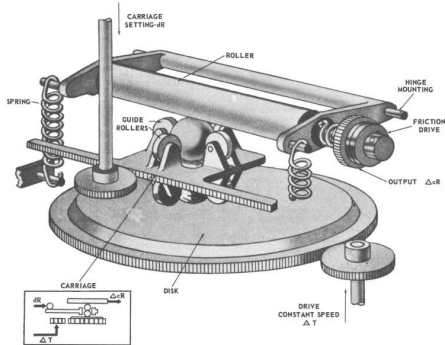


Cours 2: Calcul propositionnel. Calcul des prédicats.



Olivier Bournez
bournez@lix.polytechnique.fr

Ecole Polytechnique
INF412

Au menu

Calcul propositionnel

Calcul des prédicats

Plus précisément

Calcul propositionnel

Rappel

Quelques équivalences

Complétude fonctionnelle

Formes normales

Systèmes de déduction

Preuves à la Hilbert-Fregge

Preuves en déduction naturelle

Satisfaction d'un ensemble de formules - Théorème de

Compacité

Retour sur l'épisode précédent

■ Syntaxe :

L'ensemble des formules propositionnelles \mathcal{F} sur \mathcal{P} est le langage sur l'alphabet $\mathcal{P} \cup \{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow, (,)\}$ défini inductivement par les règles suivantes :

(B) il contient \mathcal{P} : toute variable propositionnelle est une formule propositionnelle ;

(I) si $F \in \mathcal{F}$ alors $\neg F \in \mathcal{F}$;

(I) si $F, G \in \mathcal{F}$ alors $(F \wedge G) \in \mathcal{F}$, $(F \vee G) \in \mathcal{F}$, $(F \Rightarrow G) \in \mathcal{F}$, et $(F \Leftrightarrow G) \in \mathcal{F}$.

■ Semantique : définie inductivement.

p	q	$\neg p$	$p \vee q$	$p \wedge q$	$p \Rightarrow q$	$p \Leftrightarrow q$
0	0	1	0	0	1	1
0	1	1	1	0	1	0
1	0	0	1	0	0	0
1	1	0	1	1	1	1

- Lorsque la formule F s'évalue en 1, on dit que F est **satisfaite** en v , et que v est un **modèle** de F .

Plus précisément

Calcul propositionnel

Rappel

Quelques équivalences

Complétude fonctionnelle

Formes normales

Systèmes de déduction

Preuves à la Hilbert-Fregge

Preuves en déduction naturelle

Satisfaction d'un ensemble de formules - Théorème de

Compacité

Tautologies, formules équivalentes

- Une **tautologie** est une formule F qui est satisfaite en toute valuation.
- Deux formules F et G sont dites **équivalentes** si elles s'évaluent en 1 (et donc aussi en 0) pour exactement les mêmes valuations.
 - ▶ On écrit dans ce cas $F \equiv G$.
- Exemples :
 - ▶ La formule $p \vee \neg p$ est une tautologie ;
 - ▶ Les formules p et $\neg\neg p$ sont équivalentes.

Quelques équivalences

- Pour toutes formules F et G , les formules suivantes sont des tautologies :

