Fondements de l'informatique
Logique, modèles, et calculs

Chapitre: Modèles. Complétude.

Cours CSC_41012_EP

de l'Ecole Polytechnique

Olivier Bournez

bournez@lix.polytechnique.fr

Version du 11 juillet 2025

Modèles. Complétude.

Nous pouvons maintenant décrire différents objets, et parler de leurs propriétés. Nous avons en effet tous les ingrédients pour parler de modèles et de théories. Nous nous intéresserons ensuite au théorème de complétude

Le concept de base est celui de théorie.

Définition 1 (Théorie)
— *Une* théorie $\mathcal{T}$ *est un ensemble de formules closes sur une signature donnée. Les formules d'une théorie sont appelées les* axiomes *de cette théorie.*
— *Une structure* $\mathfrak{M}$ *est un* modèle de la théorie $\mathcal{T}$ *si* $\mathfrak{M}$ *est un modèle de chacune des formules de la théorie.*

Définition 2 (Théorie consistante) *Une théorie est dite* consistante *si elle possède un modèle. Elle est dite* inconsistante *dans le cas contraire.*

Bien entendu, les théories inconsistantes sont de peu d'intérêt.

Remarque 3 *D'un point de vue informatique, on peut voir une théorie comme la spécification d'un objet : on décrit l'objet à l'aide de la logique du premier ordre, i.e. à l'aide des axiomes qui le décrivent.*

Une spécification (théorie) consistante est donc ni plus ni moins qu'une théorie qui spécifie au moins un objet.

Remarque 4 *Dans ce contexte, la question de la complétude est de savoir si l'on décrit bien l'objet en question, ou la classe des objets en question : le théorème de complétude permet de dire que oui pour une spécification consistante, tant que l'on s'intéresse à la classe de tous les modèles de ces spécifications.*

Nous allons commencer par donner différents exemples de théories, pour rendre notre discussion beaucoup moins abstraite.

1 Exemples de théories

1.1 Graphe

Un graphe orienté peut se voir comme un modèle de la théorie sans axiome sur la signature $\Sigma = (\emptyset, \emptyset, \{E\})$, où le symbole de relation E est d'arité 2 : $E(x, y)$ signifie

qu'il y a un arc entre x et y.

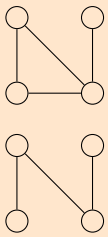
Exemple 5 *La formule $\exists y(E(x,y) \wedge \forall z(E(x,z) \Rightarrow x = y))$ est vraie en x si et seulement si x est de degré extérieur 1 (modulo le commentaire de la sous-section qui suit sur l'égalité).*

Un graphe non-orienté peut se voir comme un modèle de la théorie avec l'unique axiome

$$\forall x \forall y \ (E(x,y) \Leftrightarrow E(y,x)), \tag{1}$$

sur la même signature. Cet axiome signifie que s'il y a un arc entre x et y, alors il y en a aussi un de y vers x et réciproquement.

Exemple 6 *Voici 2 graphes (non-orientés).*



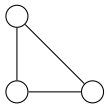
La formule $\exists x \forall y(\neg(x = y) \Rightarrow E(x,y))$ est satisfaite sur le premier et pas sur le second.

1.2 Remarques simples

Remarque 7 *Sur la signature $\Sigma = (\emptyset, \emptyset, \{E\})$, il n'y a aucun terme. On ne peut donc pas désigner un sommet particulier autrement que par une variable libre, ou via des quantifications.*

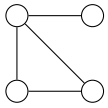
Si l'on veut désigner un ou des sommets particuliers, on peut ajouter un ou des symboles de constantes. On peut considérer la signature $(V, \emptyset, \{E\})$ où $V = \{a, b, c\}$.

Par exemple, le graphe



est un modèle de $E(a,b) \wedge E(b,c) \wedge E(a,c)$.

Mais attention, ce n'est pas le seul : le graphe



en est aussi un modèle : le domaine d'un modèle peut contenir des éléments qui ne correspondent à aucun terme.

Par ailleurs l'interprétation de a, b ou c pourrait être la même.

Exemple 8 *On peut aussi parfois se passer de constantes. La formule*

$$\exists x \exists y \exists z (\neg(x = y) \wedge \neg(y = z) \wedge \neg(x = z) \wedge E(x, y) \wedge E(y, z) \wedge E(x, z) \wedge \forall t (t = x \vee t = y \vee t = z)) \tag{2}$$

caractérise les triangles comme le graphe plus haut (modulo le commentaire de la sous-section qui suit sur l'égalité) pour les graphes sans boucle. On peut ajouter $\neg E(x, x) \wedge \neg E(y, y) \wedge \neg E(z, z)$ à l'intérieur de la parenthèse si l'on veut explicitement une caractérisation sur les graphes (et du coup interdire les boucles dans des graphes qui pourraient en avoir).

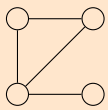
Remarque 9 *Attention : toutes les propriétés ne peuvent pas s'écrire facilement. Par exemple, on peut prouver qu'il n'est pas possible d'écrire une formule (du premier ordre) qui caractériserait les graphes connexes. Exercice : essayer de l'écrire pour réaliser où sont les problèmes.*

Remarque 10 *C'est la présence de modèles "parasites", i.e. d'autres modèles que ceux que l'on arrive à décrire et que l'on ne peut pas éviter, qui sera quelque part au cœur des difficultés de l'axiomatisation des entiers.*

1.3 Égalité

Attention, la discussion précédente est impropre : on a utilisé à plusieurs reprises le symbole d'égalité. La discussion suppose que l'interprétation de l'égalité est bien l'égalité.

Exemple 11 *En fait*



est bien un modèle de (2)*, et donc il est parfaitement faux que* (2) *caractérise les triangles.*

En effet, appelons $\{a, b, c, d\}$ les sommets de haut en bas et de gauche à droite ; on peut considérer l'interprétation $\equiv$ de $=$ avec $a \equiv a, b \equiv b, c \equiv c, d \equiv b$ et $a \not\equiv b, a \not\equiv c, b \not\equiv c$. Un tel modèle vérifie bien (2)*. Cependant, $\equiv$, l'interprétation de $=$ n'est pas l'égalité. Remarquons que l'on a une arête entre a et b, $b = d$ qui est vrai mais pas d'arête entre a et d.*

Il faut pour rendre correct la discussion ajouter d'une part le symbole $=$ à la signature dans les exemples, et d'autre part, ajouter les axiomes vérifiés par l'égalité.

