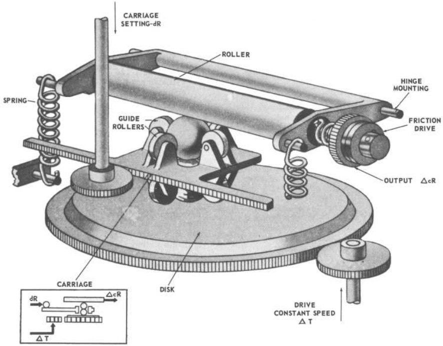
Cours 3: Complétude. Grands théorèmes de la logique. Incomplétude de la logique du premier ordre.



Olivier Bournez
bournez@lix.polytechnique.fr

Ecole Polytechnique
INF423

Retour sur l'épisode précédent

- On a introduit le calcul des prédicats :
  - Syntaxe :
  - Sémantique :

Retour sur l'épisode précédent

- On a introduit le calcul des prédicats :
  - Syntaxe :
    - Etant fixée une signature $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$,
  - Sémantique :

Retour sur l'épisode précédent

- On a introduit le calcul des prédicats :
  - Syntaxe :
    - Etant fixée une signature $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$,
    - On définit la notion de **terme**, **terme clos**, **formule atomique**, **formule**, **formule close** sur cette signature.
  - Sémantique :

Retour sur l'épisode précédent

- On a introduit le calcul des prédicats :
  - Syntaxe :
    - Etant fixée une signature $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$,
    - On définit la notion de **terme**, **terme clos**, **formule atomique**, **formule**, **formule close** sur cette signature.
  - Sémantique :
    - Etant donnée une structure $\mathfrak{M}$ de signature Σ de domaine M,

Retour sur l'épisode précédent

- On a introduit le calcul des prédicats :
  - Syntaxe :
    - Etant fixée une signature $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$,
    - On définit la notion de **terme**, **terme clos**, **formule atomique**, **formule**, **formule close** sur cette signature.
  - Sémantique :
    - Etant donnée une structure $\mathfrak{M}$ de signature Σ de domaine M,
    - et pour une valuation v, on définit **l'interprétation d'un terme, d'une formule atomique et d'une formule pour cette valuation**.

- Pour une formule close F, la satisfaction de F dans la structure $\mathfrak{M}$ ne dépend pas de la valuation v.

- On dit alors que $\mathfrak{M}$ est un modèle de F, lorsque F est satisfaite sur $\mathfrak{M}$.

Théories

- Une **théorie** $\mathcal{T}$ est un ensemble de formules closes sur une signature donnée. Les formules d'une théorie sont appelées des **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.

- Une théorie est dite **consistante** si elle possède un modèle.

Au menu

Plus précisément

Premiers exemples de théories du premier ordre

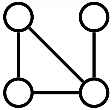
- Graphe
- Groupes
- Corps

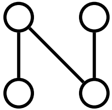
Graphe

- Un graphe orienté peut se voir comme un modèle de la théorie sans axiome sur la signature $(\emptyset, \emptyset, \{R\})$.

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

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

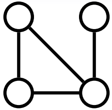


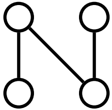


Pour la signature $(\emptyset, \emptyset, \{=, R\})$, la formule

$$\exists x \forall y (\neg(x = y) \Rightarrow R(x, y))$$

est satisfaite sur le premier et pas sur le second.





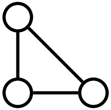
Pour la signature $(\emptyset, \emptyset, \{=, R\})$, la formule

$$\exists x \forall y (\neg(x = y) \Rightarrow R(x, y))$$

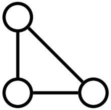
est satisfaite sur le premier et pas sur le second.

(Remarque : Sur cette signature comme sur la signature $\Sigma = (\emptyset, \emptyset, \{R\})$, il n'y a aucun terme).

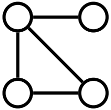
- On considère la signature $(\{a, b, c\}, \emptyset, \{R\})$

- On considère la signature $(\{a, b, c\}, \emptyset, \{R\})$
- 

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

- On considère la signature $(\{a, b, c\}, \emptyset, \{R\})$
- 

  est un modèle de $R(a, b) \wedge R(b, c) \wedge R(a, c)$.
- Attention :

  aussi.