$$(F \Rightarrow F),$$

$$(F \Rightarrow (G \Rightarrow F)),$$

$$(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H)).$$

- Idempotence : pour toute formule F

$$(F \vee F) \equiv F,$$

$$(F \wedge F) \equiv F.$$

- Associativité : pour toutes formules F, G, H

$$(F \wedge (G \wedge H)) \equiv ((F \wedge G) \wedge H),$$

$$(F \vee (G \vee H)) \equiv ((F \vee G) \vee H).$$

Quelques équivalences

- Commutativité : pour toutes formules F et G

$$(F \wedge G) \equiv (G \wedge F),$$

$$(F \vee G) \equiv (G \vee F).$$

- Distributivité : pour toutes formules F, G, H

$$(F \wedge (G \vee H)) \equiv ((F \wedge G) \vee (F \wedge H)),$$

$$(F \vee (G \wedge H)) \equiv ((F \vee G) \wedge (F \vee H)).$$

- Lois de De Morgan : pour toutes formules F et G

$$\neg(F \wedge G) \equiv (\neg F \vee \neg G),$$

$$\neg(F \vee G) \equiv (\neg F \wedge \neg G).$$

- Absorption : pour toutes formules F et G

$$(F \wedge (F \vee G)) \equiv F$$

$$(F \vee (F \wedge G)) \equiv F.$$

- En raison des équivalences précédentes (associativité), on va dorénavant souvent ne pas écrire toutes les parenthèses

Plus précisément

Calcul propositionnel

Rappel

Quelques équivalences

Complétude fonctionnelle

Formes normales

Systèmes de déduction

Preuves à la Hilbert-Fregge

Preuves en déduction naturelle

Satisfaction d'un ensemble de formules - Théorème de

Compacité

Complétude fonctionnelle

Théorème

Toute fonction f des valuations sur $\{0,1\}^n$ dans $\{0,1\}$ est la valeur de vérité d'une formule propositionnelle.

■ Démonstration :

- ▶ Par récurrence sur le nombre n de variables de f .
- ▶ Pour $n = 1$, il y a quatre fonctions de $\{0, 1\}^1$ dans $\{0, 1\}$, qui se représentent par les formules p , $\neg p$, $(p \vee \neg p)$, $(p \wedge \neg p)$.
- ▶ Supposons la propriété vraie pour $n - 1$.
- ▶ Chaque valuation v' sur $\{p_1, p_2, \dots, p_{n-1}\}$ peut se voir comme la restriction d'une valuation sur $\{p_1, \dots, p_n\}$.
- ▶ Soit f_0 (respectivement f_1) la restriction de f à la valuation v telle que $v(p_n) = 0$ (resp. $v(p_n) = 1$).
- ▶ Les fonctions f_0 et f_1 se représentent par des formules $G(p_1, \dots, p_{n-1})$ et $H(p_1, \dots, p_{n-1})$ respectivement par hypothèse de récurrence.
- ▶ La fonction f peut alors se représenter par la formule
$$(\neg p_n \wedge G(p_1, \dots, p_{n-1})) \vee (p_n \wedge H(p_1, \dots, p_{n-1})),$$
ce qui prouve l'hypothèse de récurrence au rang n .

Plus précisément

Calcul propositionnel

Rappel

Quelques équivalences

Complétude fonctionnelle

Formes normales

Systèmes de déduction

Preuves à la Hilbert-Fregge

Preuves en déduction naturelle

Satisfaction d'un ensemble de formules - Théorème de

Compacité

Formes normales

- Un **littéral** est de la forme p , ou $\neg p$, pour $p \in \mathcal{P}$.
- Une **forme normale disjonctive** (FND) est une disjonction $F_1 \vee F_2 \vee \dots \vee F_k$ de formules, où chaque formule F_i est une conjonction $G_1 \wedge G_2 \wedge \dots \wedge G_{\ell_i}$ de littéraux.
- Une **forme normale conjonctive** (FNC) est une conjonction $F_1 \wedge F_2 \wedge \dots \wedge F_k$ de formules, où chaque formule F_i est une disjonction $G_1 \vee G_2 \vee \dots \vee G_{\ell_i}$ de littéraux.
- Remarque. Dans ces écritures, on s'autorise à supprimer des parenthèses (par les règles d'associativité de \wedge et de \vee).
- Exemples :
 - ▶ $((p \wedge q \wedge \neg r) \vee (q \wedge \neg p))$ est une FND.
 - ▶ $\neg p \vee q$ et $(\neg p \vee q) \wedge \neg r$ sont des FNC.