Soit $\mathscr{R}$ un ensemble de symboles de relations contenant au moins le symbole d'égalité $=$.

Définition 12 (Axiomes de l'égalité) *Les axiomes de l'égalité pour une signature*

$$\Sigma = (\mathscr{C}, \mathscr{F}, \mathscr{R}),$$

avec $= \in \mathscr{R}$*, sont*

- *l'axiome* $\forall x\ x = x$
- *pour chaque symbole de fonction* $f \in \mathscr{F}$ *d'arité n, l'axiome*

$$\forall x_1 \cdots \forall x_i \forall x'_i \cdots \forall x_n (x_i = x'_i \Rightarrow f(x_1, \cdots, x_i, \cdots, x_n) = f(x_1, \cdots, x'_i, \cdots, x_n))$$

- *pour chaque symbole de relation* $R \in \mathscr{R}$ *d'arité n,*

$$\forall x_1 \cdots \forall x_i \forall x'_i \cdots \forall x_n (x_i = x'_i \Rightarrow (R(x_1, \cdots, x_i, \cdots, x_n) \Rightarrow R(x_1, \cdots, x'_i, \cdots, x_n))$$

Tous ces axiomes spécifient que l'égalité est reflexive et est préservée par les symboles de fonction et de relation.

Exercice 1 *(corrigé page 239) Prouver que l'on a nécessairement alors* $\forall x \forall y\ (x = y \Rightarrow y = x)$.

Exercice 2 *Prouver que l'on a nécessairement alors pour chaque symbole de relation* $R \in \mathscr{R}$ *d'arité n,*

$$\forall x_1 \cdots \forall x_i \forall x'_i \cdots \forall x_n (x_i = x'_i \Rightarrow (R(x_1, \cdots, x_i, \cdots, x_n) \Leftrightarrow R(x_1, \cdots, x'_i, \cdots, x_n)).$$

Exercice 3 *Prouver que l'on a nécessairement alors pour chaque formule* $F(x_1, x_2, \ldots, x_n)$

$$\forall x_1 \cdots \forall x_i \forall x'_i \cdots \forall x_n (x_i = x'_i \Rightarrow (F(x_1, \cdots, x_i, \cdots, x_n) \Leftrightarrow F(x_1, \cdots, x'_i, \cdots, x_n)).$$

Exercice 4 *Prouver que l'on a nécessairement alors* $\forall x \forall y \forall z\ ((x = y \wedge y = z) \Rightarrow x = z)$.

On déduit des deux exercices précédents, que $=$ (et son interprétation) est une relation d'équivalence.

1.4 Petite parenthèse

Définition 13 *Un modèle* $\mathfrak{M}$ *d'une théorie* $\mathscr{T}$ *sur une signature avec le symbole de relation* $=$ *est dit* égalitaire, *si l'interprétation de* $=$ *dans* $\mathfrak{M}$ *est l'égalité.*

En d'autres termes, l'interprétation du symbole = dans $\mathfrak{M}$ est le sous-ensemble $\{(x,x)|x \in M\}$ où M est l'ensemble de base de $\mathfrak{M}$.

Il se trouve que si ce n'est pas le cas, et si les axiomes de l'égalité font partie de la théorie $\mathscr{T}$, alors on peut s'y ramener :

Proposition 14 *Soit $\mathscr{T}$ une théorie sur une signature Σ, avec au moins le symbole = comme symbole de relation, qui contient tous les axiomes de l'égalité pour Σ.*

Si $\mathscr{T}$ possède un modèle, alors $\mathscr{T}$ possède un modèle égalitaire.

Démonstration: On peut quotienter le domaine M de tout modèle $\mathfrak{M}$ de $\mathscr{T}$ par la relation d'équivalence qui place dans la même classe d'équivalence x et y lorsque l'interprétation de $x = y$ est vraie dans $\mathfrak{M}$ (i.e. l'interprétation de =). Le modèle quotient, c'est-à-dire celui dont les éléments sont les classes d'équivalence de cette relation d'équivalence, est par définition égalitaire. □

Du coup, une théorie $\mathscr{T}$ possède un modèle égalitaire si et seulement si l'union de la théorie et des axiomes de l'égalité (pour la signature correspondante) possèdent un modèle.

Exemple 15 *Dans l'exemple 8, la phrase devrait être : les modèles égalitaires de la formule* (2) *caractérisent les triangles.*

Ou encore : la formule (2) *avec les axiomes de l'égalité (dans ce cas $\forall x\ x = x, \forall x \forall x' \forall y (x = x' \Rightarrow (R(x,y) \Rightarrow R(x',y))), \forall x \forall y \forall y' (y = y' \Rightarrow (R(x,y) \Rightarrow R(x,y'))))$) caractérise les triangles.*

1.5 Groupes

Commençons par parler des groupes, en théorie des groupes.

Exemple 16 (Groupe) *Un groupe est un modèle de la théorie constituée des axiomes de l'égalité et des deux formules :*

$$\forall x \forall y \forall z\ x * (y * z) = (x * y) * z \tag{3}$$

$$\exists e \forall x\ (x * e = e * x = x \wedge \exists y (x * y = y * x = e)) \tag{4}$$

sur la signature $\Sigma = (\emptyset, \{*\}, \{=\})$, où $*$ et $=$ sont d'arité 2.

La première propriété exprime le fait que la loi du groupe $*$ est associative, et la seconde qu'il existe un élément neutre, e, tel que tout élément possède un inverse.

Exemple 17 (Groupe commutatif) *Un groupe commutatif est un modèle de la théorie constituée des axiomes de l'égalité et des trois formules :*

$$\forall x \forall y \forall z\ x * (y * z) = (x * y) * z \tag{5}$$

$$\exists e \forall x\ (x * e = e * x = x \wedge \exists y (x * y = y * x = e)) \tag{6}$$

$$\forall x \forall y\ x * y = y * x \tag{7}$$

sur la même signature.

