma}}{\Gamma \vdash \mathsf{in}_1\ M : \sigma + \tau} \qquad \dfrac{\mathcal{D}}{\Gamma, x : \sigma \vdash P : \rho} \qquad \dfrac{\mathcal{D}''}{\Gamma, x : \tau \vdash Q : \rho}}{case\ M\ of\ x\ in\ P\ \mid\ Q : \rho}$$

$$\rightarrow \qquad \frac{\mathcal{D}\{\mathcal{D}'/\Gamma, x : \sigma \vdash x : \sigma\}}{\Gamma \vdash P[x := M] : \rho}$$

6.4 Logique combinatoire

6.4.1 Syntaxe et réductions

La syntaxe

Il s'agit d'une structure algébrique avec trois opérateurs.

- Un opérateur binaire l'***application***,
- Deux constantes S et K.

$$M, N \quad ::= \quad \mathsf{S} \mid \mathsf{K} \mid x \mid M\ N$$

Les termes ainsi formés sont les ***CL-termes.***

Si M et P sont deux CL-termes, on note l'application de M à P par la concaténation soit $M\ P$.

Les règles de paranthèsage sont les même que pour le λ-calcul. On écrit $MN(PQ)$ pour $(MN)(PQ)$.

Les variables

Il n'y a ***ni abstraction***, ***ni variables liées***.

Les termes clos ne contiennent ***aucune occurrence de variables***.

On peut donc parler de ***programmation sans variables.***

Les variables servent essentiellement comme marqueurs pour les substitutions.

Par exemple dans les règles de réduction.

Les règles

On définit deux règles de réduction

$$\begin{aligned} \mathsf{S}xyz &\xrightarrow[CL]{} xz(yz) \\ \mathsf{K}xy &\xrightarrow[CL]{} x \end{aligned}$$

Quelques termes

$$\begin{aligned} \mathsf{SKK}x &\xrightarrow[CL]{} \mathsf{K}x(\mathsf{K}x) \\ &\xrightarrow[CL]{} x \end{aligned}$$

On appelle très naturellement ce terme I et on retient la règle

$$\mathsf{I}x \xrightarrow[CL]{} x$$

On remarque que

$$\begin{aligned} \mathsf{SII}x &\xrightarrow[CL]{} \mathsf{I}x(\mathsf{I}x) \\ &\xrightarrow[CL]{} x\ x \end{aligned}$$

donc

$$\mathsf{SII}(\mathsf{SII}) \xrightarrow[CL]{} \mathsf{SII}(\mathsf{SII})$$

SII correspond à ω et $\mathsf{SII}(\mathsf{SII})$ correspond à Ω.

$$\begin{aligned} \mathsf{S}(\mathsf{KS})\mathsf{K}\ xyz &\xrightarrow[CL]{} \mathsf{KS}x(\mathsf{K}x)yz \\ &\xrightarrow[CL]{} \mathsf{S}(\mathsf{K}x)yz \\ &\xrightarrow[CL]{} \mathsf{K}xz(yz) \\ &\xrightarrow[CL]{} x(yz). \end{aligned}$$

Donc $\mathsf{S}(\mathsf{KS})\mathsf{K}$ équivaut à $\mathsf{B} \equiv \lambda xyz.x(yz)$.

Questions

Question 1: Quel combinateur satisfait $\mathsf{F}xy \xrightarrow[CL]{}\!\!\!\!\!\rightarrow y$?

Question 2: Que vaut

$$\mathsf{S(BBS)(KK)}?$$

$$\begin{aligned}
\mathsf{S(BBS)(KK)}xyz &\xrightarrow[CL]{} \mathsf{BBS}x(\mathsf{KK}x)yz \\
&\xrightarrow[CL]{} \mathsf{B}(\mathsf{S}x)(\mathsf{KK}x)yz \\
&\xrightarrow[CL]{} \mathsf{S}x(\mathsf{KK}xy)z \\
&\xrightarrow[CL]{} xz(\mathsf{KK}xyz) \\
&\xrightarrow[CL]{} xz(\mathsf{K}yz) \\
&\xrightarrow[CL]{} xzy
\end{aligned}$$

6.4.2 Types

Typage

On a tout d'abord :

$$\begin{aligned}
&\vdash \mathsf{S} : (\alpha \to \beta \to \gamma) \to (\alpha \to \beta) \to \alpha \to \gamma \\
&\vdash \mathsf{K} : \alpha \to \beta \to \alpha.
\end{aligned}$$

Associé à la règle

$$\frac{\vdash M : \sigma \to \tau \qquad \vdash N : \sigma}{\vdash MN : \tau}\ (App)$$

on voit qu'on a une correspondance de Curry-Howard entre la logique combinatoire et la logique minimale à la Hilbert.

On a de plus

$$\begin{aligned}
&\vdash \mathsf{I} : \alpha \to \alpha \\
&\vdash \mathsf{B} : (\alpha \to \beta) \to (\gamma \to \alpha) \to \gamma \to \beta, \\
x : \alpha \to \beta \to \gamma \ &\vdash \mathsf{S}\ x : (\alpha \to \beta) \to \alpha \to \gamma \\
\mathsf{S(BBS)(KK)} \ &\vdash (\alpha \to \beta \to \gamma) \to \beta \to \alpha \to \gamma
\end{aligned}$$

6.4.3 Correspondance avec le lambda-calcul

Des CL-termes vers les λ-termes

On peut donner une interprétation $[\![\_]\!]_\lambda$ des CL-termes vers les lambda-termes.

$$\begin{aligned}
[\![\mathsf{K}]\!]_\lambda &= \lambda xy.x \\
[\![\mathsf{S}]\!]_\lambda &= \lambda xyz.x\ z\ (y\ z) \\
[\![M_1\ M_2]\!]_\lambda &= [\![M_1]\!]_\lambda\ [\![M_2]\!]_\lambda \\
[\![x]\!]_\lambda &= x
\end{aligned}$$

Cette interprétation préserve les types.

Autrement dit

si M est un terme de preuve de σ dans la logique propositionnelle minimale à la Hilbert,
alors $[\![M]\!]_\lambda$ est un terme de preuve de σ dans la déduction naturelle pour la logique minimale.

Au niveau des preuves, cette traduction consiste à transformer une preuve à la Hilbert en une preuve en déduction naturelle en remplaçant les utilisations des axiomes $Hilbert\_S$ et $Hilbert\_K$ par leur preuve en déduction naturelle.

On n'obtient pas une preuve minimum !

Abstractions dans les CL-termes

On définit une opération d'abstraction $[x].M$ sur les CL-termes de la façon suivante.

Si $x \notin FV(M)$ alors

$$[x].M \quad = \quad \mathsf{K}M$$

sinon

$$\begin{array}{rcl} [x].(M_1\ M_2) & = & \mathsf{S}\ ([x].M_1)\ ([x].M_2) \\ [x].x & = & \mathsf{I} \end{array}$$

Exemple.

$$\begin{array}{rcl} [x].\mathsf{K} & = & \mathsf{K}\ \mathsf{K} \\ [x].\mathsf{S}\ x & = & \mathsf{S}\ ([x].\mathsf{S})\ ([x].x) \\ & = & \mathsf{S}\ (\mathsf{K}\ \mathsf{S})\ \mathsf{I} \\ [x].[y].x & = & [x].\mathsf{K}x \\ & = & \mathsf{S}\ ([x].\mathsf{K})\ ([x].x) \\ & = & \mathsf{S}\ (\mathsf{K}\ \mathsf{K})\ \mathsf{I} \end{array}$$

$$\begin{array}{rcl} [x].[y].\mathsf{K}\ x\ y & = & [x].\mathsf{S}\ ([y].(\mathsf{K}\ x))\ ([y].y) \\ & = & [x].\mathsf{S}\ (\mathsf{K}\ (\mathsf{K}\ x))\ \mathsf{I} \\ & = & \mathsf{S}\ ([x].\mathsf{S})\ ([x].(\mathsf{K}\ (\mathsf{K}\ x))\ \mathsf{I}) \\ & = & \mathsf{S}\ (\mathsf{K}\ \mathsf{S})\ (\mathsf{S}\ ([x].(\mathsf{K}\ (\mathsf{K}\ x)))\ ([x].\mathsf{I}) \\ & = & \mathsf{S}\ (\mathsf{K}\ \mathsf{S})\ (\mathsf{S}\ (\mathsf{S}([x].\mathsf{K})\ ([x].(\mathsf{K}\ x))\ (\mathsf{K}\ \mathsf{I}) \\ & = & \mathsf{S}\ (\mathsf{K}\ \mathsf{S})\ (\mathsf{S}\ (\mathsf{S}(\mathsf{KK})\ (\mathsf{S}\ (\mathsf{K}\ \mathsf{K})\ \mathsf{I}))\ (\mathsf{K}\ \mathsf{I}) \end{array}$$

Typage des abstractions

Proposition 6.21. *Si* $x : \sigma, \Gamma \vdash M : \tau$ *alors* $\Gamma \vdash [x].M : \sigma \to \tau$.

Démonstration. Par induction sur la structure de M.

- si $x \notin FV(M)$ alors $\Gamma \vdash \mathsf{K}M : \sigma \to \tau$ pour n'importe quel σ.
- si $x \in FV(M)$ et $M \equiv M_1\ M_2$ alors par induction $x : \sigma, \Gamma \vdash M_1 : \rho \to \tau$ et $x : \sigma, \Gamma \vdash M_2 : \rho$ et $\Gamma \vdash [x].M_1 : \sigma \to \rho \to \tau$ et $\Gamma \vdash [x].M_2 : \sigma \to \rho$. On prend $\mathsf{S} : (\sigma \to \rho \to \tau) \to (\sigma \to \rho) \to \sigma \to \tau$. Par conséquent $\Gamma \vdash \mathsf{S}\ [x].M_1\ [x].M_2 : \sigma \to \tau$. C.Q.F.D.
- si $x \in FV(M)$ et $M \equiv x$ alors $\Gamma \vdash \mathsf{I} : \sigma \to \sigma$. ■

Réduction

Proposition 6.22. $([x].M)\ N \xrightarrow[CL]{}\!\!\!\!\!\rightarrow M[x := N]$

Démonstration. Par induction sur la définition de $[x].M$.

– si $x \notin FV(M)$ alors

$$\begin{array}{rcl} ([x].M)\ N & \equiv & \mathsf{K}\ M\ N \\ & \xrightarrow[CL]{} & M[x := N]. \end{array}$$

– si $x \in FV(M)$ et $M \equiv x$ alors $[x].M \equiv I$
et $([x].M)\ N \xrightarrow[CL]{} N = x[x := N]$.

– si $x \in FV(M)$ et $M \equiv M_1\ M_2$ alors par induction

$$\begin{array}{rcl} ([x].M_1\ M_2)\ N & = & \mathsf{S}\ ([x].M_1)\ ([x].M_2)\ N \\ & \xrightarrow[CL]{} & (([x].M_1)\ N)\ (([x].M_2)\ N) \\ & \xrightarrow[CL]{}\!\!\!\!\!\rightarrow & (M_1[x := N])\ (M_2[x := N]) \\ & = & (M_1\ M_2)[x := N]. \end{array}$$

■

Des λ-termes vers les CL-termes

On peut donner une interprétation $[\![\_]\!]_{CL}$ des lambda-termes vers les CL-termes.

$$\begin{array}{rcl} [\![\lambda x.M]\!]_{CL} & = & [x].[\![M]\!]_{CL} \\ [\![M_1\ M_2]\!]_{CL} & = & [\![M_1]\!]_{CL}\ [\![M_2]\!]_{CL} \\ [\![x]\!]_{CL} & = & x \end{array}$$

On a $M \xrightarrow[\beta]{} N$ implique $[\![M]\!]_{CL} \xrightarrow[CL]{}\!\!\!\!\!\rightarrow [\![N]\!]_{CL}$.