Plus précisément

Premiers exemples de théories du premier ordre

- Graphe
- Groupes
- Corps

Groupe

- Un groupe est un modèle égalitaire[1] de la théorie constituée des deux formules :

$$\forall x \forall y \forall z \; x * (y * z) = (x * y) * z \qquad (2)$$

$$\exists e \forall x \; (x * e = e * x = x \wedge \exists y (x * y = y * x = e)) \qquad (3)$$

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

1. On impose à l'interprétation de $=$ de correspondre à l'égalité.

Plus précisément

Premiers exemples de théories du premier ordre

- Graphe
- Groupes
- Corps

Corps

- Un **corps commutatif** est un modèle égalitaire de la théorie constituée des formules

$$\forall x \forall y \forall z\ (x + (y + z) = (x + y) + z) \tag{4}$$
$$\forall x \forall y (x + y = y + x) \tag{5}$$
$$\forall x (x + \mathbf{0} = x) \tag{6}$$
$$\forall x \exists y (x + y = \mathbf{0}) \tag{7}$$
$$\forall x \forall y \forall z\ x * (y + z) = x * y + x * z \tag{8}$$
$$\forall x \forall y \forall z\ ((x * y) * z) = (x * (y * z)) \tag{9}$$
$$\forall x \forall y\ (x * y = y * x) \tag{10}$$
$$\forall x\ (x * \mathbf{1} = x) \tag{11}$$
$$\forall x \exists y (x = \mathbf{0} \vee x * y = \mathbf{1}) \tag{12}$$
$$\neg \mathbf{1} = \mathbf{0} \tag{13}$$

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.

- Corps de caractéristique p :
  - On ajoute à la théorie précédente la formule F_p définie par $\mathbf{1} + \cdots + \mathbf{1} = \mathbf{0}$, où $\mathbf{1}$ est répété p fois.
- Corps de caractéristique 0 :
  - On ajoute à la théorie précédente l'union des formules $\neg F_2, \cdots, \neg F_p$ pour p un nombre premier.
- 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 x^k est $x * \cdots * x$ avec x répété k fois.
  - on ajoute à la théorie précédente l'union des formules G_n pour $n \in \mathbb{N}$.

Exercice : corps réel clos

- Un **corps réel clos** est un corps totalement ordonné F tel que tout élément positif soit un carré et que tout polynôme de degré impair à coefficients dans F ait au moins une racine dans F.
  - $\mathbb{R}$ est un corps réel clos.
- Cela correspond à une théorie du calcul des prédicats.

Au menu

Un système de déduction

- Il nous faut définir une notion de démonstration
  - c'est-à-dire $\mathcal{T} \vdash F$.
- Nous choisissons de considérer une notion basée sur la notion de preuve à la Frege et Hilbert.

Règle de généralisation

- 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.

$$\frac{F}{\forall x F}$$

- Règle troublante ?

Règle de généralisation

- 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.

$$\frac{F}{\forall x F}$$

- Règle troublante ?
  - non, 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 $\forall x F(x)$.

Axiomes logiques

- 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

     2.1 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 ;

     2.2 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 ;

     2.3 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.

Preuve par modus ponens et généralisation

- Soit $\mathcal{T}$ une théorie et F une formule.

- 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'un formule F_j avec $j < i$ par généralisation.

- Et on note $\mathcal{T} \vdash F$ dans ce cas.

Théorème de complétude

- Ce système de déduction est valide et complet.
  - Rappel : $\mathcal{T} \vdash F$ pour “F se prouve à partir de $\mathcal{T}$” dans ce système.
  - Notons : $\mathcal{T} \models F$ pour “tout modèle de $\mathcal{T}$ est un modèle de F.”
- C’est-à-dire :
- Théorème de Validité : Soit $\mathcal{T}$ une théorie. Soit F une formule close.
  Si $\mathcal{T} \vdash F$ alors $\mathcal{T} \models F$.
- Théorème de Complétude. Soit $\mathcal{T}$ une théorie. Soit F une formule close.
  Si $\mathcal{T} \models F$ alors $\mathcal{T} \vdash F$.