Formes normales

Théorème

- *Toute formule propositionnelle est équivalente à une formule en forme normale conjonctive.*
- *Toute formule propositionnelle est équivalente à une formule en forme normale disjonctive.*

Formes normales

Théorème

- *Toute formule propositionnelle est équivalente à une formule en forme normale conjonctive.*
- *Toute formule propositionnelle est équivalente à une formule en forme normale disjonctive.*

Corollaire

Toute formule propositionnelle s'écrit avec uniquement les connecteurs \vee , \wedge et \neg .

Formes normales

Théorème

- *Toute formule propositionnelle est équivalente à une formule en forme normale conjonctive.*
- *Toute formule propositionnelle est équivalente à une formule en forme normale disjonctive.*

Corollaire

Toute formule propositionnelle s'écrit avec uniquement les connecteurs \vee , \wedge et \neg .

Corollaire

- *Toute formule propositionnelle s'écrit avec uniquement les connecteurs \neg et \wedge .*
- *Toute formule propositionnelle s'écrit avec uniquement les connecteurs \neg et \vee .*

Formes normales

Théorème

- *Toute formule propositionnelle est équivalente à une formule en forme normale conjonctive.*
- *Toute formule propositionnelle est équivalente à une formule en forme normale disjonctive.*

Corollaire

Toute formule propositionnelle s'écrit avec uniquement les connecteurs \vee , \wedge et \neg .

Corollaire

- *Toute formule propositionnelle s'écrit avec uniquement les connecteurs \neg et \wedge .*
- *Toute formule propositionnelle s'écrit avec uniquement les connecteurs \neg et \vee .*

- **Démonstration** : remplacer les \vee ou les \wedge en utilisant les lois de Morgan.

■ Démonstration par induction sur la formule :

- ▶ Par récurrence sur n comme dans la preuve précédente.
- ▶ Pour $n = 1$, p , $\neg p$, $p \vee \neg p$, $p \wedge \neg p$ sont en FNC et FND.
- ▶ On suppose la propriété vraie pour $n - 1$.
- ▶ Comme dans la dernière preuve, on peut construire une formule qui représente la fonction valeur de vérité f associée à la formule $F(p_1, \dots, p_n)$ par une formule de la forme

$$(\neg p_n \wedge G(p_1, \dots, p_{n-1})) \vee (p_n \wedge H(p_1, \dots, p_{n-1})).$$

- ▶ Par hypothèse de récurrence, G et H sont équivalentes à

$$G \equiv (G_1 \vee G_2 \vee \dots \vee G_k) \text{ et } H \equiv (H_1 \vee H_2 \vee \dots \vee H_\ell)$$

- ▶ On peut alors écrire

$$(\neg p_n \wedge G) \equiv (\neg p_n \wedge G_1) \vee (\neg p_n \wedge G_2) \vee \dots \vee (\neg p_n \wedge G_k)$$

$$(p_n \wedge H) \equiv (p_n \wedge H_1) \vee (p_n \wedge H_2) \vee \dots \vee (p_n \wedge H_\ell)$$

qui sont les deux en FND.

- ▶ La fonction f est donc représentée par la disjonction de ces deux formules, et donc par une FND.
- ▶ Si l'on veut obtenir F en forme normale conjonctive, on utilise l'équivalence $F \equiv ((\neg p_n \vee H) \wedge (p_n \vee G))$.

Plus précisément

Calcul propositionnel

Rappel

Quelques équivalences

Complétude fonctionnelle

Formes normales

Systèmes de déduction

Preuves à la Hilbert-Fregge

Preuves en déduction naturelle

Satisfaction d'un ensemble de formules - Théorème de

Compacité

Introduction

- On va commencer à aborder la question suivante :

qu'est-ce qu'une démonstration ?

- Exemple :
 - ▶ on se donne une formule propositionnelle F ,
 - ▶ et on veut décider si F est une tautologie.

Une première méthode

■ Première méthode :

- ▶ Une formule propositionnelle F s'écrit à l'aide d'un nombre fini de variables p_1, \dots, p_n .
- ▶ On détermine la valeur de F sur les 2^n valuations possibles de p_1, \dots, p_n , et on vérifie que c'est bien 1 pour toutes les valuations.
- ▶ Soucis :

1. Complexité exponentielle :

pour n grand,

le temps explose, car 2^n est très grand ;
en outre, le temps explose **TOUJOURS**.