1.6 Corps

Exemple 18 (Corps commutatif) *Un* corps commutatif *est un modèle de la théorie constituée des axiomes de l'égalité et des formules*

$$\forall x \forall y \forall z\ (x + (y + z) = (x + y) + z) \tag{8}$$
$$\forall x \forall y (x + y = y + x) \tag{9}$$
$$\forall x (x + \mathbf{0} = x) \tag{10}$$
$$\forall x \exists y (x + y = \mathbf{0}) \tag{11}$$
$$\forall x \forall y \forall z\ x * (y + z) = x * y + x * z \tag{12}$$
$$\forall x \forall y \forall z\ ((x * y) * z) = (x * (y * z)) \tag{13}$$
$$\forall x \forall y\ (x * y = y * x) \tag{14}$$
$$\forall x\ (x * \mathbf{1} = x) \tag{15}$$
$$\forall x \exists y (x = \mathbf{0} \vee x * y = \mathbf{1}) \tag{16}$$
$$\neg \mathbf{1} = \mathbf{0} \tag{17}$$

sur une signature avec deux symboles de constantes $\mathbf{0}$ *et* $\mathbf{1}$*, deux symboles de fonctions* $+$ *et* $*$ *d'arité* 2*, et le symbole de relation* $=$ *d'arité 2.*

Par exemple $\mathbb{R}$ ou $\mathbb{C}$ avec l'interprétation standard sont des modèles de ces théories.

Si l'on ajoute à la théorie la formule F_p définie par $\mathbf{1} + \cdots + \mathbf{1} = \mathbf{0}$, où $\mathbf{1}$ est répété p fois, les modèles sont les corps de caractéristique p : par exemple $\mathbb{Z}_p$, lorsque p est premier.

Si l'on veut décrire un corps de caractéristique nulle, il faut considérer la théorie constituée des axiomes précédents et de l'union des négations des axiomes F_p, pour p un nombre premier.

Exemple 19 (Corps algébriquement clos) *Pour chaque entier* n*, on considère la formule* G_n

$$\forall x_0 \forall x_1 \cdots \forall x_{n-1} \exists x (x_0 + x_1 * x + x_2 * x^2 + \cdots + x_{n-1} * x^{n-1} + x^n = 0)$$

où le lecteur aura deviné que x^k *est* $x * \cdots * x$ *avec* x *répété* k *fois.*

Un corps commutatif algébriquement clos est un modèle de la théorie constituée des axiomes des corps commutatifs et de l'union des formules G_n *pour* $n \in \mathbb{N}$*.*

Par exemple, $\mathbb{C}$ est algébriquement clos. $\mathbb{R}$ n'est pas algébriquement clos, car $x^2 + 1$ ne possède pas de racine réelle.

1.7 Arithmétique de Robinson

On peut aussi chercher à axiomatiser les entiers. Voici une première tentative.

Exemple 20 (Arithmétique de Robinson) *Considérons la signature constituée du symbole de constante* $\mathbf{0}$*, d'une fonction unaire* s*, et de deux fonctions binaires* $+$ *et* $*$*, et des relations binaires* $<$ *et* $=$*.*

Les axiomes de l'arithmétique de Robinson sont les axiomes de l'égalité et

$$\forall x\ \neg s(x) = \mathbf{0} \tag{18}$$
$$\forall x\ \forall y\ (s(x) = s(y) \Rightarrow x = y) \tag{19}$$
$$\forall x\ (x = \mathbf{0} \vee \exists y\ \ s(y) = x) \tag{20}$$
$$\forall x\ \mathbf{0} + x = x \tag{21}$$
$$\forall x\ s(x) + y = s(x + y) \tag{22}$$
$$\forall x\ \mathbf{0} * x = \mathbf{0} \tag{23}$$
$$\forall x\ s(x) * y = x * y + y \tag{24}$$
$$\tag{25}$$

La structure dont l'ensemble de base est les entiers, et où l'on interprète $+$ par l'addition, $*$ par la multiplication, et $s(x)$ par $x+1$ est un modèle de cette théorie. On appelle ce modèle *le modèle standard des entiers.*

Exercice 5 *(corrigé page 239) Soit* n *et* m *deux entiers. On note* $s^n(\mathbf{0})$ *pour* $s(s(\cdots s(\mathbf{0})))$ *avec* s *répété* n *fois, avec la convention* $s^{(0)} = \mathbf{0}$*.*

Montrer par récurrence que

$$s^n(\mathbf{0}) + s^m(\mathbf{0}) = s^{n+m}(\mathbf{0}).$$

Trouver un modèle des axiomes de Robinson où deux éléments a *et* b *sont tels que* $a + b \neq b + a$*.*

En déduire que les axiomes de Robinson ne suffisent pas à axiomatiser les entiers : il y a d'autres modèles que le modèle standard des entiers de ces axiomes.

Exercice 6 *Ajoutons* $\forall x \forall y (x + y = y + x)$ *aux axiomes précédents pour garantir la commutativité de l'addition. Produire un modèle des axiomes obtenus qui n'est pas le modèle standard des entiers : par exemple, avec deux éléments* a *et* b *tels que* $a * b \neq b * a$*.*

Plutôt que de chercher à ajouter certains axiomes pour garantir des propriétés comme la commutativité de l'addition ou la multiplication, on va considérer des familles d'axiomes.