Autre façon de comprendre ce qu'on obtient :

- prouvabilité et conséquence (sémantique) sont les mêmes notions.

$$\mathcal{T} \vdash F \text{ si et seulement si } \mathcal{T} \models F.$$

Autre façon de le comprendre :

$$\boxed{F \text{ est prouvable ssi } F \text{ est vraie dans tous les modèles}}$$

Autre façon de le comprendre :

$$\boxed{\boxed{F \text{ est prouvable ssi } F \text{ est vraie dans tous les modèles}}}$$

- F est prouvable à partir des axiomes $\mathcal{T}$ ssi F est vraie dans tous les modèles de $\mathcal{T}$.

Au menu

Plus précisément

Exemples de théories du premier ordre

- Arithmétique de Peano : première tentative
- Arithmétique de Peano

Axiomes de l'arithmétique

- 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 $=$.

- On souhaite que $(\mathbb{N}, =, s, +, *, 0)$ en soit un modèle.

1ière tentative

- On considère les axiomes

$$\forall x \ \neg s(x) = \mathbf{0} \tag{14}$$

$$\forall x \forall y \ (s(x) = s(y) \Rightarrow x = y) \tag{15}$$

$$\forall x \ (x = \mathbf{0} \vee \exists y \ s(y) = x) \tag{16}$$

$$\forall x \ \mathbf{0} + x = x \tag{17}$$

$$\forall x \ s(x) + y = s(x + y) \tag{18}$$

$$\forall x \ \mathbf{0} * x = 0 \tag{19}$$

$$\forall x \ s(x) * y = x * y + y \tag{20}$$

Conséquence/Non-conséquence

- Rappel : une formule F est dite une **conséquence** d'un ensemble de formules $\mathcal{T}$ si tout modèle de la théorie $\mathcal{T}$ est un modèle de F.
  - se note : $\mathcal{T} \models F$

Conséquence/Non-conséquence

- Rappel : une formule F est dite une **conséquence** d'un ensemble de formules $\mathcal{T}$ si tout modèle de la théorie $\mathcal{T}$ est un modèle de F.
  - se note : $\mathcal{T} \models F$
- Comment se persuader qu'une formule close n'est pas une conséquence de $\mathcal{T}$?

Conséquence/Non-conséquence

- Rappel : une formule F est dite une **conséquence** d'un ensemble de formules $\mathcal{T}$ si tout modèle de la théorie $\mathcal{T}$ est un modèle de F.
  - se note : $\mathcal{T} \models F$
- Comment se persuader qu'une formule close n'est pas une conséquence de $\mathcal{T}$?
  - en exhibant un modèle de $\mathcal{T}$ qui n'est pas un modèle de F.

Faits

- Pour chaque entier n et m, la formule

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

  est une conséquence des axiomes précédents, où $s^n(\mathbf{0})$ est $s(s(\cdots s(\mathbf{0})))$ avec s répété n fois.

Faits

- Pour chaque entier n et m, la formule

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

  est une conséquence des axiomes précédents, où $s^n(\mathbf{0})$ est $s(s(\cdots s(\mathbf{0})))$ avec s répété n fois.

- Mais

$$\forall x \forall y \; x + y = y + x$$

  n'est pas une conséquence de ces axiomes.

Un modèle où l'addition n'est pas commutative

- Soit X un ensemble avec au moins deux éléments.
- On considère la structure $\mathfrak{M}$ dont l'ensemble de base est

$$M = \mathbb{N} \cup (X \times \mathbb{Z}),$$

  et où les symboles $s, +, *, =$ sont interprétés par les conditions suivantes :
  - $=$ est interprété par l'égalité. $s, +, *$ étendent les fonctions correspondantes sur $\mathbb{N}$;
  - pour $a = (x, n)$:
    - $s(a) = (x, n+1)$;
    - $a + m = m + a = (x, n+m)$;
    - $a * m = (x, n * m)$ si $m \neq 0$, et $(x, n) * 0 = 0$;
    - $m * a = (x, m * n)$;
  - pour $a = (x, n)$ et $b = (y, m)$:
    - $(x, n) + (y, m) = (x, n+m)$;
    - $(x, n) * (y, m) = (x, n * m)$.