2. Cela ne correspond pas à ce que l'on aurait pu vouloir appeler une "démonstration".

Des systèmes de preuve

- Preuves à la Hilbert-Fregge.
- Dédution naturelle.
- Preuves par résolution. (cf PC de demain).
- Méthode des tableaux.

Plus précisément

Calcul propositionnel

Rappel

Quelques équivalences

Complétude fonctionnelle

Formes normales

Systèmes de déduction

Preuves à la Hilbert-Fregge

Preuves en déduction naturelle

Satisfaction d'un ensemble de formules - Théorème de

Compacité

Preuves à la Hilbert-Fregge

■ Principe :

- ▶ on part d'un ensemble d'axiomes, qui sont des tautologies ;
- ▶ et on utilise une unique règle de déduction, le **modus ponens**, aussi appelé **coupure**, qui vise à capturer un type de raisonnement tout à fait naturel en mathématique.

- La règle du modus ponens dit qu'à partir de la formule F et d'une formule $F \Rightarrow G$, on déduit G .

$$\frac{F \quad (F \Rightarrow G)}{G}$$

- Exemple : à partir de $(A \wedge B)$ et de $(A \wedge B) \Rightarrow C$ on déduit C .

- On dit qu'une formule F est une **instance** d'une formule G si F s'obtient en substituant certaines variables propositionnelles de G par des formules F_i .

- Un **axiome de la logique booléenne** est n'importe quelle **instance** d'une des formules suivantes :
 1. $(X_1 \Rightarrow (X_2 \Rightarrow X_1))$ (axiome 1 pour l'implication);
 2. $((X_1 \Rightarrow (X_2 \Rightarrow X_3)) \Rightarrow ((X_1 \Rightarrow X_2) \Rightarrow (X_1 \Rightarrow X_3)))$ (axiome 2 pour l'implication);
 3. $(X_1 \Rightarrow \neg\neg X_1)$ (axiome 1 pour la négation);
 4. $(\neg\neg X_1 \Rightarrow X_1)$ (axiome 2 pour la négation);
 5. $((X_1 \Rightarrow X_2) \Rightarrow (\neg X_2 \Rightarrow \neg X_1))$ (axiome 3 pour la négation);
 6. $(X_1 \Rightarrow (X_2 \Rightarrow (X_1 \wedge X_2)))$ (axiome 1 pour la conjonction);
 7. $((X_1 \wedge X_2) \Rightarrow X_1)$ (axiome 2 pour la conjonction);
 8. $((X_1 \wedge X_2) \Rightarrow X_2)$ (axiome 3 pour la conjonction);
 9. $(X_1 \Rightarrow (X_1 \vee X_2))$ (axiome 1 pour la disjonction);
 10. $(X_2 \Rightarrow (X_1 \vee X_2))$ (axiome 2 pour la disjonction);
 11. $(\neg X_1 \Rightarrow ((X_1 \vee X_2) \Rightarrow X_2))$ (axiome 3 pour la disjonction).

Preuve par modus ponens

- Soit T un ensemble de formules propositionnelles, et F une formule propositionnelle.
- Une **preuve de F à partir de T** est une suite finie F_1, F_2, \dots, F_n de formules propositionnelles telle que :
 - ▶ F_n est égale à F ,
 - ▶ et pour tout i ,
 - ou bien F_i est dans T ;
 - ou bien F_i est un axiome de la logique booléenne ;
 - ou bien F_i s'obtient par modus ponens à partir de deux formules F_j, F_k avec $j < i$ et $k < i$.
- Notation :
 - ▶ On dit que F est **prouvable à partir de T** , noté $T \vdash F$ dans ce cas. F est dite **prouvable** si elle est prouvable à partir de $T = \emptyset$.