Cette interprétation préserve les types.

Autrement dit

si M est un terme de preuve de σ dans la déduction naturelle de la logique propositionnelle minimale
alors $[\![M]\!]_{CL}$ est un terme de preuve de σ dans la logique propositionnelle minimale à la Hilbert.

La taille de $[\![M]\!]_{CL}$ est en $O(3^n)$ où n est la taille de M.

Clairement, $[\![[\![M]\!]_\lambda]\!]_{CL}$ n'est pas en général égal à M.

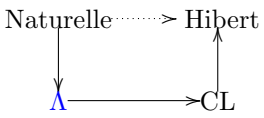
Ainsi,

$$\begin{array}{rcl} [\![[\![K]\!]_\lambda]\!]_{CL} & = & [\![\lambda x \lambda y.x]\!]_{CL} \\ & = & [x].[y].x \\ & = & \mathsf{S}\ (\mathsf{K}\ \mathsf{K})\ \mathsf{I}. \end{array}$$

De la déduction naturelle à la logique à la Hilbert

Corollaire : Toute preuve en déduction naturelle d'une proposition de la logique minimale peut être traduite en une preuve de la même proposition en logique à la Hilbert.

Il suffit de traduire le terme associé à la preuve en déduction naturelle en un CL-terme en logique combinatoire et d'en extraire la preuve en logique à la Hilbert.



Chapitre 7

Modèles de Kripke

Notations

À partir de maintenant, je note

1. les propositions $\varphi, \psi, \chi, \theta$ etc.
2. les variables propositionnelles p, q, r, s, t,
3. les environnements Γ, Θ, Σ

Les modèles de Kripke (cas général)

Un ***modèle de Kripke*** est un triplet $\mathcal{M} = (\mathcal{U}_\mathcal{M}, \mathcal{I}_\mathcal{M}, \mathcal{R}_\mathcal{M})$ où

- $\mathcal{U}_\mathcal{M}$ est un ensemble dont les éléments sont appelés, suivant les auteurs,
  - des ***mondes***,
  - des ***mondes possibles***,
  - des ***étapes (de raisonnement)***,
  - des ***états***.
- $\mathcal{I}_\mathcal{M} : Variables \to \mathcal{P}(\mathcal{U}_\mathcal{M})$. Intuitivement $\mathcal{I}_\mathcal{M}(p)$ est l'ensemble des mondes où la variable p est satisfaite.

Les mondes sont notés u, v, w.

- $\mathcal{R}_\mathcal{M} = (R_1, ..R_n)$ est un ensemble de relations dites ***relations d'accessibilité***.Si $u\, R_i\, v$ alors le monde v est accessible à partir de u pour i[1].

Les propriétés (transitivité, réflexivité, symétrie ou antisymétrie) des relations R_i jouent un rôle.

$\mathcal{I}_\mathcal{M}$ doit satisfaire des propriétés de compatibilité avec les R_i.

Les modèles de Kripke (cas propositionnelle intuitionniste)

1. Il n'y a qu'une relation notée $\leqslant_\mathcal{M}$, qui est un ordre, c-à-d réflexive, antisymétrique et transitive.
2. $\mathcal{I}_\mathcal{M}$ est ***dirigé***, c'est-à-dire que pour toute variable propositionnelle p, si $u \in \mathcal{I}_\mathcal{M}(p)$ et $u \leqslant_\mathcal{M} v$ alors $v \in \mathcal{I}_\mathcal{M}(p)$.

Forçage

On définit sur $\mathcal{U}_\mathcal{M}$ une relation dite de ***forçage*** ou de *réalisabilité* qui s'écrit[2] :

[1] On verra plus tard ce que ça signifie.

[2] parfois aussi notée $\mathcal{M}, u \vDash \varphi$

- $\mathcal{M}, u \Vdash \varphi$
- ou $u \Vdash_{\mathcal{M}} \varphi$
- ou $u \Vdash \varphi$ s'il n'y a pas d'ambiguïtés sur $\mathcal{M}$.

1. Si φ est une ***variable*** p :
   $\mathcal{M}, u \Vdash \varphi$ si et seulement si $u \in \mathcal{I}_{\mathcal{M}}(p)$
2. Si φ est une ***conjonction*** $\psi \wedge \theta$:
   $\mathcal{M}, u \Vdash \varphi$ si et seulement si $\mathcal{M}, u \Vdash \psi$ et $\mathcal{M}, u \Vdash \theta$
3. Si φ est une ***disjonction*** $\psi \vee \theta$:
   $\mathcal{M}, u \Vdash \varphi$ si et seulement si $\mathcal{M}, u \Vdash \psi$ ou $\mathcal{M}, u \Vdash \theta$
4. Si φ est une ***implication*** $\psi \Rightarrow \theta$:
   $\mathcal{M}, u \Vdash \varphi$ si et seulement si pour tout $v \geqslant_M u$ si $\mathcal{M}, v \Vdash \psi$ alors $\mathcal{M}, v \Vdash \theta$
5. Si $\bot$ est l'***absurde***, alors $\mathcal{M}, u \nVdash \bot$.

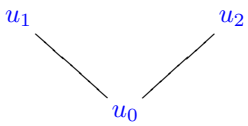
Monotonie du forçage

Proposition 7.1. *$\Vdash_{\mathcal{M}}$ est monotone.*
Si $\mathcal{M}, u \Vdash \varphi$ et $u \leqslant_{\mathcal{M}} v$ alors $\mathcal{M}, v \Vdash \varphi$

En exercice !
Donc pour tout φ, l'ensemble $\{u \in \mathcal{U}_{\mathcal{M}} \mid u \Vdash \varphi\}$ est dirigé.

Exercice

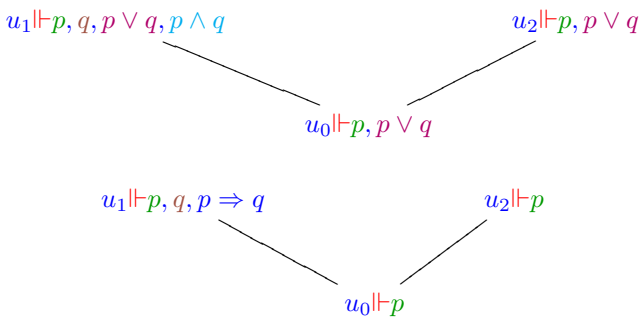
Soit le modèle de Kripke $\mathcal{A}$:



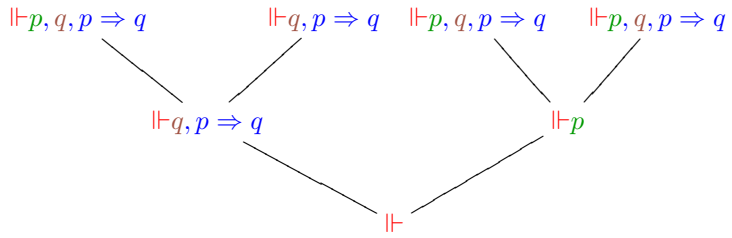
où $u_0 \Vdash p$ et $u_1 \Vdash q$.

1. Donnez les valeurs de $\mathcal{I}_{\mathcal{A}}$ pour p et q.
2. Annotez les mondes qui forcent $p \vee q$, $p \wedge q$, $p \Rightarrow q$

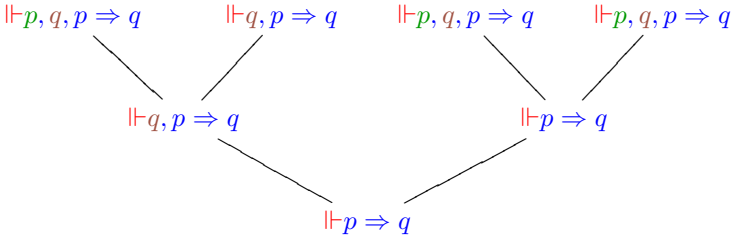
Solution de l'exercice



Un autre exemple



Encore un autre exemple



Quelques définitions

1. $\mathcal{M} \vDash \varphi$ se lit $\mathcal{M}$ ***modélise*** φ, φ ***est valide dans*** $\mathcal{M}$ et signifie : pour tout $u \in \mathcal{M}$, on a $\mathcal{M}, u \Vdash \varphi$.
2. $\vDash \varphi$ se lit φ ***est valide*** et signifie pour tout modèle de Kripke $\mathcal{M}$, on a $\mathcal{M} \vDash \varphi$.

7.1 Théorème de correction

Théorème 7.2 (de correction). *Si* $\vdash \varphi$ *alors* $\vDash \varphi$.

On a besoin d'une définition.

Définition. $\Gamma \vDash \varphi$ où $\Gamma \equiv \{\varphi_1, \ldots, \varphi_n\}$ signifie que pour tout modèle $\mathcal{M}$ et tout $u \in \mathcal{U}_\mathcal{M}$,

$$u \Vdash_\mathcal{M} \varphi_1, \ldots, u \Vdash_\mathcal{M} \varphi_n \text{ implique } u \Vdash_\mathcal{M} \varphi.$$

Démonstration. La démonstration se fait par induction sur la structure de l'arbre de preuve de $\Gamma \vdash \varphi$.

On fixe le modèle $\mathcal{M}$ dans la preuve.
On suppose que pour tout u, on a $u \Vdash_\mathcal{M} \varphi_1, \ldots, u \Vdash_\mathcal{M} \varphi_n$.
On cherche à montrer que $u \Vdash_\mathcal{M} \varphi$.

- L'arbre est réduit à une feuille. Alors $\varphi \in \Gamma$ et comme $u \Vdash_\mathcal{M} \varphi_1, \ldots, u \Vdash_\mathcal{M} \varphi_n$, on a $u \Vdash_\mathcal{M} \varphi$
- Le nœud de la racine est la règle $\Rightarrow I$ et donc le jugement est $\Gamma \vdash \psi \Rightarrow \theta$.
  Par induction il existe un arbre de preuve pour $\Gamma, \psi \vdash \theta$.
  L'hypothèse d'induction nous dit que pour n'importe quel monde w, si $w \Vdash \varphi_1, \ldots, w \Vdash \varphi_n, w \Vdash \psi$ alors $w \Vdash \theta$.
  Considérons maintenant un monde u tel que $u \Vdash \varphi_1, \ldots, u \Vdash \varphi_n$.

Si v est monde tel que $u \leqslant_{\mathcal{M}} v$ et $v \Vdash \psi$.
Par monotonie, $v \Vdash \varphi_1, \ldots, v \Vdash \varphi_n$. On peut donc appliquer l'hypothèse de récurrence à v et l'on a $v \Vdash \theta$.
Par la définition de $\Vdash$ sur $\varphi \equiv \psi \Rightarrow \theta$ cela donne $u \Vdash \varphi$.

– Le nœud de la racine est la règle $\Rightarrow E$
On a donc deux arbres de preuve pour $\Gamma \vdash \psi$ et $\Gamma \vdash \psi \Rightarrow \varphi$.
Soit u tel que

$$u \Vdash \varphi_1, \ldots, u \Vdash \varphi_n.$$

alors par hypothèse d'induction d'une part $u \Vdash \psi$ d'autre part $u \Vdash \psi \Rightarrow \varphi$.
Par définition de $u \Vdash \psi \Rightarrow \varphi$, on a $u \Vdash \varphi$.

– Le nœud de la racine est la règle $\bot$.
Si $u \Vdash \psi$ (pour tout $\psi \in \Gamma$) alors $u \Vdash \bot$, mais on sait que ça n'est pas possible, donc chaque fois qu'on a $u \Vdash \psi$ (pour tout $\psi \in \Gamma$), on aussi $u \Vdash \varphi$, donc $\Gamma \vDash \varphi$.