- Ce modèle est un modèle des axiomes précédents.
- L'addition n'y est pas commutative.

Plus précisément

Exemples de théories du premier ordre

- Arithmétique de Peano : première tentative
- Arithmétique de Peano

Idée des axiomes de Peano

- ajouter une famille (un schéma) d'axiomes pour permettre les preuves par récurrence.

- cette fois l'addition sera bien nécessairement commutative, i.e.

$$\forall x \forall y \; x + y = y + x$$

  sera bien toujours satisfaite.

  - et on capture en pratique toutes les propriétés de l'arithmétique.

Axiomes de Peano

- Les axiomes de l'arithmétique de Peano sont :
  - les axiomes précédent
  - et l'ensemble de toutes les formules de la forme

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

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

Axiomes de Peano

- Les axiomes de l'arithmétique de Peano sont :
  - les axiomes précédent + ceux de l'égalité ;
  - et l'ensemble de toutes les formules de la forme

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

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

Au menu

Plus précisément

Grands théorèmes du calcul des prédicats

- Théorème de complétude
- Théorème de compacité
- Théorème d'incomplétude

Retour sur l'énoncé

- On peut construire un (des) système(s) de preuve valide(s) et complet(s) :
  - Notons : $\mathcal{T} \vdash F$ pour "F se prouve à partir de $\mathcal{T}$" dans ce système.
  - Notons : $\mathcal{T} \models F$ pour "tout modèle de $\mathcal{T}$ est un modèle de F."
- C'est-à-dire :
- Théorème de Validité : Soit $\mathcal{T}$ une théorie. Soit F une formule close.
  Si $\mathcal{T} \vdash F$ alors $\mathcal{T} \models F$.
- Théorème de Complétude. Soit $\mathcal{T}$ une théorie. Soit F une formule close.
  Si $\mathcal{T} \models F$ alors $\mathcal{T} \vdash F$.

Autre façon de comprendre ce qu'on obtient :

- prouvabilité et conséquence sémantique sont les mêmes notions.

$$\mathcal{T} \vdash F \text{ si et seulement si } \mathcal{T} \models F.$$

Autre façon de le comprendre :

$$\boxed{\boxed{F \text{ est prouvable ssi } F \text{ est vraie dans tous les modèles}}}$$

Autre façon de le comprendre :

$$\boxed{\boxed{\text{F est prouvable ssi F est vraie dans tous les modèles}}}$$

- F prouvable à partir des axiomes $\mathcal{T}$ ssi F est vraie dans tous les modèles de $\mathcal{T}$.

Autres formulations équivalentes du théorème de complétude

- Une théorie $\mathcal{T}$ est dite cohérente s'il n'existe pas de formule F telle que $\mathcal{T} \vdash F$ et $\mathcal{T} \vdash \neg F$.
- 3 formulations équivalentes du théorème de Complétude.

  1. Si $\mathcal{T} \models F$ alors $\mathcal{T} \vdash F$.
  2. Si F n'est pas prouvable à partir de $\mathcal{T}$ alors $\mathcal{T} \cup \{\neg F\}$ possède un modèle.
  3. **Si $\mathcal{T}$ est cohérente, alors $\mathcal{T}$ possède un modèle.**

Autres formulations équivalentes du théorème de complétude

- Une théorie $\mathcal{T}$ est dite cohérente s'il n'existe pas de formule F telle que $\mathcal{T} \vdash F$ et $\mathcal{T} \vdash \neg F$.
- 3 formulations équivalentes du théorème de Complétude.
  1. Si $\mathcal{T} \models F$ alors $\mathcal{T} \vdash F$.
  2. Si F n'est pas prouvable à partir de $\mathcal{T}$ alors $\mathcal{T} \cup \{\neg F\}$ possède un modèle.
  3. **Si $\mathcal{T}$ est cohérente, alors $\mathcal{T}$ possède un modèle.**
- Equivalences :
  - Entre 1. et 2. trivial (contraposé).
  - 2. implique 3. : trivial.
  - 3. implique 2. :
    - soit F non prouvable dans $\mathcal{T}$.
    - $\mathcal{T} \cup \{\neg F\}$ est cohérente.
    - $\mathcal{T} \cup \{\neg F\}$ possède donc un modèle $\mathfrak{M}$.