1.8 Arithmétique de Peano

Exemple 21 (Arithmétique de Peano) *Considérons une signature constituée du symbole de constante* $\mathbf{0}$*, d'une fonction unaire* s*, et de deux fonctions binaires* $+$ *et* $*$*, et de la relation binaire* $=$*.*

Les axiomes de l'arithmétique de Peano sont les axiomes de l'égalité et

$$\forall x\ \neg(s(x) = \mathbf{0}) \tag{26}$$
$$\forall x \forall y\ (s(x) = s(y) \Rightarrow x = y) \tag{27}$$
$$\forall x\ (x = \mathbf{0} \vee \exists y\ s(y) = x) \tag{28}$$
$$\forall x\ \mathbf{0} + x = x \tag{29}$$
$$\forall x\ s(x) + y = s(x + y) \tag{30}$$
$$\forall x\ \mathbf{0} * x = \mathbf{0} \tag{31}$$
$$\forall x\ s(x) * y = x * y + y \tag{32}$$
$$\tag{33}$$

et l'ensemble de toutes les formules de la forme

$$\forall x_1 \cdots \forall x_n((F(\mathbf{0}, x_1, \cdots, x_n) \wedge \forall x_0(F(x_0, x_1, \cdots, x_n) \Rightarrow F(s(x_0), x_1, \cdots, x_n)))$$

$$\Rightarrow \forall x_0 F(x_0, x_1, \cdots, x_n)) \tag{34}$$

où n *est n'importe quel entier et* $F(x_0, \cdots, x_n)$ *est n'importe quelle formule de variables libres* $x_0, \cdots, x_n$*.*

Il y a donc en fait une infinité d'axiomes. Les derniers axiomes visent à capturer le raisonnement par récurrence que l'on fait régulièrement sur les entiers.

Bien entendu, ces axiomes garantissent la propriété suivante : le modèle standard des entiers est un modèle de ces axiomes.

Exercice 7 *Prouver que l'axiome* $\forall x\ (x = \mathbf{0} \vee \exists y\ s(y) = x)$ *est en fait inutile : cette formule est conséquence des autres.*

Un intérêt est que cette fois on a :

Exercice 8 *(corrigé page 240) Prouver que dans tout modèle des axiomes de Peano, l'addition est commutative : la formule* $\forall x \forall y(x + y = y + x)$ *est satisfaite.*

Exercice 9 *Prouver que dans tout modèle des axiomes de Peano, la multiplication est commutative : la formule* $\forall x \forall y(x * y = y * x)$ *est satisfaite.*

Autrement dit, ces familles d'axiomes suffisent à garantir nombre des propriétés qui sont vraies sur les entiers.

On verra ultérieurement (théorème d'incomplétude) qu'il y a cependant d'autres modèles que le modèle standard des entiers des axiomes de Peano.

Remarquons que l'on peut définir dans tout modèle des axiomes de Peano précédents un ordre, par la règle $x < y$ ssi $\exists z\ (x + s(z) = y)$.

Une alternative est de prendre $<$ comme symbole de relation primitif d'arité 2 et d'ajouter les axiomes

$$\forall x\ \neg x < \mathbf{0} \tag{35}$$
$$\forall x\ \mathbf{0} = x \vee \mathbf{0} < x \tag{36}$$
$$\forall x\ \forall y\ (x < y \Leftrightarrow (s(x) < y \vee s(x) = y)) \tag{37}$$
$$\forall x\ \forall y\ (x < s(y) \Leftrightarrow (x < y \vee x = y)) \tag{38}$$

Exercice 10 *Prouver que l'ordre défini par la règle $x < y$ ssi $\exists z\ (x + s(z) = y)$ satisfait ces formules.*

Remarque 22 *La règle $x < y$ ssi $\exists z\ (x + s(z) = y)$ ne suiffit pas à défnir une relation ordre si l'un part seulement des axiomes de l'arithmétique de Robinson, et pas de ceux de Peano. Par contre, si l'on ajoute aux axiomes de Robinson un axiome qui impose la commutativité de l'addition à ces axiomes, on a bien une relation d'ordre.*

2 Complétude

Le *théorème de complétude*, dû à Kurt Gödel, et parfois appelé *premier théorème de Gödel*, relie la notion de conséquence à la notion de prouvabilité, en montrant que ces deux notions coïncident.

2.1 Conséquence

La notion de conséquence est facile à définir.

Définition 23 (Conséquence) *Soit F une formule. La formule F est dite* une conséquence (sémantique) *de la théorie $\mathcal{T}$ si tout modèle de la théorie $\mathcal{T}$ est un modèle de F. On note dans ce cas $\mathcal{T} \models F$.*

Exemple 24 *Par exemple, la formule $\forall x \forall y\ x * y = y * x$, qui exprime la commutativité, n'est pas une conséquence de la théorie des groupes (définition 16), car il y a des groupes qui ne sont pas commutatifs.*

Exemple 25 *On peut montrer que la formule* $\forall x\ \mathbf{0} + x = x$ *est une conséquence des axiomes de Peano.*

Exemple 26 *L'exercice 5 prouve que la formule* $\forall x \forall y (x + y = y + x)$ *(commutativité de l'addition) n'est pas une conséquence des axiomes de Robinson.*

2.2 Démonstration

Il faut aussi fixer la notion de démonstration, ce que nous allons faire, mais disons dans un premier temps que nous avons une notion de démonstration telle que l'on note $\mathscr{T} \vdash F$ si l'on peut prouver la formule close F à partir des axiomes de la théorie $\mathscr{T}$.

On espère au minimum de cette notion de preuve d'être valide : c'est-à-dire de dériver uniquement des conséquences : si F est une formule close, et si $\mathscr{T} \vdash F$, alors F est une conséquence de $\mathscr{T}$.

2.3 Énoncé du théorème de complétude

Le théorème de complétude dit en fait qu'on arrive à atteindre toutes les conséquences : les relations $\models$ et $\vdash$ sont les mêmes.

Théorème 27 (Théorème de complétude) *Soit* $\mathscr{T}$ *une théorie sur une signature dénombrable. Soit* F *une formule close.* F *est une conséquence de* $\mathscr{T}$ *si et seulement si* F *se prouve à partir de* $\mathscr{T}$.

2.4 Signification de ce théorème

Arrêtons-nous sur ce que cela signifie : autrement dit, **les énoncés démontrables sont exactement ceux qui sont vrais dans tous les modèles de la théorie.**

Cela signifie en particulier que

— si une formule close F n'est pas démontrable alors c'est qu'il existe un modèle qui n'est pas un modèle de F.

— si une formule close F est vraie dans tous les modèles des axiomes de la théorie, alors F est démontrable.