– Le nœud de la racine est la règle $\vee I_g$ avec $\Gamma \vdash \theta \vee \chi$.
L'hypothèse d'induction dit que pour tout $u \in \mathcal{U}_{\mathcal{M}}$
– si pour tout $\psi \in \Gamma$ on a $u \Vdash \psi$ alors $u \Vdash \theta$,
donc aussi $u \Vdash \theta \vee \chi$.

– Le nœud de la racine est la règle $\vee E$ avec comme prémisses
$\Gamma \vdash \varphi \vee \psi$, $\Gamma, \varphi \vdash \theta$ et $\Gamma, \psi \vdash \theta$; et comme conclusion $\Gamma \vdash \theta$.
Considérons les u qui satisfont $u \Vdash \chi$ pour $\chi \in \Gamma$. L'hypothèse d'induction nous dit que pour ces u, on doit avoir $u \Vdash \varphi \vee \psi$.
Si de plus $u \Vdash \varphi$ alors $u \Vdash \theta$. Et si de plus $u \Vdash \psi$ alors $u \Vdash \theta$ aussi.
Mais comme on sait que $u \Vdash \varphi$ ou $u \Vdash \psi$ alors dans tous les cas $u \Vdash \theta$. ■

Exercice

$\mathcal{I}_{\mathcal{M}} p = \{u_1\}$. Donc $u_1 \Vdash p$ et $u_0 \nVdash p$.

On sait que $u \Vdash \varphi \Rightarrow \bot$ ssi $(\forall v :)\ v \geqslant_{\mathcal{M}} u \Rightarrow v \nVdash \varphi$.
Donc $u \nVdash \varphi \Rightarrow \bot$ ssi $(\exists v \in \mathcal{U}_{\mathcal{M}})\ v \geqslant_{\mathcal{M}} u \quad \& \quad v \Vdash \varphi$.
Par conséquent, $u_0 \nVdash p \Rightarrow \bot$.

D'où il vient que $u_0 \nVdash p \vee p \Rightarrow \bot$.

Donc $\mathcal{M} \nVdash p \vee \neg p$ Donc $\nVdash p \vee \neg p$.

Donc par le ***théorème de correction*** $\nvdash p \vee \neg p$.

Le ***tiers exclus*** n'est pas prouvable dans le logique intuitionniste.

7.2 Théorème de complétude

On se restreint au connecteurs $\vee$ et $\Rightarrow$.
Un ensemble Γ de propositions est ***stable par sous terme*** (ou sous-formule) si quand Γ contient φ il contient toutes les propositions qui sont des sous-termes de φ.

7.2.1 Réduction des modèles finis aux modèles infinis

Soient $\mathbf{K}$ un modèle de Kripke et Γ un ensemble fini de propositions stable par sous-terme.

Nous associons à $\mathbf{K}$ un modèle de Kripke fini $\mathbf{K}_\Gamma = (U_\Gamma, \leqslant_\Gamma, \mathcal{I}_\Gamma)$ comme suit.

Pour chaque $u \in U$,

- $[u] = \{\varphi \in \Gamma \mid u \Vdash \varphi\}$
- et $U_\Gamma = \{[u] \mid u \in U\}$.

L'ordre $\leqslant_\Gamma$ est l'ordre d'inclusion des sous-ensembles de propositions. Par définition $\mathcal{I}_\Gamma(p) = \{[u] \mid p \in [u]\}$. On dit que $\mathbf{K}_\Gamma$ est obtenu par ***filtration*** à partir de $\mathbf{K}$.

U_Γ est fini. $\mathcal{I}_\Gamma$ est dirigé pour $\leqslant_\Gamma$ qui est aussi $\subseteq$.

Proposition 7.3. *Les deux conditions suivantes sont équivalentes :*

1. $[u] \Vdash_{\boldsymbol{K}_\Gamma} \varphi$,
2. $u \Vdash_{\boldsymbol{K}} \varphi$ *(autrement dit dans ce cas* $\varphi \in [u]$*).*

$\vDash \varphi$ si et seulement si $\mathbf{K} \vDash \varphi$ pour tous les modèles $\mathbf{K}$ finis.

7.2.2 Ensembles premiers

Définition d'un ensemble premier

Un ensemble de propositions Δ est ***premier*** s'il satisfait les deux conditions :

- Δ est clos par $\vdash$,
- si $\psi \vee \chi \in \Delta$ alors ou bien $\psi \in \Delta$, ou bien $\chi \in \Delta$.

Construction d'un premier tel que $\Gamma' \nvdash \varphi$

Soient Γ un ensemble de propositions et φ une proposition telle $\Gamma \nvdash \varphi$, on veut construire un ensemble Γ' premier tel que

- $\Gamma' \supseteq \Gamma$
- et tel que $\Gamma' \nvdash \varphi$.

On ordonne les propositions disjonctives en une suite $(\psi_1 \vee \chi_1, \dots, \psi_n \vee \chi_n, \dots)$.

On construit la suite Γ_k. $\Gamma_0 \triangleq \Gamma$.

Supposons construit Γ_k avec $\Gamma_k \nvdash \varphi$. Considérons la première proposition de la suite ci-dessus telle que $\Gamma_k \vdash \psi_{n_k} \vee \chi_{n_k}$ et $\Gamma_k \nvdash \psi_{n_k}$ et $\Gamma_k \nvdash \chi_{n_k}$.

On n'a pas à la fois $\Gamma_k, \psi_{n_k} \vdash \varphi$ et $\Gamma_k, \chi_{n_k} \vdash \varphi$.

On peut donc définir

$$\Gamma_{k+1} := \begin{cases} \Gamma_k \cup \{\psi_{n_k}\} \text{ si } \Gamma_k, \psi_{n_k} \nvdash \varphi \\ \Gamma_k \cup \{\chi_{n_k}\} \text{ dans les autres cas.} \end{cases}$$

et

$$\Gamma' = \bigcup_{k \geqslant 0} \Gamma_k$$

- $\Gamma' \nvdash \varphi$,
- Γ' est premier.

Proposition 7.4. Γ' *est premier.*

Démonstration. Soit $\varphi \vee \chi \in \Gamma'$. Soit k le plus petit entier tel que $\Gamma_k \vdash \varphi \vee \chi$. Clairement,

- $\varphi \vee \chi$ n'a pas été examiné avant l'étape k,
- et $\Gamma_h \vdash \varphi \vee \chi$, pour $h \geqslant k$.

Donc $\varphi \vee \chi$ a été examiné à une étape $h \geqslant k$ et ainsi
- $\varphi \in \Gamma_h$ ou $\chi \in \Gamma_h$,
- donc $\varphi \in \Gamma'$ ou $\chi \in \Gamma'$.

■

7.2.3 La complétude

L'objectif

Supposons $\Gamma \nvdash \varphi$.
On va construire
- un modèle de Kripke $\mathbf{K} = (U, \leqslant, \mathcal{I})$
- et un monde u *minimum* dans U tels que $u \Vdash \Gamma$ et $u \not\Vdash \varphi$.

Soit Γ' un ensemble premier de propositions tel que
- $\Gamma' \supseteq \Gamma$
- et $\Gamma' \nvdash \varphi$.

La construction

U est l'ensemble des suites finies d'entiers ordonnées par l'ordre préfixe
ε est la suite vide.
Un monde $\alpha \in U$ est une suite finie d'entiers $\alpha \equiv a_1 \dots a_p$.
On construit le modèle $\mathbf{K}$ et des ensembles $\Gamma(\alpha)$ associés à chaque suite d'entiers α.
- cas ε. $\Gamma(\varepsilon) = \Gamma'$.
- cas αi. Soit une suite $((\sigma_0, \tau_0), (\sigma_1, \tau_1), \dots, (\sigma_n, \tau_n), \dots,)$ énumérant tous les (σ_i, τ_i) tels que $\Gamma(\alpha), \sigma_i \nvdash \tau_i$. On peut construire un ensemble premier $\Gamma(\alpha i)$ tel que $\sigma_i \in \Gamma(\alpha i)$ et $\Gamma(\alpha i) \nvdash \tau_i$. Pourquoi ?

Par définition, $\alpha \in \mathcal{I}(p)$ si et seulement si $p \in \Gamma(\alpha)$.
On a besoin d'un lemme qui s'énonce :

Lemme 7.5. *Supposons que*

$$(\forall \beta \in \mathbb{N}^*)\ \beta \Vdash \psi_1 \quad \Leftrightarrow \quad \Gamma(\beta) \vdash \psi_1 \qquad (H_1)$$

et

$$(\forall \beta \in \mathbb{N}^*)\ \beta \Vdash \psi_2 \quad \Leftrightarrow \quad \Gamma(\beta) \vdash \psi_2 \qquad (H_2)$$

Alors $\alpha \Vdash \psi_1 \Rightarrow \psi_2$ *implique* $\Gamma(\alpha) \vdash \psi_1 \Rightarrow \psi_2$

Démonstration. Supposons $\Gamma(\alpha) \nvdash \psi_1 \Rightarrow \psi_2$
Soit k l'entier correspondant au couple $(\psi_i, \psi_1 \Rightarrow \psi_2)$ dans la construction des $\Gamma(\alpha\ i)$.

1. $\Gamma(\alpha\ k) \ni \psi_1$
2. $\Gamma(\alpha\ k) \nvdash \psi_1 \Rightarrow \psi_2$
3. donc de 1. et 2. on déduit $\Gamma(\alpha\ k) \nvdash \psi_2$.

De (H_1) et 1. on déduit $\alpha\ k \Vdash \psi_1$. De (H_2) et 3. on déduit $\alpha\ k \not\Vdash \psi_2$.
Donc $\alpha \not\Vdash \psi_1 \Rightarrow \psi_2$. ■

Proposition 7.6. $\alpha \Vdash \psi$ *si et seulement si* $\Gamma(\alpha) \vdash \psi$.

La démonstration se fait par induction sur la structure de ψ en utilisant le lemme.
On peut prouver que
- $\alpha \Vdash \psi$ si et seulement si $\Gamma(\alpha) \vdash \psi$.

On en déduit
- que $\varepsilon \Vdash \psi$ (pour chaque $\psi \in \Gamma$)
- et que $\varepsilon \nVdash \varphi$.

Le résultat

On a montré que si $\Gamma \nvdash \varphi$ alors $\Gamma \nvDash \varphi$

On conclut :

Théorème 7.7. *Si* $\vDash \varphi$ *alors* $\vdash \varphi$.

Chapitre 8

Calcul des prédicats

8.1 Les structures

Structures

Une ***structure*** est un triplet $\mathfrak{A} = \langle A, \mathbf{P}, \mathbf{F}, \{c_i \in I\}\rangle$ où
- A est un ensemble non vide (le ***support*** ou l'***univers*** de la structure),
- $\mathbf{P}$ est un n-uple $P_1, \ldots, P_n$ de prédicats,
- $\mathbf{F}$ est un m-uple $F_1, \ldots, F_m$ de fonctions totales,
- les c_i sont des éléments de A (les ***constantes***).

Exemples

Exemples.
- $\langle \mathbb{R}, +, \cdot, ^{-1}, 0, 1\rangle$ est le corps des réels,
- $\langle \mathbb{N}, <\rangle$ est l'ensemble ordonné des naturels.

Le type de similarité

Le ***type de similarité*** d'une structure $\mathfrak{A} = \langle A, R_1, \ldots R_n, F_1, \ldots, F_m, \{c_i \in I\}\rangle$ est la suite $\langle r_1, \ldots, r_n; a_1, \ldots, a_m, \kappa\rangle$ où
- $R_i \subseteq A^{r_i}$,
- $F_j : A^{a_j} \to A$,
- $\kappa = |\{c_i \in I\}|$ (le cardinal de I).