Effet de bord [2]

- Théorème de 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.

2. De la preuve du théorème de complétude.

Plus précisément

Grands théorèmes du calcul des prédicats

- Théorème de complétude
- Théorème de compacité
- Théorème d'incomplétude

Effet de bord [3]

- Théorème de Compacité.
  - Soit $\mathcal{T}$ une théorie.
  - $\mathcal{T}$ possède un modèle si et seulement si toute partie finie de $\mathcal{T}$ possède un modèle.

3. De la nature de ce que l'on appelle une preuve :
du fait qu'une preuve fait intervenir un nombre fini de formules.

Plus précisément

Grands théorèmes du calcul des prédicats

- Théorème de complétude
- Théorème de compacité
- Théorème d'incomplétude

- On note $Th(\mathbb{N})$ l'ensemble des formules closes F qui sont vraies sur les entiers.

- Théorème d'incomplétude.

  - Il existe des formules closes de $Th(\mathbb{N})$ qui ne sont pas prouvables, à partir des axiomes de Peano, ou de toute axiomatisation "raisonnable"[4] des entiers.

- Second théorème d'incomplétude.

  - La cohérence de l'arithmétique (ou sa négation) est un exemple de telle formule.

4. Formellement, "récursivement énumérable" : voir suite du cours.

Au menu

Entiers non-standards

- Il y a d'autres modèles que $\mathbb{N}$ des axiomes de Peano.
  - il existe des modèles **non-standards** de l'arithmétique.

Corps réels clos

- Application du théorème de Löwenheim-Skolem :
  - il existe des corps réels clos dénombrables.

Corps réels clos

- Application du théorème de Löwenheim-Skolem :
  - il existe des corps réels clos dénombrables.
    - (exemple : les réels algébriques $\overline{\mathbb{Q}} \cap \mathbb{R}$).

Entiers non-standards

- Il y a d'autres modèles que $\mathbb{N}$ des axiomes de Peano :
  - considérons un nouveau symbole de constante c.
  - considérons $\mathcal{T}$ défini comme l'union des axiomes de Peano et des formules $\neg c = s^n(\mathbf{0})$, pour n un entier.
  - Tout sous-ensemble fini de $\mathcal{T}$ admet un modèle, car il est inclus dans l'union des axiomes de Peano et des formules $\neg c = s^n(\mathbf{0})$ pour $1 \leq n \leq N$ pour un certain entier N :
    - il suffit d'interpréter c par $N + 1$.
  - Donc $\mathcal{T}$ admet un modèle.
- Ce modèle contient donc un élément qui n'est pas un entier standard.

⋮

Analyse non-standard

⋮

. . .f est continue si et seulement si pour tout y infiniment petit et pour tout réel x standard, $f(x+y)-f(x)$ est infiniment petit . . .

⋮

Deux autres utilisations de la logique

- Comment prouver qu'un axiome F est indépendant d'une théorie $\mathcal{T}$?
  - On utilise un modèle de $\mathcal{T}$ pour construire un modèle de $\mathcal{T} \cup \{F\}$.
  - On prouve en fait la **cohérence relative** : si $\mathcal{T}$ cohérent, alors $\mathcal{T} \cup \{F\}$ cohérent.
- Définissabilité :
  - On se donne un modèle d'une théorie sur une signature contenant un symbole de relation R binaire.
  - Peut-on définir :
    - la relation "être accessible en deux coups" par une formule ?
    - la relation "être accessible par un chemin" ?
  - ...applications aux requêtes dans les bases de données ...

Exprimez vous.