Exemple 28 *Par exemple, la formule* $\forall x \forall y\ x * y = y * x$*, qui exprime la commutativité, n'est pas démontrable à partir des axiomes de la théorie des groupes.*

Exemple 29 *La formule* $\forall x\ \mathbf{0} + x = x$ *est démontrable à partir des axiomes de Peano.*

2.5 Autre formulation du théorème

On dit qu'une théorie $\mathscr{T}$ est *cohérente* s'il n'existe pas de formule F telle que $\mathscr{T} \vdash F$ et $\mathscr{T} \vdash \neg F$.

On verra au détour de la preuve que cela revient aussi à dire :

Théorème 30 (Théorème de complétude) *Soit $\mathscr{T}$ une théorie sur une signature dénombrable. $\mathscr{T}$ possède un modèle si et seulement si $\mathscr{T}$ est cohérente.*

3 Preuve du théorème de complétude

3.1 Un système de déduction

Il nous faut définir une notion de démonstration. Nous choisissons de considérer une notion basée sur la notion de preuve à la Frege et Hilbert, c'est-à-dire basée sur le modus ponens.

Par rapport au calcul propositionnel, on n'utilise plus seulement la règle de modus ponens, mais aussi une règle de *généralisation* : si F est une formule et x une variable, la règle de généralisation déduit $\forall x F$ de F.

Cette règle peut être considérée comme troublante, mais c'est ce que l'on fait dans le raisonnement courant régulièrement : si on arrive à prouver $F(x)$ sans hypothèse particulière sur x, alors on saura que $\forall x F(x)$.

On considère alors un certain nombre d'axiomes :

Définition 31 (Axiomes logiques du calcul des prédicats) *Les* axiomes logiques du calcul des prédicats *sont :*

1. *toutes les instances des tautologies du calcul propositionnel ;*
2. *les axiomes des quantificateurs, c'est-à-dire*
   (a) *les formules de la forme $(\exists x F \Leftrightarrow \neg \forall x \neg F)$, où F est une formule quelconque et x une variable quelconque ;*
   (b) *les formules de la forme $(\forall x (F \Rightarrow G) \Rightarrow (F \Rightarrow \forall x G))$ où F et G sont des formules quelconques et x une variable qui n'a pas d'occurrence libre dans F ;*
   (c) *les formules de la forme $(\forall x F \Rightarrow F(t/x))$ où F est une formule, t un terme et aucune occurrence libre de x dans F ne se trouve dans le champ d'un quantificateur liant une variable de t, où $F(t/x)$ désigne la substitution de x par t.*

Exercice 11 *Montrer que les axiomes logiques sont valides.*

Remarque 32 *On pourrait ne pas mettre toutes les tautologies du calcul propositionnel, et comme pour le calcul propositionnel se limiter à certains axiomes, essentiellement les axiomes de la logique booléenne. Nous le faisons ici pour simplifier les preuves.*

On obtient la notion de démonstration.

Définition 33 (Démonstration par modus ponens et généralisation) *Soit une théorie $\mathcal{T}$ et soit une formule F. Une* preuve de F à partir de $\mathcal{T}$ *est une suite finie $F_1, F_2, \cdots, F_n$ de formules telle que F_n est égale à F, et pour tout i, ou bien F_i est dans $\mathcal{T}$, ou bien F_i est un axiome logique, ou bien F_i s'obtient par modus ponens à partir de deux formules F_j, F_k avec $j < i$ et $k < i$, ou bien F_i s'obtient à partir d'une formule F_j avec $j < i$ par généralisation.*

On note $\mathcal{T} \vdash F$ si F est démontrable à partir de $\mathcal{T}$.

3.2 Théorème de finitude

On obtient d'abord facilement au passage le théorème de finitude.

Théorème 34 (Théorème de finitude) *Pour toute théorie $\mathcal{T}$, et pour toute formule F, si $\mathcal{T} \vdash F$, alors il existe un sous-ensemble fini $\mathcal{T}_0$ de $\mathcal{T}$ tel que $\mathcal{T}_0 \vdash F$.*

Démonstration: Une démonstration est une suite finie de formules $F_1, F_2, \cdots, F_n$. Elle ne fait donc appel qu'à un nombre fini $\mathcal{T}_0$ de formules de $\mathcal{T}$. Cette démonstration est aussi une démonstration de F dans la théorie $\mathcal{T}_0$. □

Corollaire 35 *Si $\mathcal{T}$ est une théorie dont toutes les parties finies sont cohérentes, alors $\mathcal{T}$ est cohérente.*

Démonstration: Sinon $\mathcal{T}$ prouve $(F \wedge \neg F)$, pour une certaine formule F, et par le théorème de finitude on en déduit qu'il existe un sous-ensemble fini $\mathcal{T}_0$ de $\mathcal{T}$ qui prouve aussi $(F \wedge \neg F)$. □

3.3 Quelques résultats techniques

On aura besoin des résultats suivants, dont les preuves relèvent de jeux d'écriture ou de réécriture sur les démonstrations.

Tout d'abord une observation, qui a cependant son importance :

Lemme 36 *Si une théorie $\mathcal{T}$ n'est pas cohérente, alors toute formule est démontrable dans $\mathcal{T}$.*

Démonstration: En effet, supposons que $\mathcal{T} \vdash F$ et que $\mathcal{T} \vdash \neg F$, et soit G une formule quelconque. On peut alors mettre bout à bout une démonstration de F et une démonstration de $\neg F$. Pour obtenir une démonstration de G, il suffit d'ajouter les formules suivantes à cette suite : la tautologie $F \Rightarrow (\neg F \Rightarrow G)$. La formule $\neg F \Rightarrow G$ qui s'obtient alors par modus ponens, puisque F est déja apparue. Puis la formule G, qui s'obtient par modus ponens, puisque $\neg F$ est déja apparu. □

Lemme 37 (Lemme de déduction) *Supposons que $\mathcal{T} \cup \{F\} \vdash G$, avec F une formule close. Alors $\mathcal{T} \vdash (F \Rightarrow G)$.*

Démonstration: A partir d'une démonstration $G_0 G_1 \cdots G_n$ de G dans $\mathcal{T} \cup \{F\}$ on construit une démonstration de $(F \Rightarrow G)$ dans $\mathcal{T}$ en faisant des insertions dans la suite $(F \Rightarrow G_0)(F \Rightarrow G_1) \cdots (F \Rightarrow G_n)$.