Chaque structure contient la relation binaire d'***identité*** qui est notée $=$.

Exemples

Exemples.
- $\langle \mathbb{R}, +, \cdot, ^{-1}, 0, 1\rangle$ a pour type de similarité $\langle -; 2, 2, 1; 2\rangle$,
- $\langle \mathbb{N}, <\rangle$ a pour type de similarité $\langle 2; -; 0\rangle$.

8.2 La syntaxe

La syntaxe

Supposons que l'on a un langage de type de similarité $\langle r_1, \ldots, r_n; a_1, \ldots, a_m, \kappa\rangle$.

Les entités syntaxiques sont

1. les ***symboles de prédicats*** $R_1, \ldots, R_n, Q, R, \doteq$,
2. les ***symboles de fonctions*** $f_1, \ldots, f_m$,

3. les ***symboles de constantes*** $\overline{c}_i$ pour $i \in I$,
4. les ***variables*** $x_0, x_1, x_2, \ldots$
5. les ***connecteurs*** $\vee, \wedge, \Rightarrow, \Leftrightarrow, \bot, \forall, \exists$

Les ***termes*** sont

$$t, t' \quad ::= \quad \overline{c}_i \,|\, x_j \,|\, f(t, \ldots, t)$$

Les ***formules*** sont

$$\begin{array}{lll} \varphi, \psi & ::= & \bot \,|\, P(t, \ldots, t) \,|\, t \doteq t' \qquad\qquad \textbf{\textit{Les atomes}} \\ & & |\, \varphi \vee \psi \,|\, \varphi \wedge \psi \,|\, \varphi \Rightarrow \psi \,|\, \varphi \Leftrightarrow \psi \,|\, \neg\varphi \,|\, (\forall x_i)\varphi \,|\, (\exists x_i)\varphi \end{array}$$

Les notions de ***variables libres***, de ***variables liées***, de ***formules closes*** sont les mêmes qu'en lambda-calcul, sauf qu'ici les lieurs sont $\forall$ et $\exists$

Les formules closes sont appelées des ***sentences***.

Parenthèses et priorités

Les conventions sur les parenthèses sont les suivantes.

- On omet les parenthèses les plus externes.
- On enlève les parenthèses dans les négations.
- $\vee$ et $\wedge$ ont priorité sur $\Rightarrow$ et $\Leftrightarrow$.
- $\neg$ a priorité sur tout autre opérateur.
- On enlève les parenthèses autour des quantifications $\forall x$ et $\exists x$ chaque fois que c'est possible.
- Les quantificateurs ont priorité sur tous les connecteurs logiques.
- On fusionne les listes de quantificateurs identiques $\exists x_1 x_2 \forall x_3 x_4 x_5 \varphi$ au lieu de $\exists x_1 \exists x_2 \forall x_3 \forall x_4 \forall x_5 \varphi$.

Le cas du signe $=$

On peut vouloir utiliser le symbole $=$ à la fois dans la théorie est la méta-théorie. Pour faire la différence on emploie souvent

- $\equiv$ pour l'égalité syntaxique des expressions dans la métathéorie,
- $=$ comme symbole d'égalité dans la structure.
- et $\doteq$ comme symbole d'égalité du langage de la théorie,

Nous accepterons l'utilisation de $=$ à la place de $\doteq$ quand il n'y aura pas de confusion possible.

Substitutions de termes dans les termes

- $x[x := t] = t$
- $y[x := t] = y$
- $\overline{c}[x := t] = \overline{c}$
- $f(t_1, \ldots, t_p)[x := t] = f(t_1[x := t], \ldots, t_p[x := t])$

Substitutions de termes dans les formules

On applique la convention de Barendregt

- $\bot[x := t] \quad = \quad \bot$
- $P[x := t] \quad = \quad P$
- $(t_1 \doteq t_2)[x := t] \quad = \quad (t_1[x := t] \doteq t_2[x := t]$
- $P(t_1, \ldots, t_p)[x := t] \quad = \quad P(t_1[x := t], \ldots, t_p[x := t])$

- $(\varphi \Box \gamma)[x := t] \quad = \quad \varphi[x := t] \Box \gamma[x := t]$
- $(\neg\varphi)[x := t] \quad = \quad \neg(\varphi[x := t])$
- $(\forall y\varphi)[x := t] \quad = \quad \forall y(\varphi[x := t])$
- $(\exists y\varphi)[x := t] \quad = \quad \exists y(\varphi[x := t])$

Convention

Parfois pour mettre en évidence que x peut apparaître dans φ on écrit $\varphi(x)$. Au lieu de $\varphi(x)[x := t]$, on écrit alors $\varphi(t)$.

Le langage étendu

Le ***langage étendu*** $L(\mathfrak{A})$ de $\mathfrak{A}$ est obtenu en ajoutant au langage L du type de similarité de $\mathfrak{A}$ des symboles de constantes pour tous les éléments de A (le support de $\mathfrak{A}$).

Substitutions de formules dans les formules

Pas difficile !

8.3 La sémantique

Un exemple

Considérons la structure $\mathfrak{Z} = \langle \mathbb{Z}, <, +, -, 0 \rangle$.

Le langage a son alphabet

- des ***symboles de prédicats*** $\doteq, L$,
- des ***symboles de fonctions*** P, M,
- des ***symboles de constantes*** $\overline{0}$.

$L(\mathfrak{Z})$ contient de plus un symbole de constante $\overline{m}$ pour chaque $m \in \mathbb{Z}$.

Interprétation des termes dans $\mathfrak{Z}$

L'interprétation $t^{\mathfrak{Z}}$ de chaque terme t de $L(\mathfrak{Z})$ est un élément de $\mathbb{Z}$.

t	$t^{\mathfrak{Z}}$
$\overline{m}$	m
$P(t_1, t_2)$	$t_1^{\mathfrak{Z}} + t_2^{\mathfrak{Z}}$
$M(t)$	$-t^{\mathfrak{Z}}$

Grosso modo, on interprète

- m par «son nombre»,
- P par ***plus***
- et M par ***moins***.

Interprétation des sentences dans $\mathfrak{Z}$

$$
\begin{array}{lcl}
[\![\bot]\!]_{\mathfrak{Z}} & = & 0 \\
[\![t \doteq s]\!]_{\mathfrak{Z}} & = & \begin{cases} 1 \text{ si } t^{\mathfrak{Z}} = s^{\mathfrak{Z}} \\ 0 \text{ sinon} \end{cases} \\
[\![L(t,s)]\!]_{\mathfrak{Z}} & = & \begin{cases} 1 \text{ si } t^{\mathfrak{Z}} < s^{\mathfrak{Z}} \\ 0 \text{ sinon} \end{cases}
\end{array}
$$

$$\begin{array}{rcl}
[\![\varphi \wedge \psi]\!]_3 & = & min([\![\varphi]\!]_3, [\![\psi]\!]_3) \\
[\![\varphi \vee \psi]\!]_3 & = & max([\![\varphi]\!]_3, [\![\psi]\!]_3) \\
[\![\varphi \Box \psi]\!]_3 & = & \textit{(comme d'habitude)} \\
[\![\forall x \varphi]\!]_3 & = & min\,\{[\![\varphi[x := \overline{n}]]\!]_3 \mid n \in \mathbb{Z}\} \\
[\![\exists x \varphi]\!]_3 & = & max\,\{[\![\varphi[x := \overline{n}]]\!]_3 \mid n \in \mathbb{Z}\}
\end{array}$$

On voit que $[\![\forall x\varphi]\!]_{\mathfrak{A}}$ prend la valeur 1 si toutes les instances de $[\![\varphi]\!]_{\mathfrak{A}}$ prennent la valeur 1.

C'est une généralisation de $\wedge$.

De même $[\![\exists x\varphi]\!]_{\mathfrak{A}}$ est une généralisation de $\vee$.

Quand il n'y aura pas de confusion on écrira $[\![\varphi]\!]$ au lieu de $[\![\varphi]\!]_{\mathfrak{A}}$.

Interprétation des termes

Considérons $\mathfrak{A} = \langle A, P_1, \ldots P_n, F_1, \ldots, F_m, \{c_i \in I\}\rangle$ de type de similarité $\langle r_1, \ldots, r_n; a_1, \ldots, a_m, |I|\rangle$

On définit la fonction $(\cdot)^{\mathfrak{A}}$: $\mathsf{termes}_{\mathfrak{A}} \to A$

$$\begin{array}{rcl}
\overline{c_i}^{\mathfrak{A}} & = & c_i \\
\overline{a}^{\mathfrak{A}} & = & a \\
(\overline{F_i}(t_1, \ldots t_p))^{\mathfrak{A}} & = & F_i(t_1^{\mathfrak{A}}, \ldots, t_p^{\mathfrak{A}}).
\end{array}$$

où $\overline{F_i}$ est le symbole correspondant à la fonction F_i et où $p = a_i$.

Interprétation des sentences

$$\begin{array}{rcl}
[\![\bot]\!]_{\mathfrak{A}} & = & 0 \\
[\![\overline{R}]\!]_{\mathfrak{A}} & = & R \\
[\![\overline{R_i}(t_1, \ldots t_p)]\!]_{\mathfrak{A}} & = & \left\{ \begin{array}{ll} 1 \text{ si } \langle t_1^{\mathfrak{A}}, \ldots, t_p^{\mathfrak{A}}\rangle \in R_i & \text{où } p = r_i \\ 0 \text{ sinon} & \end{array} \right. \\
[\![t_1 \doteq t_2]\!]_{\mathfrak{A}} & = & \left\{ \begin{array}{l} 1 \text{ si } t_1^{\mathfrak{A}} = t_2^{\mathfrak{A}} \\ 0 \text{ sinon} \end{array} \right.
\end{array}$$

$$\begin{array}{rcl}
[\![\varphi \wedge \psi]\!]_{\mathfrak{A}} & = & min([\![\varphi]\!]_{\mathfrak{A}}, [\![\psi]\!]_{\mathfrak{A}}) \\
[\![\varphi \vee \psi]\!]_{\mathfrak{A}} & = & max([\![\varphi]\!]_{\mathfrak{A}}, [\![\psi]\!]_{\mathfrak{A}}) \\
[\![\varphi \Rightarrow \psi]\!]_{\mathfrak{A}} & = & max(1 - [\![\varphi]\!]_{\mathfrak{A}}, [\![\psi]\!]_{\mathfrak{A}}) \\
[\![\varphi \Leftrightarrow \psi]\!]_{\mathfrak{A}} & = & \left\{ \begin{array}{l} 1 \text{ si } [\![\varphi]\!]_{\mathfrak{A}} = [\![\psi]\!]_{\mathfrak{A}} \\ 0 \text{ sinon} \end{array} \right. \\
[\![\neg\varphi]\!]_{\mathfrak{A}} & = & 1 - [\![\varphi]\!]_{\mathfrak{A}} \\
[\![\forall x \varphi]\!]_{\mathfrak{A}} & = & min\{[\![\varphi[x := \overline{a}]]\!]_{\mathfrak{A}} \mid a \in A\} \\
[\![\exists x \varphi]\!]_{\mathfrak{A}} & = & max\{[\![\varphi[x := \overline{a}]]\!]_{\mathfrak{A}} \mid a \in A\}
\end{array}$$

À partir de maintenant, nous supposerons que toutes les structures ont les mêmes types de similarité.

On écrira $\mathfrak{A} \vDash_K \varphi$ pour $[\![\varphi]\!]_{\mathfrak{A}} = 1$.