Page du cours.

Commentaires, avis
sur les cours et les PCs.

- Page du cours:
  www.enseignement.polytechnique.fr/informatique/INF423.
- Commentaires, avis sur les cours et les PCs.
  www.enseignement.polytechnique.fr/informatique/INF423/AVIS.

ANNEXES

Substitutions

- Début d'une parenthèse : que signifie exactement $F(t/x)$?

Substitutions

- Début d'une parenthèse : que signifie exactement $F(t/x)$?
  - $F(4/x)$ pour $F = \forall x P(x)$:
    - $\forall x \; P(4)$
    - $\forall x \; P(x)$?

Substitutions

- Début d'une parenthèse : que signifie exactement $F(t/x)$?
  - $F(4/x)$ pour $F = \forall x P(x)$:
    - $\forall x\ P(4)$
    - $\forall x\ P(x)$?
- Règle 1 : ne substituer que les variables libres.

Substitutions

- Début d'une parenthèse : que signifie exactement $F(t/x)$?
  - $F(4/x)$ pour $F = \forall x P(x)$:
    - $\forall x \; P(4)$
    - $\forall x \; P(x)$?
- Règle 1 : ne substituer que les variables libres.
- Mais cela ne suffit pas :

Substitutions

- Début d'une parenthèse : que signifie exactement $F(t/x)$?
  - $F(4/x)$ pour $F = \forall x P(x)$:
    - $\forall x \; P(4)$
    - $\forall x \; P(x)$?
- Règle 1 : ne substituer que les variables libres.
- Mais cela ne suffit pas :
  - $F(x/y)$ pour $F = \forall x \; P(x + y)$?
    - si on écrit $\forall x \; P(x + x)$, l'occurence libre de x a été capturée.

Substitutions

- Début d'une parenthèse : que signifie exactement $F(t/x)$?
  - $F(4/x)$ pour $F = \forall x P(x)$:
    - $\forall x \; P(4)$
    - $\forall x \; P(x)$?
- Règle 1 : ne substituer que les variables libres.
- Mais cela ne suffit pas :
  - $F(x/y)$ pour $F = \forall x \; P(x + y)$?
    - si on écrit $\forall x \; P(x + x)$, l'occurence libre de x a été capturée.
- Règle 2 : éviter les captures de variables

Substitutions

- Début d'une parenthèse : que signifie exactement $F(t/x)$?
  - $F(4/x)$ pour $F = \forall x P(x)$:
    - $\forall x\ P(4)$
    - $\forall x\ P(x)$?
- Règle 1 : ne substituer que les variables libres.
- Mais cela ne suffit pas :
  - $F(x/y)$ pour $F = \forall x\ P(x+y)$?
    - si on écrit $\forall x\ P(x+x)$, l'occurence libre de x a été capturée.
- Règle 2 : éviter les captures de variables
  - $F(x/y)$ pour $F = \forall x\ P(x+y)$ est $\forall w\ P(w+x)$.

Substitutions

- Début d'une parenthèse : que signifie exactement $F(t/x)$?
  - $F(4/x)$ pour $F = \forall x P(x)$:
    - $\forall x \; P(4)$
    - $\forall x \; P(x)$?
- Règle 1 : ne substituer que les variables libres.
- Mais cela ne suffit pas :
  - $F(x/y)$ pour $F = \forall x \; P(x + y)$?
    - si on écrit $\forall x \; P(x + x)$, l'occurence libre de x a été capturée.
- Règle 2 : éviter les captures de variables
  - $F(x/y)$ pour $F = \forall x \; P(x + y)$ est $\forall w \; P(w + x)$.
  - besoin de renommer.... équivalence alphabétique.

Plus formellement : étape 1. Renommage de variables

- Etape 1 : définir ce qu'est le renommage d'une variable liée, appelé α-conversion.
  - on définit pour cela l'échange de deux variables sur F.
  - Notation : $(xy)F$:
    - partout où l'on a écrit x lié ou non-lié, on met y et vice-versa.
    - $\exists x\ F$ est identifié avec $\exists y\ (xy)F$ si $y \notin \ell(F)$.
    - $\forall x\ F$ est identifié avec $\forall y\ (xy)F$ si $y \notin \ell(F)$.