Si G_i est une tautologie, alors il n'y a rien à faire car $(F \Rightarrow G_i)$ en est une aussi.

Si G_i est F, alors il n'y a rien à faire car $(F \Rightarrow G_i)$ est une tautologie.

Si G_i est un axiome des quantificateurs ou encore un élément de $\mathcal{T}$, alors il suffit d'insérer[1] entre $(F \Rightarrow G_{i-1})$ et $(F \Rightarrow G_i)$ les formules G_i et $(G_i \Rightarrow (F \Rightarrow G_i))$ (qui est une tautologie).

Supposons maintenant que G_i soit obtenue par modus ponens : il y a des entiers $j, k < i$ tels que G_k soit $(G_j \Rightarrow G_i)$. On insère alors entre $(F \Rightarrow G_{i-1})$ et $(F \Rightarrow G_i)$ les formules ;

1. $((F \Rightarrow G_j) \Rightarrow ((F \Rightarrow (G_j \Rightarrow G_i)) \Rightarrow (F \Rightarrow G_i)))$ (une tautologie) ;
2. $(F \Rightarrow (G_j \Rightarrow G_i)) \Rightarrow (F \Rightarrow G_i)$ qui s'obtient par modus ponens à partir de la précédente à l'aide de $(F \Rightarrow G_j)$ qui est déjà apparue ;
3. $(F \Rightarrow G_i)$ se déduit alors par modus ponens de cette dernière formule et de $(F \Rightarrow (G_j \Rightarrow G_i))$, qui est déjà apparue puisque c'est $(F \Rightarrow G_k)$.

Supposons enfin que G_i soit obtenue par généralisation à partir de G_j avec $j < i$. On insère dans ce cas entre $(F \Rightarrow G_{i-1})$ et $(F \Rightarrow G_i)$ les formules :

1. $\forall x (F \Rightarrow G_j)$ obtenue par généralisation en partant de $(F \Rightarrow G_j)$;
2. $(\forall x (F \Rightarrow G_j) \Rightarrow (F \Rightarrow \forall x G_j))$ (un axiome des quantificateurs). F étant une formule close, x n'y est pas libre ;
3. $(F \Rightarrow G_i)$ se déduit alors par modus ponens à partir des deux précédentes.

□

Le corollaire qui suit peut être vu comme la justification des preuves par l'absurde :

Corollaire 38 *$\mathcal{T} \vdash F$ si et seulement si $\mathcal{T} \cup \{\neg F\}$ n'est pas cohérente.*

Démonstration: Il est clair que si $\mathcal{T} \vdash F$ alors $\mathcal{T} \cup \{\neg F\}$ n'est pas cohérente. Réciproquement, si $\mathcal{T} \cup \{\neg F\}$ n'est pas cohérente, elle démontre n'importe quelle formule, et en particulier F par le lemme 36. Maintenant, par le lemme de déduction qui précède, on obtient que $\mathcal{T} \vdash \neg F \Rightarrow F$. Or $(\neg F \Rightarrow F) \Rightarrow F$ est une tautologie, ce qui montre que l'on a $\mathcal{T} \vdash F$. □

Lemme 39 *Soit $\mathcal{T}$ une théorie, et $F(x)$ une formule dont la seule variable libre est x. Soit c un symbole de constante qui n'apparaît ni dans F ni dans $\mathcal{T}$. Si $\mathcal{T} \vdash F(c/x)$ alors $\mathcal{T} \vdash \forall x F(x)$.*

1. Pour $i = 0$, il suffit de placer ces formules au début.

Démonstration: Considérons une démonstration $F_1F_2\cdots F_n$ de $F(c/x)$ dans $\mathscr{T}$. On considère une variable w qui n'est dans aucune formule F_i et on appelle K_i la formule obtenue en remplaçant dans F_i le symbole c par w.

Il s'avère que cela donne une preuve de $F(w/x)$: si F_i est un axiome logique, K_i aussi; si F_i se déduit par modus ponens, alors K_i se déduit des mêmes formules, et si $F_i \in \mathscr{T}$ alors K_i est F_i.

Par généralisation, on obtient donc une preuve de $\forall wF(w/x)$, et par la remarque qui suit, on peut alors obtenir une preuve de $\forall xF(x)$. □

Remarque 40 *Si w est une variable qui n'a aucune occurence dans F (ni libre ni liée) alors on peut prouver $\forall wF(w/x) \Rightarrow \forall xF$: en effet, puisque w n'a pas d'occurence dans F, on peut donc prouver $\forall wF(w/x) \Rightarrow F$, (axiome (c) des quantificateurs, en observant que $(F(w/x))(x/w) = F$ avec ces hypothèses). Par généralisation, on obtient $\forall x(\forall wF(w/x) \Rightarrow F)$, et puisque x n'est pas libre dans $\forall wF(w/x)$, la formule $\forall x(\forall wF(w/x) \Rightarrow F) \Rightarrow (\forall wF(w/x) \Rightarrow \forall xF)$ fait partie des axiomes (b) des quantificateurs, ce qui permet d'obtenir $\forall wF(w/x) \Rightarrow \forall xF$ par modus ponens.*

3.4 Validité du système de déduction

La validité de la méthode de preuve utilisée est facile à établir.

Théorème 41 (Validité) *Soit $\mathscr{T}$ une théorie. Soit F une formule.*
Si $\mathscr{T} \vdash F$, alors tout modèle de $\mathscr{T}$ est un modèle de la clôture universelle de F.

Démonstration: Il suffit de se convaincre que les axiomes logiques sont valides, et que le modus ponens et la généralisation ne font qu'inférer des faits qui sont valides dans tout modèle de $\mathscr{T}$. □

C'était le sens facile du théorème de complétude.

3.5 Complétude du système de déduction

L'autre sens consiste à montrer que si F est une conséquence de $\mathscr{T}$ alors F peut se prouver par notre méthode de preuve.