Exemple

Voici une preuve de $(F \Rightarrow H)$ à partir de $\{(F \Rightarrow G), (G \Rightarrow H)\}$:

- $F_1 : (G \Rightarrow H)$ (hypothèse) ;
- $F_2 : ((G \Rightarrow H) \Rightarrow (F \Rightarrow (G \Rightarrow H)))$ (instance de l'axiome 1.) ;
- $F_3 : (F \Rightarrow (G \Rightarrow H))$ (modus ponens à partir de F_1 et F_2) ;
- $F_4 : ((F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H)))$
(instance de l'axiome 2.) ;
- $F_5 : ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$ (modus ponens à partir de F_3 et F_4) ;
- $F_6 : (F \Rightarrow G)$ (hypothèse) ;
- $F_7 : (F \Rightarrow H)$ (modus ponens à partir de F_6 et F_5).

Validité et complétude de cette méthode de preuve

Théorème (Validité)

Toute formule propositionnelle prouvable est une tautologie.

Théorème (Complétude)

Toute tautologie est prouvable.

■ Plus généralement :

- ▶ Notons $T \models F$ pour signifier que tout modèle de chacune des formules de T est un modèle de F .
- ▶ On dit que F est une **conséquence** (sémantique) de T .
- ▶ On a :

$$T \vdash F \text{ ssi } T \models F.$$

Plus précisément

Calcul propositionnel

Rappel

Quelques équivalences

Complétude fonctionnelle

Formes normales

Systèmes de déduction

Preuves à la Hilbert-Fregge

Preuves en déduction naturelle

Satisfaction d'un ensemble de formules - Théorème de

Compacité

Déduction naturelle

- La notion de démonstration précédente est pénible à utiliser en pratique.

Déduction naturelle

- La notion de démonstration précédente est pénible à utiliser en pratique.
- Une alternative : la **déduction naturelle**.

Déduction naturelle

- La notion de démonstration précédente est pénible à utiliser en pratique.
- Une alternative : la **déduction naturelle**.
- Principe :
 - ▶ On manipule des couples (appelés **séquents**) $\Gamma \vdash A$, où Γ est un ensemble fini de formules (propositionnelles) et A est une formule (propositionnelle).
 - ▶ On utilise les règles de déduction du transparent suivant

Déduction naturelle

- La notion de démonstration précédente est pénible à utiliser en pratique.
- Une alternative : la **déduction naturelle**.
- Principe :
 - ▶ On manipule des couples (appelés **séquents**) $\Gamma \vdash A$, où Γ est un ensemble fini de formules (propositionnelles) et A est une formule (propositionnelle).
 - Motivation sous-jacente : $\Gamma \vdash A$ exprime le fait que sous les hypothèses Γ , on a A .
 - ▶ On utilise les règles de déduction du transparent suivant

Déduction naturelle

- La notion de démonstration précédente est pénible à utiliser en pratique.
- Une alternative : la **déduction naturelle**.
- Principe :
 - ▶ On manipule des couples (appelés **séquents**) $\Gamma \vdash A$, où Γ est un ensemble fini de formules (propositionnelles) et A est une formule (propositionnelle).
 - Motivation sous-jacente : $\Gamma \vdash A$ exprime le fait que sous les hypothèses Γ , on a A .
 - ▶ On utilise les règles de déduction du transparent suivant
 - i.e. : on définit inductivement **l'ensemble des séquents dérivables** par les règles du transparent suivant.

Déduction naturelle

- La notion de démonstration précédente est pénible à utiliser en pratique.
- Une alternative : la **déduction naturelle**.
- Principe :
 - ▶ On manipule des couples (appelés **séquents**) $\Gamma \vdash A$, où Γ est un ensemble fini de formules (propositionnelles) et A est une formule (propositionnelle).
 - Motivation sous-jacente : $\Gamma \vdash A$ exprime le fait que sous les hypothèses Γ , on a A .
 - ▶ On utilise les règles de déduction du transparent suivant
 - i.e. : on définit inductivement **l'ensemble des séquents dérivables** par les règles du transparent suivant.
 - Ici, on considère que les formules incluent aussi \perp , interprété par faux, et \top interprété par vrai.