Plus formellement : étape 2. Substitutions

- Etape 2 : définir $F(t/x)$ inductivement.
  - sur les termes : trivial.
  - sur les formules qui ne sont pas de la forme $\exists yG$ ou $\forall yG$: inductif.
  - $(\exists y\ G)(t/x)$ est $\exists y\ G(t/x)$ si $x \neq y$ et $y \notin \ell(t)$.
  - $(\forall y\ G)(t/x)$ est $\forall y\ G(t/x)$ si $x \neq y$ et $y \notin \ell(t)$.
  - sinon, renommer y
    - remplacer $(\exists y\ G)$ par $(\exists z\ (zy)G)$ ou $(\forall y\ G)$ par $(\forall z\ (zy)G)$ où z est une variable fraiche (qui n'apparaît nul par ailleurs).
    - et réappliquer ces règles.
- Fin de cette parenthèse.

Théorème de validité

- Théorème de Validité : Soit $\mathcal{T}$ une théorie. Soit F une formule. Si $\mathcal{T} \vdash F$, alors tout modèle de $\mathcal{T}$ est un modèle de la clôture universelle de F.

- Rappel : la **clôture universelle** de F est la formule $\forall x_1 \forall x_2 \cdots \forall x_n F(x_1, \cdots, x_n)$, où $x_1, \cdots, x_n$ sont les variables libres de F.

Théorème de complétude : comment le prouver ?

- Théorème de Complétude. Soit $\mathcal{T}$ une théorie cohérente. Alors $\mathcal{T}$ possède un modèle.

Théorème de complétude : comment le prouver ?

- Théorème de Complétude. Soit $\mathcal{T}$ une théorie cohérente. Alors $\mathcal{T}$ possède un modèle.

- On se donne une signature Σ, une théorie $\mathcal{T}$ cohérente.

Théorème de complétude : comment le prouver ?

- Théorème de Complétude. Soit $\mathcal{T}$ une théorie cohérente. Alors $\mathcal{T}$ possède un modèle.
- On se donne une signature Σ, une théorie $\mathcal{T}$ cohérente.
- On veut construire un modèle $\mathfrak{M}$ de $\mathcal{T}$.

Théorème de complétude : comment le prouver ?

- Théorème de Complétude. Soit $\mathcal{T}$ une théorie cohérente. Alors $\mathcal{T}$ possède un modèle.

- On se donne une signature Σ, une théorie $\mathcal{T}$ cohérente.

- On veut construire un modèle $\mathfrak{M}$ de $\mathcal{T}$.

- Comment faire ?

Théorème de complétude : comment le prouver ?

- Théorème de Complétude. Soit $\mathcal{T}$ une théorie cohérente. Alors $\mathcal{T}$ possède un modèle.

- On se donne une signature Σ, une théorie $\mathcal{T}$ cohérente.

- On veut construire un modèle $\mathfrak{M}$ de $\mathcal{T}$.

- Comment faire ?

  - Pas grand chose à se mettre sous la dent...

Théorème de complétude : comment le prouver ?

- Théorème de Complétude. Soit $\mathcal{T}$ une théorie cohérente. Alors $\mathcal{T}$ possède un modèle.

- On se donne une signature Σ, une théorie $\mathcal{T}$ cohérente.

- On veut construire un modèle $\mathfrak{M}$ de $\mathcal{T}$.

- Comment faire ?

  - Pas grand chose à se mettre sous la dent...

  - Idée 1 : considérer les termes clos sur la signature Σ comme ensemble de base.

Théorème de complétude : comment le prouver ?