Cela se lira la structure $\mathfrak{A}$ valide la sentence φ ou bien la sentence φ est valide dans la structure $\mathfrak{A}$

Interprétation des formules

Si $FV(\varphi) = \{z_1, \dots z_k\}$, la ***clôture universelle*** de φ est

$$Cl(\varphi) = \forall z_1 \dots z_k \varphi.$$

$\mathfrak{A} \vDash_K \varphi$ ssi $\mathfrak{A} \vDash_K Cl(\varphi)$.
$\vDash_K \varphi$ ssi $\mathfrak{A} \vDash_K \varphi$ pour tout $\mathfrak{A}$ de type adéquat.
$\mathfrak{A} \vDash_K \Gamma$ ssi $\mathfrak{A} \vDash_K \psi$ pour tout $\psi \in \Gamma$,
$\Gamma \vDash_K \varphi$ ssi $\mathfrak{A} \vDash_K \Gamma$ implique $\mathfrak{A} \vDash_K \varphi$, si $\Gamma \cup \{\varphi\}$ est constitué de sentences.

Lemme 8.1. $\mathfrak{A} \vDash_K \varphi \wedge \psi$ *si et seulement si* $\mathfrak{A} \vDash_K \varphi$ *et* $\mathfrak{A} \vDash_K \psi$
$\mathfrak{A} \vDash_K \varphi \vee \psi$ *si et seulement si* $\mathfrak{A} \vDash_K \varphi$ *ou* $\mathfrak{A} \vDash_K \psi$
$\mathfrak{A} \vDash_K \neg\varphi$ *si et seulement si* $\mathfrak{A} \nvDash \varphi$
$\mathfrak{A} \vDash_K \varphi \Rightarrow \psi$ *si et seulement si* $\mathfrak{A} \vDash_K \varphi$ *implique* $\mathfrak{A} \vDash_K \psi$
$\mathfrak{A} \vDash_K \varphi \Leftrightarrow \psi$ *si et seulement si* $\mathfrak{A} \vDash_K \varphi$ *est équivalent à* $\mathfrak{A} \vDash_K \psi$
$\mathfrak{A} \vDash_K \forall x\varphi$ *si et seulement si* $\mathfrak{A} \vDash_K \varphi[x := \overline{a}]$ *pour tout* $a \in A$.
$\mathfrak{A} \vDash_K \exists x\varphi$ *si et seulement si* $\mathfrak{A} \vDash_K \varphi[x := \overline{a}]$ *pour un* $a \in A$.

Démonstration. On le fait dans deux cas seulement.

$\mathfrak{A} \vDash_K \varphi \vee \psi$ équivaut à $\max([\![\varphi]\!]_{\mathfrak{A}}, [\![\psi]\!]_{\mathfrak{A}}) = 1$ ce qui équivaut à ce que $[\![\varphi]\!]_{\mathfrak{A}} = 1$ ou $[\![\psi]\!]_{\mathfrak{A}} = 1$ ce qui équivaut donc à $\mathfrak{A} \vDash_K \varphi$ ou $\mathfrak{A} \vDash_K \psi$.

$\mathfrak{A} \vDash_K \forall x\varphi$ équivaut à $\min\{[\![\varphi[x := \overline{a}]]\!]_{\mathfrak{A}} \mid a \in A\} = 1$ ce qui équivaut à ce que pour tout $a \in A$ on ait $[\![\varphi[x := \overline{a}]]\!]_{\mathfrak{A}} = 1$ ce qui revient donc à ce que pour tout $a \in A$ on ait $\mathfrak{A} \vDash_K \varphi[x := \overline{a}]$. ■

8.4 Quelques propriétés

Quantificateurs et négations

$\vDash_K \neg\forall x\varphi \Leftrightarrow \exists x\neg\varphi$
$\vDash_K \neg\exists x\varphi \Leftrightarrow \forall x\neg\varphi$
$\vDash_K \forall x\varphi \Leftrightarrow \neg\exists x\neg\varphi$
$\vDash_K \exists x\varphi \Leftrightarrow \neg\forall x\neg\varphi$

Permutation et oubli de quantificateurs

$\vDash_K \forall x\forall y\varphi \Leftrightarrow \forall y\forall x\varphi$
$\vDash_K \exists x\exists y\varphi \Leftrightarrow \exists y\exists x\varphi$
$\vDash_K \forall x\varphi \Leftrightarrow \varphi$ si $x \notin FV(\varphi)$
$\vDash_K \exists x\varphi \Leftrightarrow \varphi$ si $x \notin FV(\varphi)$

Formules prénexes

Une formule φ est en ***forme prénexe***, on dit aussi que φ est ***prénexe***, si φ consiste d'un suite (éventuellement vide) de quantificateurs suivie d'une formule sans quantificateurs.

Exemple. $(\forall x)P(x) \Rightarrow (\exists y)P(y)$ n'est pas en forme prénexe, tandis que $(\exists y\, x)(P(x) \Rightarrow P(y))$ est en forme prénexe.

Formules en forme prénexe

Théorème 8.2. *Pour chaque* φ *il existe une formule prénexe* ψ *telle que* $\vDash_K \varphi \Leftrightarrow \psi$.

8.5 La déduction naturelle

Les règles

On ajoute à la logique propositionelle les règles

$$\frac{\Gamma \vdash_K \varphi(x)}{\Gamma \vdash_K \forall x \varphi(x)} \forall I \qquad \frac{\Gamma \vdash_K \forall x \varphi(x)}{\Gamma \vdash_K \varphi(t)} \forall E$$

Complétude

Théorème 8.3. *$\Gamma \vDash_K \varphi$ implique $\Gamma \vdash_K \varphi$.*

Autrement dit, la logique classique est complète pour les modèles à base de structures tel que nous venons de les présenter.

Je fais l'impasse !

8.6 L'approche à la Hilbert

Les axiomes et les règles

On a deux axiomes

Axiome :

$$\frac{}{\vdash \forall x\ \varphi(x) \Rightarrow \varphi(t)} \forall_1$$

Axiome :

$$\frac{}{\vdash (\forall x\ (\varphi \Rightarrow \psi(x))) \Rightarrow \varphi \Rightarrow \forall x\ \psi(x)} \forall_2 \quad x \notin FV(\varphi)$$

et une règle

$$\frac{\vdash \varphi(x)}{\vdash \forall x\ \varphi(x)} \forall I$$

Chapitre 9

Calcul des séquents

9.1 Le calcul des séquents

Rétablir la symétrie rompue

Dans la déduction naturelle classique, la symétrie ***introduction-élimination*** est rompue par la règle de réduction à l'absurde.

Le but du calcul des séquents est de rétablir cette symétrie.

Les séquents

Dans le calcul des séquents, les jugements sont de la forme :

$$\Gamma \vdash \Delta.$$

où Γ et Δ sont des multi-ensembles de propositions.

Le cas intuitionniste est le cas particulier où Δ est constitué d'une et une seule proposition.

Les règles

Les règles du calcul des séquents respectent une symétrie gauche/droite.

Il y a

- ***les règles structurelles***,
- ***les règles logiques***, il n'y a que des règles d'introduction,
- ***l'axiome***,
- ***la règle de coupure***.

L'axiome

Axiome :

$$\Gamma, \varphi \vdash \Delta, \varphi$$

Les règles structurelles

L'affaiblissement

$$\frac{\Gamma \vdash \Delta}{\Gamma, \varphi \vdash \Delta} \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \varphi}$$

La contraction

$$\frac{\Gamma, \varphi, \varphi \vdash \Delta}{\Gamma, \varphi \vdash \Delta} \qquad \frac{\Gamma \vdash \Delta, \varphi, \varphi}{\Gamma \vdash \Delta, \varphi}$$

Les règles logiques (conjonction)

L'introduction d'une conjonction à gauche

$$\frac{\Gamma, \varphi \vdash \Delta}{\Gamma, \varphi \wedge \psi \vdash \Delta} \qquad \frac{\Gamma, \psi \vdash \Delta}{\Gamma, \varphi \wedge \psi \vdash \Delta}$$

L'introduction d'une conjonction à droite

$$\frac{\Gamma \vdash \Delta, \varphi \qquad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \wedge \psi}$$

Les règles logiques (disjonction)

L'introduction d'une disjonction à gauche

$$\frac{\Gamma, \varphi \vdash \Delta \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \vee \psi \vdash \Delta}$$

L'introduction d'une disjonction à droite

$$\frac{\Gamma \vdash \Delta, \varphi}{\Gamma \vdash \Delta, \varphi \vee \psi} \qquad \frac{\Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \vee \psi}$$

Les règles logiques (implication)

L'introduction d'une implication à gauche

$$\frac{\Gamma, \psi \vdash \Delta \qquad \Gamma \vdash \Delta, \varphi}{\Gamma, \varphi \Rightarrow \psi \vdash \Delta}$$

L'introduction d'une implication à droite

$$\frac{\Gamma, \varphi \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \Rightarrow \psi}$$

Les règles logiques (négation)

L'introduction d'une négation à gauche

$$\frac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg\varphi \vdash \Delta}$$

L'introduction d'une négation à droite

$$\frac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi}$$

Les règles logiques (quantification universelle)

L'introduction d'une quantification universelle à gauche

$$\frac{\Gamma, \varphi[x := t] \vdash \Delta}{\Gamma, \forall x\varphi \vdash \Delta}$$

L'introduction d'une quantification universelle à droite

$$\frac{\Gamma \vdash \Delta, \varphi}{\Gamma \vdash \Delta, \forall x\varphi}$$

Les règles logiques (quantification existentielle)

L'introduction d'une quantification existentielle à gauche

$$\frac{\Gamma, \varphi \vdash \Delta}{\Gamma, \exists x\varphi \vdash \Delta}$$

L'introduction d'une quantification existentielle à droite

$$\frac{\Gamma \vdash \Delta, \varphi[x := t]}{\Gamma \vdash \Delta, \exists x\varphi}$$

La preuve de la formule de Pierce

$$\dfrac{\dfrac{\dfrac{\varphi \vdash \varphi \qquad \dfrac{\varphi \vdash \psi, \varphi}{\vdash \varphi \Rightarrow \psi, \varphi}\ \text{introduction de } \Rightarrow \text{ à droite}}{(\varphi \Rightarrow \psi) \Rightarrow \varphi \vdash \varphi, \varphi}\ \text{introduction de } \Rightarrow \text{ à gauche}}{(\varphi \Rightarrow \psi) \Rightarrow \varphi \vdash \varphi}\ \text{contraction à droite}}{\vdash ((\varphi \Rightarrow \psi) \Rightarrow \varphi) \Rightarrow \varphi}\ \text{introduction de } \Rightarrow \text{ à droite}$$

Le calcul des séquents sans coupure

La calcul qui ne contient que les règles précédentes : axiomes, règles structurelles, règles logiques,

s'appelle ***le calcul des séquents sans coupure***.

Proposition 9.1. *Le calcul des séquents sans coupure satisfait la* ***propriété de la sous-formule****, à savoir que les formules figurant dans la preuve d'un séquent sont des sous-formules de ce séquent.*

La règle de coupure

$$\frac{\Gamma \vdash \Delta, \varphi \qquad \Gamma', \varphi \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

En fait c'est l'utilisation d'un lemme dans une démonstration qui permet de faire une démonstration plus courte et plus «intelligente».

L'élimination des coupures

La règle de coupure n'augmente pas la puissance du calcul des séquents.

Gentzen a démontré le ***théorème d'élimination des coupures***. Si une démonstration comporte des coupures, on peut la transformer en une démonstration équivalente qui ne comporte pas de coupures.

La démonstration du théorème d'élimination des coupures utilise la symétrie du calcul des séquents.

Ce théorème ne se généralise pas aux théories où l'on accepterait d'autres axiomes.