Définition 42

On dit qu'une théorie $\mathscr{T}$ est complète *si pour toute formule close F on a $\mathscr{T} \vdash F$ ou $\mathscr{T} \vdash \neg F$.*

On dit qu'une théorie $\mathscr{T}$ admet des témoins de Henkin *si pour toute formule $F(x)$ avec une variable libre x, il existe un symbole de constante c dans la signature tel que $(\exists xF(x) \Rightarrow F(c))$ soit une formule de la théorie $\mathscr{T}$.*

Le preuve du théorème de complétude due à *Henkin* que nous présentons ici fonctionne en deux étapes.

1. On montre qu'une théorie cohérente, complète, et avec des témoins de Henkin admet un modèle.

2. On montre que toute théorie consistante admet une extension avec ces trois propriétés.

Lemme 43 *Si $\mathcal{T}$ est une théorie cohérente, complète, et avec des témoins de Henkin, alors $\mathcal{T}$ possède un modèle.*

Démonstration: L'astuce est de construire de toutes pièces un modèle, dont l'ensemble de base (le domaine) est l'ensemble M des termes clos sur la signature de la théorie : ce domaine n'est pas vide, car la signature a au moins les constantes.

La structure $\mathfrak{M}$ est définie de la façon suivante :

1. si c est une constante, l'interprétation $c^{\mathfrak{M}}$ de c est la constante c elle-même.
2. si f est un symbole de fonction d'arité n, son interprétation $f^{\mathfrak{M}}$ est la fonction qui aux termes clos $t_1, \cdots, t_n$ associe le terme clos $f(t_1, \cdots, t_n)$.
3. si R est un symbole de relation d'arité n, son interprétation $R^{\mathfrak{M}}$ est le sous-ensemble de M^n constitué des $(t_1, \cdots, t_n)$ tels que $\mathcal{T} \vdash R(t_1, \cdots, t_n)$.

On observe que la structure obtenue vérifie la propriété suivante : pour toute formule close F, $\mathcal{T} \vdash F$ si et seulement si $\mathfrak{M}$ est un modèle de F. Cela se prouve par induction structurelle sur F.

La propriété est vraie pour les formules atomiques.

En raison des propriétés des quantificateurs et connecteurs, et de la possibilité d'utiliser des occurrences des tautologies du calcul propositionnel dans notre méthode de preuve, il suffit de se convaincre de ce fait inductivement sur les formules du type $\neg G$, $(G \vee H)$ et $\exists x G$.

1. Cas $\neg G$: puisque $\mathcal{T}$ est complète, $\mathcal{T} \vdash \neg G$ si et seulement si $\mathcal{T} \nvdash G$, ce qui signifie inductivement $\mathfrak{M} \not\models G$, ou encore $\mathfrak{M} \models \neg G$.
2. Cas $(G \vee H)$: supposons $\mathfrak{M} \models (G \vee H)$, et donc $\mathfrak{M} \models G$ ou $\mathfrak{M} \models H$. Dans le premier cas par exemple, par hypothèse d'induction on a $\mathcal{T} \vdash G$, et puisque $(G \Rightarrow (G \vee H))$ est une tautologie, on a $\mathcal{T} \vdash (G \vee H)$. Réciproquement supposons que $\mathcal{T} \vdash (G \vee H)$. Si $\mathcal{T} \vdash G$ alors par hypothèse d'induction $\mathfrak{M} \models G$ et donc $\mathfrak{M} \models (G \vee H)$. Sinon, c'est que $\mathcal{T} \nvdash G$, et parce que la théorie est complète, on a $\mathcal{T} \vdash \neg G$. Or puisque $(G \vee H \Rightarrow (\neg G \Rightarrow H))$ est une tautologie, on obtient que $\mathcal{T} \vdash H$ et par hypothèse d'induction, $\mathfrak{M} \models H$ et donc $\mathfrak{M} \models (G \vee H)$.
3. Cas $\exists x G(x)$: si $\mathfrak{M} \models \exists x G(x)$ c'est qu'il existe un terme clos t tel que $\mathfrak{M} \models G(t/x)$. Par hypothèse d'induction, $\mathcal{T} \vdash G(t/x)$. Or il est facile de trouver une démonstration formelle de $\exists x G(x)$ à partir d'une de $G(t/x)$. Réciproquement, supposons que $\mathcal{T} \vdash \exists x G(x)$. Grâce aux témoins de Henkin, on en déduit qu'il existe une constante c telle que $\mathcal{T} \vdash G(c/x)$, et par hypothèse d'induction $\mathfrak{M} \models G(c/x)$, et donc $\mathfrak{M} \models \exists x G(x)$.

□

Il reste la seconde étape. Une *extension d'une théorie $\mathcal{T}$* est une théorie $\mathcal{T}'$ qui contient $\mathcal{T}$.

Proposition 44 *Toute théorie cohérente $\mathscr{T}$ sur une signature Σ dénombrable possède une extension $\mathscr{T}'$ sur une signature Σ' (avec Σ' qui contient Σ) dénombrable qui est cohérente, complète et avec des témoins de Henkin.*

Avant de prouver cette proposition, discutons de ce que nous obtenons : puisqu'un modèle de $\mathscr{T}'$ est un modèle de $\mathscr{T}$, le lemme précédent et la proposition précédente permettent tout d'abord d'obtenir :

Corollaire 45 *Une théorie cohérente dénombrable possède un modèle.*

La remarque suivante relève d'un jeu sur les définitions :

Proposition 46 *Pour toute théorie $\mathscr{T}$ et pour toute formule close F, F est une conséquence de T si et seulement si $\mathscr{T} \cup \{\neg F\}$ n'a pas de modèle.*

Démonstration: Si F est une conséquence de $\mathscr{T}$, alors par définition tout modèle de $\mathscr{T}$ est un modèle de F, autrement dit, il n'y pas de modèle de $\mathscr{T} \cup \{\neg F\}$. La réciproque est triviale. □

On obtient avec cette remarque exactement le théorème de complétude (ou le sens manquant de ce que nous avons appelé le théorème de complétude).