- Théorème de Complétude. Soit $\mathcal{T}$ une théorie cohérente. Alors $\mathcal{T}$ possède un modèle.
- On se donne une signature Σ, une théorie $\mathcal{T}$ cohérente.
- On veut construire un modèle $\mathfrak{M}$ de $\mathcal{T}$.
- Comment faire ?
  - Pas grand chose à se mettre sous la dent...
  - Idée 1 : considérer les termes clos sur la signature Σ comme ensemble de base.
  - Idée 2 : arriver à obtenir que pour toute formule close F,

$$\mathfrak{M} \text{ est un modèle de } F \text{ ssi } \mathcal{T} \vdash F$$

Idée 1

- Son ensemble de base (le domaine) est l'ensemble M des termes clos sur la signature Σ de la théorie.

- Interprétations ?

  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 $\mathcal{T} \vdash R(t_1, \cdots, t_n)$.

Trop naïf sans hypothèses sur $\mathcal{T}$

- Cela ne suffit pas.

- Illustration d'un premier problème : un seul axiome $P(c) \vee Q(c)$.

  - Les formules $P(c), \neg P(c), Q(c), \neg Q(c)$ sont non-démontrables.
  - Il faut forcer à avoir $P(c)$ ou $\neg P(c)$.
  - Remarque : si l'on fixe le choix $\neg P(c)$, alors $Q(c)$ sera prouvable, et donc on aura fixé $Q(c)$.

- Illustration du second problème : deux axiomes $\neg P(c)$ et $\exists x P(x)$.

  - Idée : construire un "témoin" de l'existence d'un objet vérifiant P.

Comment y arriver ?

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

- On dit qu'une théorie $\mathcal{T}$ **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 $(\exists x F(x) \Rightarrow F(c))$ soit une formule de la théorie $\mathcal{T}$.

- Proposition. Si $\mathcal{T}$ est cohérente, complète, et avec des témoins de Henkin, alors on a la propriété

$$\mathfrak{M} \text{ est un modèle de } F \text{ ssi } \mathcal{T} \vdash F,$$

  - et donc $\mathcal{T}$ possède un modèle.

Comment y arriver ?

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

- On dit qu'une théorie $\mathcal{T}$ **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 $(\exists x F(x) \Rightarrow F(c))$ soit une formule de la théorie $\mathcal{T}$.

- Proposition. Si $\mathcal{T}$ est cohérente, complète, et avec des témoins de Henkin, alors on a la propriété

$$\mathfrak{M} \text{ est un modèle de } F \text{ ssi } \mathcal{T} \vdash F,$$

  - et donc $\mathcal{T}$ possède un modèle.

- Démonstration de la proposition : par induction (pas très difficile).

Complétion d'une théorie

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

- 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 $\mathcal{T}'$ est obtenue comme l'union d'une suite croissante de théories $\mathcal{T}_n$, définie par récurrence, en partant de $\mathcal{T}_0 = \mathcal{T}$.
  - Supposons $\mathcal{T}_n$ cohérente construite.
    - Pour construire $\mathcal{T}_{n+1}$ on considère la formule F_{n+1} dans l'énumération des formules closes de Σ'.
    - Si $\mathcal{T}_n \cup F_{n+1}$ est cohérente, alors on pose $G_n = F_{n+1}$, sinon on pose $G_n = \neg F_{n+1}$.
    - Dans les deux cas $\mathcal{T}_n \cup \{G_n\}$ est cohérente.

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

  1. $\mathcal{T}_{n+1} = \mathcal{T}_n \cup \{G_n\}$ si G_n n'est pas de la forme $\exists x H$.
  2. $\mathcal{T}_{n+1} = \mathcal{T}_n \cup \{G_n, H(c/x)\}$ sinon

     - 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 $T_n \cup \{G_n\}$.

- on montre que par construction la théorie $\mathcal{T}_{n+1}$ est cohérente.

- La théorie
$$\mathcal{T}' = \bigcup_{n\in\mathbb{N}} \mathcal{T}_n$$
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, on obtient facilement $\mathcal{T}_{n+1} \vdash \exists x H(x) \Rightarrow H(c/x)$,
  - ce qui prouve que $(\exists x H(x) \Rightarrow F(c))$ est dans $\mathcal{T}'$
    - (sinon, puisque $\mathcal{T}'$ est complète, sa négation y serait, et $\mathcal{T}'$ ne serait pas cohérente).

- Et donc on a prouvé le théorème de complétude.