Dans ce cas, l'utilisation de coupure permet des démonstrations plus puissantes.

9.2 $\lambda\mu\tilde{\mu}$-calcul

The implicative sequent calculus

Propositions are made only
- of propositional variables
- and of the implication operators.

The implicative sequent calculus (the rules)

$$\frac{}{\Gamma, A \vdash \Delta, A}\,(ax)$$

$$\frac{\Gamma \vdash A, \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta}\,(\to L) \qquad \frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}\,(\to R)$$

$$\frac{\Gamma \vdash A, \Delta \qquad \Gamma, A \vdash \Delta}{\Gamma \vdash \Delta}\,(cut)$$

A proof of the Pierce law

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash B, A}\,(ax)}{\vdash A \to B, A}\,(\to R) \qquad \dfrac{}{A \vdash A}\,(ax)}{(A \to B) \to A \vdash A}\,(\to L)}{\vdash ((A \to B) \to A) \to A}\,(\to R)$$

The active formula

The ***active formula*** is the formula on the lower part of a rule which is *«split»* by the rule.

For instance in

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta}\,(\to L)$$

the active formula is $A \to B$.

It makes sense to track the active formulae and to suppose that A and B become the new active formulae :

$$\frac{\Gamma \vdash A, \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta}\,(\to L)$$

Similarly

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}\,(\to R)$$

We have to prove B using the proposition A and to split B if necessary.

But our proof of the Pierce law does not fulfill this statement on active formulae.

$$\dfrac{\dfrac{\dfrac{}{A \vdash B, A}\,(ax)}{\vdash A \to B, A}\,(\to R) \qquad \dfrac{}{A \vdash A}\,(ax)}{\dfrac{(A \to B) \to A \vdash A}{\vdash ((A \to B) \to A) \to A}\,(\to R)}\,(\to L)$$

The rules of the implicative sequent calculus with active formulæ

$$\frac{}{\Gamma, A \vdash \Delta, A}\,(L - ax) \qquad \frac{}{\Gamma, A \vdash \Delta, A}\,(R - ax)$$

$$\frac{\Gamma \vdash A, \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta}\,(\to L) \qquad \frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}\,(\to R)$$

$$\frac{\Gamma \vdash A, \Delta \qquad \Gamma, A \vdash \Delta}{\Gamma \vdash \Delta}\,(cut)$$

$$\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A, \Delta}\,(\mu) \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma, A \vdash \Delta}\,(\tilde{\mu})$$

Four requirements :

- One needs to introduce two axioms according to the side of the active formula.
- In (cut) the new introduced proposition becomes the active formula.
- The lower sequent of (cut) has no active formula.
- One needs to introduce a new rule that ***activates*** a formula and enables a (cut) above that rule.

A new proof of the Pierce law

$$\dfrac{\dfrac{(A\to B)\to A\vdash (A\to B)\to A, A \qquad \dfrac{\mathcal{A}_1 \qquad \mathcal{A}_2}{(A\to B)\to A, (A\to B)\to A\vdash A}\,(cut)}{\dfrac{(A\to B)\to A\vdash A}{(A\to B)\to A\vdash A}\,(\mu)}}{\vdash ((A\to B)\to A)\to A}\,(\to R)$$

where

$$\dfrac{\mathcal{A}_1 \qquad \mathcal{A}_2}{(A\to B)\to A, (A\to B)\to A\vdash A}$$

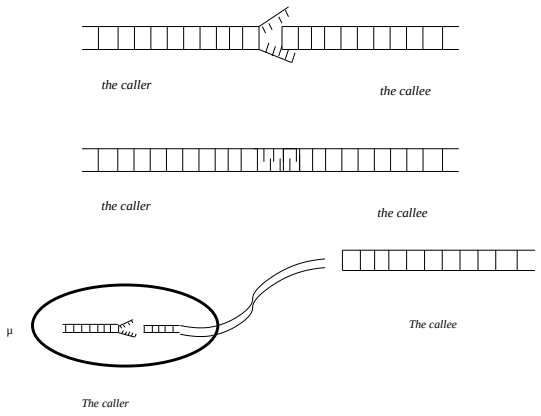
$$=$$

$$\dfrac{\dfrac{\dfrac{(A\to B)\to A, A\vdash A, B, A \qquad (A\to B)\to A, A, A\vdash A, B}{(A\to B)\to A, A\vdash B, A}\,(cut)}{(A\to B)\to A\vdash A\to B, A}\,(\mu)}{(A\to B)\to A, (A\to B)\to A\vdash A}\,(\to R) \qquad \dfrac{}{(A\to B)\to A, A\vdash A}\,(\to L)$$

9.2.1 The model of computation : Herbelin's calculus

A model of computation

The model of computation relies on ***capsules***.



A model of computation : GEMINI

The model of computation relies on ***capsules*** $\langle r \parallel e\rangle$ that contain two constituents :

- a ***caller*** r
- and a ***callee*** e .

with the syntax

$$\begin{array}{lcl} c & ::= & \langle r \parallel e \rangle \\ r & ::= & x \mid \lambda x.r \mid \mu\alpha.c \\ e & ::= & \alpha \mid r \bullet e \mid \widetilde{\mu}x.c \end{array}$$

Callers

A ***caller*** is
- either a variable x,
- or a λ-abstraction $\lambda x.r$ which expects a value to take the place of x in r,
- or a μ-abstraction $\mu\alpha.c$ which expects a callee to take the place of α in c producing a new capsule.

Note : ***values*** and ***callers*** are the same.

Callees

A ***callee*** is basically a list of values, more precisely it is
- either a variable α,
- or a pair $r \bullet e$ of a value (caller) r and a callee e,
- or an $\widetilde{\mu}$-abstraction $\widetilde{\mu}x.c$

The reductions

$$\begin{array}{lrcl} (\lambda) & \langle \lambda x \cdot r \parallel r' \bullet e \rangle & \longrightarrow & \langle r[x \leftarrow r'] \parallel e \rangle \\ (\mu) & \langle \mu\alpha \cdot c \parallel e \rangle & \longrightarrow & c[\alpha \leftarrow e] \\ (\widetilde{\mu}) & \langle r \parallel \widetilde{\mu}x \cdot c \rangle & \longrightarrow & c[x \leftarrow r] \end{array}$$

The system is ambiguous !
$\langle \mu\alpha.c \parallel \widetilde{\mu}x.c' \rangle$ has two possible reductions at the top.
$c[\alpha \leftarrow \widetilde{\mu}x.c']$, $c[x \leftarrow \mu\alpha \cdot c]$ is a ***critical pair***.
The system is ambiguous !
$\langle \mu\alpha.c \parallel \widetilde{\mu}x.c' \rangle$ has two possible reductions at the top.
$c[\alpha \leftarrow \widetilde{\mu}x.c']$, $c[x \leftarrow \mu\alpha \cdot c]$ is a ***critical pair***

This ambiguity is ***inherent to proofs*** in classical logic
Can we type capsules, callers and callees ?
- to prove that *nothing wrong can happen*, i.e., *capsules reduces always* to capsules,
- to guarantee ***termination***, i.e., *a typed capsule always reduces to a normal form* whatever strategy we adopt.

9.2.2 The link between the sequent calculus and Herbelin's calculus

The type judgments

Thanks to colors, I will consider three types of judgments
They can be seen as annotations of sequent calculus judgments ;

Judgments for capsules

In $c\ : x_1 : A_1, \ldots, x_p : A_p \vdash \alpha_1 : B_1, \ldots, \alpha_q : B_q$ (or in short $c\ : \Gamma \vdash \Delta$), one says that

– c takes the x_i as arguments with type A_i

– c takes a continuation α_j with type B_j.

Judgments for callers

$x_1 : A_1, \ldots, x_p : A_p \vdash r : A, \alpha_1 : B_1, \ldots, \alpha_q : B_q$ or in short $\Gamma \vdash r : A, \Delta$, or $\Gamma \vdash \boxed{\text{r: A}}, \Delta$, when one does not have color.

Judgments for callees

$x_1 : A_1, \ldots, x_p : A_p, e : A \vdash \alpha_1 : B_1, \ldots, \alpha_q : B_q$ or in short $\Gamma, e : A \vdash \Delta.$ or $\Gamma, \boxed{\text{e: A}} \vdash \Delta$, when one does not have color.

The type system $G^{\to}$

$$\frac{}{\Gamma, \alpha : A \vdash \alpha : A, \Delta}\,(L-ax) \qquad \frac{}{\Gamma, x : A \vdash x : A, \Delta}\,(R-ax)$$

$$\frac{\Gamma \vdash r : A, \Delta \qquad \Gamma, e : B \vdash \Delta}{\Gamma, r \bullet e : A \to B \vdash \Delta}\,(\to L) \qquad \frac{\Gamma, x : A \vdash r : B, \Delta}{\Gamma \vdash \lambda x.r : A \to B, \Delta}\,(\to R)$$

$$\frac{\Gamma \vdash r : A, \Delta \qquad \Gamma, e : A \vdash \Delta}{\langle r \parallel e \rangle : (\Gamma \vdash \Delta)}\,(cut)$$

$$\frac{c : (\Gamma \vdash \beta : B, \Delta)}{\Gamma \vdash \mu\beta.c : B, \Delta}\,(\mu) \qquad \frac{c : (\Gamma, x : A \vdash \Delta)}{\Gamma, \tilde{\mu}x.c : A \vdash \Delta}\,(\tilde{\mu})$$

$$\frac{}{\Gamma, A \vdash \Delta, A}\,(L-ax) \qquad \frac{}{\Gamma, A \vdash \Delta, A}\,(R-ax)$$

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta}\,(\to L) \qquad \frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}\,(\to R)$$

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma, A \vdash \Delta}{\Gamma \vdash \Delta}\,(cut) \qquad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash B, \Delta}\,(\mu)$$

$$\frac{}{\Gamma, \alpha : A \vdash \alpha : A, \Delta}\,(L-ax) \qquad \frac{}{\Gamma, x : A \vdash x : A, \Delta}\,(R-ax)$$

$$\frac{\Gamma \vdash r : A, \Delta \qquad \Gamma, e : B \vdash \Delta}{\Gamma, r \bullet e : A \to B \vdash \Delta}\,(\to L) \qquad \frac{\Gamma, x : A \vdash r : B, \Delta}{\Gamma \vdash \lambda x.r : A \to B, \Delta}\,(\to R)$$

$$\frac{\Gamma \vdash r : A, \Delta \qquad \Gamma, e : A \vdash \Delta}{\langle r \parallel e \rangle : (\Gamma \vdash \Delta)}\,(cut) \qquad \frac{c : (\Gamma \vdash \beta : B, \Delta)}{\Gamma \vdash \mu\beta.c : B, \Delta}\,(\mu)$$

Curry-Howard correspondence

One gets a Curry-Howard correspondence, namely
- ***terms*** are ***proofs***,
- ***types*** are ***propositions***,
- ***term reductions*** are ***proof simplifications*** (normalization).

Pierce law again

Let T be $(A \to B) \to A$.

$$\dfrac{\dfrac{\dfrac{\dfrac{x : T, y : A \vdash y : A, \beta : B, \alpha : A \qquad x : T, y : A, \alpha : A \vdash \alpha : A, \beta : B}{\langle y \parallel \alpha \rangle : (x : T, y : A \vdash \beta : B, \alpha : A)}\,(cut)}{x : T, y : A \vdash \mu\beta.\langle y \parallel \alpha \rangle : B, \alpha : A}\,(\mu)}{x : T \vdash \lambda y.\mu\beta.\langle y \parallel \alpha \rangle : A \to B, \alpha : A}\,(\to R) \qquad x : T, \alpha : A \vdash \alpha : A}{x : T, (\lambda y.\mu\beta.\langle y \parallel \alpha \rangle) \bullet \alpha : T \vdash \alpha : A}\,(\to L)$$

is called $\mathcal{A}$ in the following screens.