Théorème 47 *Soit F une formule close. Si F est une conséquence de la théorie $\mathscr{T}$, alors $\mathscr{T} \vdash F$.*

Démonstration: Si $\mathscr{T}$ ne prouve pas F, alors $\mathscr{T} \cup \{\neg F\}$ est cohérente : par le corollaire précédent, $\mathscr{T} \cup \{\neg F\}$ possède donc un modèle. Cela veut donc dire que F n'est pas une conséquence de la théorie $\mathscr{T}$. □

Il ne reste plus qu'à prouver la proposition 44.

Démonstration: La signature Σ' est obtenue en ajoutant un nombre dénombrable de nouvelles constantes à la signature Σ. La signature Σ' obtenue reste dénombrable et on peut énumérer les formules closes $(F_n)_{n\in\mathbb{N}}$ de Σ'. La théorie $\mathscr{T}'$ est obtenue comme l'union d'une suite croissante de théories $\mathscr{T}_n$, définie par récurrence, en partant de $\mathscr{T}_0 = \mathscr{T}$. Supposons $\mathscr{T}_n$ cohérente construite. Pour construire $\mathscr{T}_{n+1}$ on considère la formule F_{n+1} dans l'énumération des formules closes de Σ'. Si $\mathscr{T}_n \cup F_{n+1}$ est cohérente, alors on pose $G_n = F_{n+1}$, sinon on pose $G_n = \neg F_{n+1}$. Dans les deux cas $\mathscr{T}_n \cup \{G_n\}$ est cohérente.

La théorie $\mathscr{T}_{n+1}$ est définie par :

1. $\mathscr{T}_{n+1} = \mathscr{T}_n \cup \{G_n\}$ si G_n n'est pas de la forme $\exists x H$.
2. sinon : $\mathscr{T}_{n+1} = \mathscr{T}_n \cup \{G_n, H(c/x)\}$ où c est un nouveau symbole de constante qui n'apparaît dans aucune formule de $T_n \cup \{G_n\}$: il y a toujours un tel symbole, car il y a un nombre fini de symboles de constantes dans $T_n \cup \{G_n\}$.

La théorie $\mathscr{T}_{n+1}$ est cohérente : en effet, si elle ne l'était pas, alors cela voudrait dire que G_n serait de la forme $\exists x H$, et que $T_n \cup \{\exists x H\} \vdash \neg H(c/x)$. Par le choix de la constante c, et par le lemme 39, on obtient que $T_n \cup \{\exists x H\} \vdash \forall x \neg H(x)$, ce qui est impossible car sinon $\mathscr{T}_n$ ne serait pas cohérente.

La théorie $\mathcal{T}' = \bigcup_{n\in\mathbb{N}} \mathcal{T}_n$ définie comme l'union des théories $\mathcal{T}_n$ est cohérente, puisque tout sous-ensemble fini de celle-ci est contenu dans l'une des théories $\mathcal{T}_n$, et donc est cohérent.

La théorie $\mathcal{T}'$ est aussi complète : si F est une formule close de Σ', elle apparaît à un moment dans l'énumération des formules F_n, et par construction, soit $F_n \in \mathcal{T}_n$ soit $\neg F_n \in \mathcal{T}_n$.

Enfin la théorie $\mathcal{T}'$ a des témoins de Henkin : si $H(x)$ est une formule avec la variable libre x, alors la formule $\exists x H$ apparaît comme une formule dans l'énumération des formules F_n. Il y a alors deux cas, soit $\neg F_n \in \mathcal{T}_{n+1}$ ou il y a une constante c telle que $H(c/x) \in \mathcal{T}_{n+1}$. Dans les deux cas, $\mathcal{T}_{n+1} \vdash \exists x H(x) \Rightarrow H(c/x)$, ce qui prouve que $(\exists x H(x) \Rightarrow H(c/x))$ est dans $\mathcal{T}'$ (sinon sa négation y serait, et $\mathcal{T}'$ ne serait pas cohérente). □

4 Compacité

Observons que l'on a en fait établi d'autres faits.

Théorème 48 (Théorème de compacité) *Soit $\mathcal{T}$ une théorie sur une signature dénombrable telle que toute partie finie de $\mathcal{T}$ possède un modèle. Alors $\mathcal{T}$ possède un modèle.*

Démonstration: Considérons un sous-ensemble fini d'une telle théorie $\mathcal{T}$. Ce sous-ensemble est cohérent puisqu'il a un modèle. $\mathcal{T}$ est donc une théorie telle que toute partie finie soit cohérente. Par le théorème de finitude, cela veut dire que la théorie elle-même est cohérente.

Par le corollaire 45, cela veut dire que $\mathcal{T}$ possède un modèle. □

Exercice 12 *(corrigé page 240) Utiliser le théorème de compacité pour prouver qu'il existe des modèles non-standards des axiomes de Peano.*

5 Autres conséquences

Théorème 49 (Löwenheim-Skolem) *Si $\mathcal{T}$ une théorie sur une signature dénombrable possède un modèle, alors elle possède un modèle dont l'ensemble de base est dénombrable.*

Exercice 13 *(corrigé page 240) Prouver le théorème.*

6 Notes bibliographiques

Lectures conseillées Pour aller plus loin sur les notions évoquées dans ce chapitre, nous suggérons la lecture de [Cori & Lascar, 1993], [Dowek, 2008] ainsi que la lecture

du livre [Lassaigne & de Rougemont, 2004].

Bibliographie Ce chapitre a été rédigé en s'inspirant essentiellement des ouvrages [Cori & Lascar, 1993] et [Lassaigne & de Rougemont, 2004].

Index

Bibliographie

[Cori & Lascar, 1993] Cori, R. & Lascar, D. (1993). *Logique mathématique. Volume I*. Masson.

[Dowek, 2008] Dowek, G. (2008). *Les démonstrations et les algorithmes*. Polycopié du cours de l'Ecole Polytechnique.

[Lassaigne & de Rougemont, 2004] Lassaigne, R. & de Rougemont, M. (2004). *Logic and complexity*. Discrete Mathematics and Theoretical Computer Science. Springer. https://doi.org/10.1007/978-0-85729-392-3