The tree for typing Pierce law is

$$\dfrac{\dfrac{\dfrac{x : T \vdash x : T, \alpha : A \qquad \mathcal{A}}{\langle x \parallel (\lambda y.\mu\beta.\langle y \parallel \alpha \rangle) \bullet \alpha \rangle : (x : T \vdash \alpha : A)}\,(cut)}{x : T \vdash \mu\alpha.\langle x \parallel (\lambda y.\mu\beta.\langle y \parallel \alpha \rangle) \bullet \alpha \rangle : A,}\,(\mu)}{\vdash \lambda x.\mu\alpha.\langle x \parallel (\lambda y.\mu\beta.\langle y \parallel \alpha \rangle) \bullet \alpha \rangle : ((A \to B) \to A) \to A,}\,(\to L)$$

The term with type the Pierce law is

$$\lambda x.\mu\alpha.\langle x \parallel (\lambda y.\mu\beta.\langle y \parallel \alpha \rangle) \bullet \alpha \rangle.$$

Reductions as simplifications of proofs

Reductions are simplifications (normalizations) of proofs

Let us look at

$$(\lambda) \quad \langle \lambda x \cdot r \parallel r' \bullet e \rangle \quad \longrightarrow \quad \langle r[x \leftarrow r'] \parallel e \rangle$$

It corresponds to

$$\dfrac{\dfrac{\dfrac{\mathcal{D}}{\Gamma, x : A \vdash r : B, \Delta}}{\Gamma \vdash \lambda x.r : A \to B, \Delta}\,(\to R) \qquad \dfrac{\Gamma \vdash r' : A, \Delta \quad \Gamma, e : B \vdash \Delta}{\Gamma, r' \bullet e : A \to B \vdash \Delta}\,(\to L)}{\langle \lambda x \cdot r \parallel r' \bullet e \rangle : \Gamma \vdash \Delta}\,(cut)$$

and

$$\dfrac{\mathcal{D}[x \leftarrow r'] \qquad \boxed{\text{ou}} \qquad \dfrac{\Gamma \vdash r' : A, \Delta \qquad \mathcal{D} \qquad \Gamma \vdash r' : A, \Delta}{\Gamma, \vdash r[x \leftarrow r'] : B, \Delta} \qquad \Gamma, e : B \vdash \Delta}{\langle r[x \leftarrow r'] \parallel e \rangle : \Gamma \vdash \Delta}\,(cut)$$

Termination or strong normalization

If c is typable in $G^{\rightarrow}$, then c does not start a non terminating reduction.

Chapitre 10

Logique épistémique

Il *croit* qu'il est Napoléon,
mais *tout le monde sait*
que c'est moi.

10.1 Des exemples

10.1.1 Un protocole

Un protocole émetteur-récepteur

Les noeuds ◯ transmettent les messages entre l'émetteur et le récepteur :

- ils *peuvent dupliquer* des messages,
- ils *peuvent perdre* des messages,
- cependant, ils ne peuvent pas *perdre indéfiniment* un même message.

C'est le principe d'Internet : *«faire de son mieux»* (en anglais *«the best effort»*). Le protocole s'appelle TCP (pour *Transmission Control Protocol*).

Tant que l'émetteur *ne sait pas* si le récepteur a reçu un message donné m_i, il le ré-émet.

Le récepteur accuse réception d'un message en émettant un message d'***accusé réception*** ack_i tant qu'il *ne sait pas* si l'émetteur a reçu cet accusé réception.

Tant que l'émetteur **ne sait pas** si le récepteur a reçu un message donné m_i, il le ré-émet.

Le récepteur accuse réception d'un message en émettant un message d'***accusé réception*** ack_i tant qu'il **ne sait pas** si l'émetteur a reçu cet accusé réception.

10.1.2 L'attaque coordonnée

L'attaque coordonnée

- Deux généraux et leurs armées sur deux collines,
- Ils doivent attaquer ***ensemble*** et chaque général doit être sûr que l'autre général attaquera en même temps.
- Ils communiquent par des messagers
  - qui mettent une heure pour aller d'un camp à l'autre,
  - qui peuvent se perdre dans le noir ou être capturés.

Comment coordonner une attaque ?

Le général 1 envoie des messagers au général 2

Mais le messager peut être capturé ou être tué !

Mais le messager peut se perdre !

L'attaque coordonnée

Le général 1 choisit une heure pour l'attaque, disons H et envoie une messager.

À l'arrivée du messager, le général 2 accepte l'heure H et envoie une messager avec son accord.

Le général 1 attaquera à l'heure H si il sait que le général 2 connaît l'heure qu'il a proposée et l'accepte.

Le général 2 attaquera à l'heure H si il (général 2) sait que le général 1 sait qu'il (général 2) connaît l'heure proposée et l'accepte. *Le général 1 doit envoyer un second messager avec un accord.*

Le général 1 attaquera à l'heure H si il (général 1) sait que le général 2 sait qu'il (général 1) sait que le général 2 connaît l'heure proposée et l'accepte. *Le général 2 doit envoyer un second messager avec un accord.*

Le général 2 attaquera à l'heure H si il (général 2) sait que le général 1 sait qu'il (général 2) sait que le général 1 sait qu'il (général 2) connaît l'heure proposée et l'accepte. *Le général 1 doit envoyer un troisième messager avec un accord.*

⋮

L'attaque coordonnée

Le processus ne va jamais s'arrêter.

*On peut démontrer qu'**avec des communications asynchrones**, une attaque coordonnée **n'est pas possible**. L'acquisition d'une **connaissance commune** n'est pas possible de façon asynchrone.*

10.1.3 Une déclaration

Le secrétaire américain à la Défense Donald Rumsfeld, lors d'un point de presse en février 2002 :

> *«Les informations annonçant que quelque chose n'a pas eu lieu m'intéressent toujours pour la bonne raison que, comme vous le savez, ce sont des nouvelles connues ; il y a des choses que nous savons que nous savons»*
>
> *«Nous savons aussi qu'il y a des choses inconnues ; ce qui revient à dire que nous savons qu'il y a certaines choses dont nous ne savons rien. Mais il existe aussi des nouvelles inexistantes que nous ne connaissons pas – ce sont celles dont nous ignorons si nous les connaissons.»*

10.2 Jouons un peu

Les as et les huit

Il y a huit cartes : quatre as et quatre 8.

Chaque joueur reçoit deux cartes qu'il ne regarde pas, mais qu'il montre à tout le monde.

Chaque joueur parle à son tour :

- Soit il dit *Je ne sais pas*,
- Soit il dit
  - *J'ai une paire*,
  - *J'ai un as et un huit.*

On fait autant de tours qu'il faut.

Il y a *toujours* un joueur qui peut deviner les cartes qu'il a.

1^{re} donne	$1 : A+A$	$2 : 8+8$	$3 : 8+8$
2^{e} donne	$1 : A+A$	$2 : 8+8$	$3 : A+A$
3^{e} donne	$1 : A+A$	$2 : 8+8$	$3 : A+8$
4^{e} donne	$1^2 : A+8$	$2 : 8+8$	$3 : A+8$
5^{e} donne	$1 : A+8$	$2^2 : A+8$	$3 : A+8$
6^{e} donne	$1 : A+8$	$2 : A+8$	$3^2 : A+A$
7^{e} donne	$1 : 8+8$	$2 : 8+8$	$3 : A+A$
8^{e} donne	$1 : 8+8$	$2^2 : A+8$	$3 : A+A$
9^{e} donne	$1 : 8+8$	$2 : A+8$	$3^2 : A+8$
10^{e} donne	$1^2 : A+8$	$2 : 8+8$	$3 : A+A$

10.3 La logique de la connaissance

10.3.1 Les modalités

Les modalités

Une modalité est un opérateur qui ***transforme*** une sentence en une autre sentence.

On crée un modalité K_A pour chaque agent A.

Une logique avec des modalités s'appelle une ***logique modale***.

Qu'est-ce que la logique de la connaissance ?

- La ***logique de la connaissance*** ou ***logique épistémique*** est la logique qui formalise
  - «L'agent i sait que p», noté $K_i(p)$,
  - «p est une connaissance commune», noté $C(p)$.

La connaissance commune

$C(p)$ formalise des phrases comme

- «C'est un fait bien connu que p, sauf des fous.»
- «L'agent i *sait que* l'agent j *sait que* l'agent i *sait que* , etc.».

On a besoin d'une modalité E, dite de «connaissance partagée», «Tout le monde *sait que* p»,

$$E_G(p) = \bigwedge_{i \in G} K_i(p).$$

La ***connaissance commune*** *n'est pas* la ***connaissance partagée***.

10.3.2 Les règles et les axiomes

Les règles

C'est une logique qui se présente à la Hilbert (avec un symbole qui signifie ***«est un théorème»***):

$$\frac{\vdash \varphi \qquad \vdash \varphi \Rightarrow \psi}{\vdash \psi}\,(MP)$$

La règle de généralisation de la connaissance

$$\frac{\vdash \varphi}{\vdash K_i\varphi}\,(GK)$$

Les axiomes

Il y a *tous les théorèmes de la logique propositionnelle classique.*

$$\frac{}{\vdash \varphi}\,(\mathbf{Cl}) \qquad \text{si } \varphi \text{ est un théorème de la logique classique.}$$

Il y a quatre axiomes.

Axiome de distribution :

$$\frac{}{\vdash K_i\varphi \Rightarrow K_i(\varphi \Rightarrow \psi) \Rightarrow K_i\psi}\,(\mathbf{K})$$

Axiome de la connaissance :

$$\frac{}{\vdash K_i\varphi \Rightarrow \varphi}\,(\mathbf{T})$$

Axiome d'introspection positive :

$$\frac{}{\vdash K_i\varphi \Rightarrow K_iK_i\varphi}\,(\mathbf{4})$$

Axiome d'introspection négative :

$$\frac{}{\vdash \neg K_i\varphi \Rightarrow K_i\neg K_i\varphi}\,(\mathbf{5})$$

Attention

En logique modale ***on n'a pas*** la ***règle de déduction*** «De $\Gamma, \varphi \vdash \psi$ je déduis $\Gamma \vdash \varphi \Rightarrow \psi$»

Les axiomes de la connaissance commune

Défintion de E_G

$$\frac{}{\vdash E_G(\varphi) \Leftrightarrow \bigwedge_{i \in G} K_i(\varphi)} (C1)$$

$C_G\varphi$ satisfait l'inégalité $\psi \Rightarrow \varphi \wedge E_G(\psi)$.

$$\frac{}{\vdash C_G\varphi \Rightarrow \varphi \wedge E_G(C_G\varphi)} (C2)$$

Les règles de la connaissance commune

$C_G\varphi$ est le plus petit dans un certain sens, c'est-à-dire si un ψ satisfait $\psi \Rightarrow \varphi \wedge E_G(\psi)$ alors $\psi \Rightarrow C_G\varphi$.

$$\frac{\vdash \psi \Rightarrow \varphi \wedge E_G(\psi)}{\vdash \psi \Rightarrow C_G\varphi} (RC1)$$

Une preuve

$$\vdash K_i(\varphi \Rightarrow \psi) \Rightarrow K_i\varphi \Rightarrow K_i\psi$$

$$\dfrac{\dfrac{}{\vdash K_i\varphi \Rightarrow K_i(\varphi \Rightarrow \psi) \Rightarrow K_i\psi}(K) \qquad \dfrac{}{\vdash (K_i\varphi \Rightarrow K_i(\varphi \Rightarrow \psi) \Rightarrow K_i\psi) \Rightarrow (K_i(\varphi \Rightarrow \psi) \Rightarrow K_i\varphi \Rightarrow K_i\psi)}(CI)}{\vdash K_i(\varphi \Rightarrow \psi) \Rightarrow K_i\varphi \Rightarrow K_i\psi}(MP)$$

10.3.3 Les modèles

Les modèles de Kripke

Un ***modèle de Kripke*** est un triplet $\mathcal{M} = (\mathcal{U}_\mathcal{M}, \mathcal{I}_\mathcal{M}, \mathcal{R}_\mathcal{M})$ où

- $\mathcal{U}_\mathcal{M}$ est un ensemble dont les éléments sont appelés, suivant les auteurs,
  - des ***mondes***,
  - des ***mondes possibles***,
  - des ***étapes (de raisonnement)***,
  - des ***états***.
- $\mathcal{I}_\mathcal{M} : Variables \rightarrow \mathcal{P}(\mathcal{U}_\mathcal{M})$. Intuitivement $\mathcal{I}_\mathcal{M}(p)$ est l'ensemble des mondes où la variable p est satisfaite.

Les mondes sont notés u, v, w.

- $\mathcal{R}_\mathcal{M} = (R_1, ..R_n)$ est un ensemble de relations dites ***relations d'accessibilité***.Si $u\,R_i\,v$ alors le monde v est accessible à partir de u pour i [1].

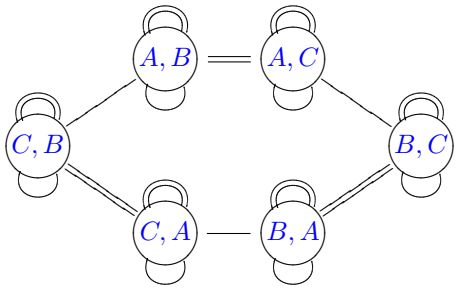
Les propriétés (transitivité, réflexivité, symétrie ou antisymétrie) des relations R_i jouent un rôle.

$\mathcal{I}_\mathcal{M}$ doit satisfaire des propriétés de compatibilité avec les R_i.

[1] On verra plus tard ce que ça signifie.

Un jeu très simple

2 agents, 3 cartes $\{A, B, C\}$.
L'agent 1 reçoit une carte
L'agent 2 reçoit un carte
La troisième carte est retournée face contre la table
Il y a six mondes possibles : $(A,B), (A,C), (B,A)(B,C), (C,A), (C,B)$.
Dans le monde (A,B) l'agent 1 (sa relation d'accessibilité est notée par $=\!=$) envisage deux mondes possibles à savoir (A,B) et (A,C).



Le modèle de Kripke $\mathcal{M}$.

Les propositions primitives sont
– $1A$ le joueur (l'agent) 1 détient la carte A,
– $2A$ le joueur (l'agent) 2 détient la carte A,
– $1B$ le joueur (l'agent) 1 détient la carte B,
– $2B$ le joueur (l'agent) 2 détient la carte B,
– $1C$ le joueur (l'agent) 1 détient la carte C,
– $2C$ le joueur (l'agent) 2 détient la carte C.

Des assertions de forçage

$(A,B) \Vdash 1A \wedge 2B$,
$(A,B) \Vdash K_1(2B \vee 2C)$,
$(A,B) \Vdash K_1 \neg K_2(1A)$.
Pour tout monde u l'assertion $u \Vdash K_1(2A \vee 2B \vee 2C)$ est vraiedonc $\mathcal{M} \vDash K_1(2A \vee 2B \vee 2C)$.

Accessibilité et forçage

1. Si φ est une ***variable*** p:
$$\mathcal{M}, u \Vdash \varphi \quad \text{ssi} \quad u \in \mathcal{I}_{\mathcal{M}}(p)$$
2. Si φ est une ***conjonction*** $\psi \wedge \theta$
$$\mathcal{M}, u \Vdash \varphi \quad \text{ssi} \quad \mathcal{M}, u \Vdash \psi \quad \text{et} \quad \mathcal{M}, u \Vdash \theta$$
3. Si φ est une ***disjonction*** $\psi \vee \theta$
$$\mathcal{M}, u \Vdash \varphi \quad \text{ssi} \quad \mathcal{M}, u \Vdash \psi \quad \text{or} \quad \mathcal{M}, u \Vdash \theta$$
4. Si φ est une ***implication*** $\psi \Rightarrow \theta$
$$\mathcal{M}, u \Vdash \varphi \quad \text{ssi} \quad \mathcal{M}, u \Vdash \psi \quad \text{implique} \quad \mathcal{M}, u \Vdash \theta$$
5. Si $\perp$ est ***absurde***, alors $\mathcal{M}, u \nVdash \perp$.

Accessibilité et forçage

6. Si φ est une *modalité* $K_i(\psi)$ alors

$$u \Vdash K_i(\psi) \qquad \text{ssi} \qquad (\forall v \in \mathcal{U}_{\mathcal{M}})\ u\ R_i\ v \quad \text{implies} \quad v \Vdash \psi.$$

Cela signifie aussi que l'agent i sait ψ dans le monde u si et seulement si dans chaque monde qu'il tient comme possible ψ est satisfaite.

Accessibilité et forçage

7. Si φ est une *modalité* $C_G(\psi)$ alors

$$u \Vdash C_G(\psi) \qquad \text{ssi} \qquad (\forall v \in \mathcal{U}_{\mathcal{M}})\ u\ (\bigcup_{i \in G} R_i)^*\ v \quad \text{implies} \quad v \Vdash \psi.$$

Cela signifie aussi que $C_G(\psi)$ est satisfaite dans le monde u si et seulement si dans chaque monde accessible par un chemin d'accessibilité, ψ est satisfaite.

Accessibilité et forçage

On doit avoir

$$u \Vdash K_i\varphi \qquad \Longleftrightarrow \qquad (\forall v \in \mathcal{U}_{\mathcal{M}})\ v\ R_i\ u \Rightarrow v \Vdash \varphi.$$

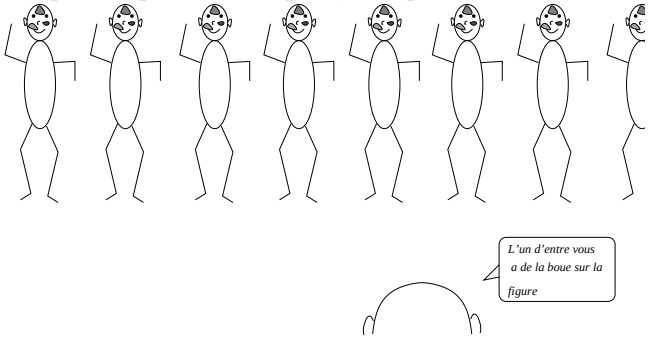
Autrement dit, $u \Vdash K_i\varphi$ si et seulement si, dans tous les mondes accessibles à partir de u, on a φ.

Ou encore, l'agent i sait φ si dans tous les mondes qu'il peut envisager, φ est satisfaite.

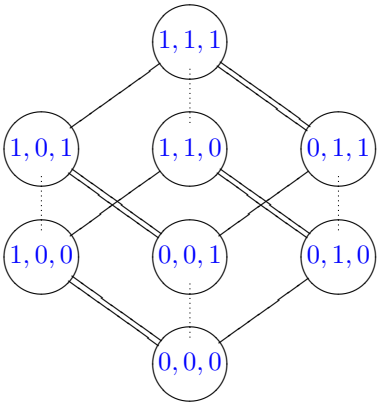
10.3.4 L'énigme des enfants sales

Les enfants sales

- Il y a n enfants dont certains ont la saleté sur le front.
- Le père déclare «L'un d'entre vous a de la saleté sur le front».
- Puis le père pose plusieurs fois (combien ?) la question «Avez-vous de la saleté sur le front ?».
- Comme les n enfants ont tous de la saleté sur le front.
- Après n questions du père, ils répondent tous ensemble «oui».

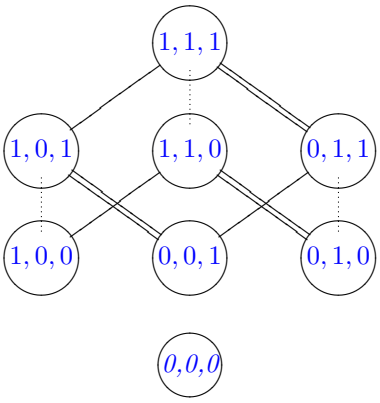


Le modèle de Kripke pour trois enfants sales

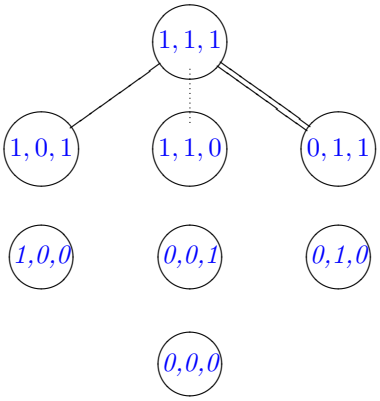


On abandonne les boucles de réflexivité.

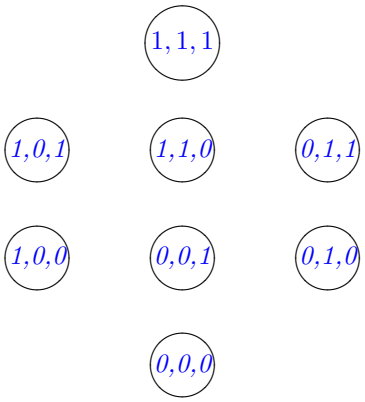
Après que le père a parlé



Après que le père a posé sa première question



Après que le père a posé sa deuxième question



10.3.5 Correction et preuves

Correction

Théorème 10.1. *Si* $\vdash \varphi$ *alors* $\vDash \varphi$.

Pourquoi pas la règle de déduction ?

Si on avait la règle de déduction *«De* $\Gamma, \varphi \vdash \psi$ *je déduis* $\Gamma \vdash \varphi \Rightarrow \psi$*»* alors du jugement $\varphi \vdash K_i\varphi$ on aurait $\varphi \vDash K_i\varphi$, c'est-à-dire *«Si dans tous les mondes de l'univers en question,* φ *est vrai, alors chaque agent* i *sait* φ*»*

on pourrait déduire $\vDash \varphi \Rightarrow K_i\varphi$ c'est-à-dire «Si φ est vrai alors chaque agent i sait φ».

Une preuve

On peut prouver $\vdash \varphi \Rightarrow K_i\neg K_i\neg\varphi$.

$$\dfrac{\dfrac{}{\vdash \neg K_i\varphi \Rightarrow K_i\neg K_i\neg\varphi}\,(\mathbf{5}) \qquad \dfrac{\dfrac{}{\vdash \psi}\,(Cl) \qquad \dfrac{}{\vdash K_i\neg\varphi \Rightarrow \neg\varphi}\,(\mathbf{T})}{\vdash (\neg K_i\varphi \Rightarrow K_i\neg K_i\neg\varphi) \Rightarrow \varphi \Rightarrow K_i\neg K_i\neg\varphi}\,(MP)}{\vdash \varphi \Rightarrow K_i\neg K_i\neg\varphi}\,(MP)$$

où $\psi \equiv (K_i\neg\varphi \Rightarrow \neg\varphi) \Rightarrow (\neg K_i\varphi \Rightarrow K_i\neg K_i\neg\varphi) \Rightarrow \varphi \Rightarrow K_i\neg K_i\neg\varphi$ qui est un théorème classique.

Car c'est un instance de $(B \Rightarrow \neg A) \Rightarrow (\neg B \Rightarrow C) \Rightarrow (A \Rightarrow C)$.