Déduction naturelle

- La notion de démonstration précédente est pénible à utiliser en pratique.
- Une alternative : la **déduction naturelle**.
- Principe :
 - ▶ On manipule des couples (appelés **séquents**) $\Gamma \vdash A$, où Γ est un ensemble fini de formules (propositionnelles) et A est une formule (propositionnelle).
 - Motivation sous-jacente : $\Gamma \vdash A$ exprime le fait que sous les hypothèses Γ , on a A .
 - ▶ On utilise les règles de déduction du transparent suivant
 - i.e. : on définit inductivement **l'ensemble des séquents dérivables** par les règles du transparent suivant.
 - Ici, on considère que les formules incluent aussi \perp , interprété par faux, et \top interprété par vrai.
- On dit que F est **prouvable à partir de T** , noté $T \vdash F$ si $T \vdash F$ est un séquent dérivable. F est dite **prouvable** si elle est prouvable à partir de $T = \emptyset$.

$\overline{\Gamma \vdash A}$ axiome pour chaque $A \in \Gamma$

$\overline{\Gamma \vdash \top}$ \top -intro

$\frac{\Gamma \vdash \perp}{\Gamma \vdash A}$ \perp -élim

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

$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}$ \wedge -élim

$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$ \wedge -élim

$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}$ \vee -intro

$\frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$ \vee -intro

$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}$ \vee -élim

$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}$ \Rightarrow -intro

$\frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}$ \Rightarrow -élim

$\frac{\Gamma, A \vdash \perp}{\Gamma \vdash \neg A}$ \neg -intro

$\frac{\Gamma \vdash A \quad \Gamma \vdash \neg A}{\Gamma \vdash \perp}$ \neg -élim

$\overline{\Gamma \vdash A \vee \neg A}$ tiers exclu

Exemple

$$\frac{\frac{\frac{}{\{(F \Rightarrow G), (G \Rightarrow H), F\} \vdash (G \Rightarrow H)} \text{ax}}{\{(F \Rightarrow G), (G \Rightarrow H), F\} \vdash H} \Rightarrow\text{-élim}}{\{(F \Rightarrow G), (G \Rightarrow H)\} \vdash (F \Rightarrow H)} \Rightarrow\text{-intro}}{\{(F \Rightarrow G), (G \Rightarrow H), F\} \vdash (F \Rightarrow G)} \text{ax} \quad \frac{\frac{}{\{(F \Rightarrow G), (G \Rightarrow H), F\} \vdash F} \text{ax}}{\{(F \Rightarrow G), (G \Rightarrow H)\} \vdash (F \Rightarrow H)} \Rightarrow\text{-élim}}{G} \Rightarrow\text{-élim}$$

Validité et complétude de cette méthode de preuve

Théorème (Validité)

Toute formule propositionnelle prouvable est une tautologie.

Théorème (Complétude)

Toute tautologie est prouvable.

■ Plus généralement :

- ▶ Notons $T \models F$ pour signifier que tout modèle de chacune des formules de T est un modèle de F .
- ▶ On dit que F est une **conséquence** (sémantique) de T .
- ▶ On a :

$$T \vdash F \text{ ssi } T \models F.$$

Plus précisément

Calcul propositionnel

Rappel

Quelques équivalences

Complétude fonctionnelle

Formes normales

Systèmes de déduction

Preuves à la Hilbert-Fregge

Preuves en déduction naturelle

Satisfaction d'un ensemble de formules - Théorème de

Compacité

Motivation

- Le calcul propositionnel reste très limité...
- Si on veut aller plus loin, on peut chercher à parler de choses plus générales que les fonctions booléennes.
 - ▶ On va se donner cette fois un ensemble Σ de formules.
 - ▶ On cherche à savoir quand on peut satisfaire toutes les formules de Σ .

Motivation

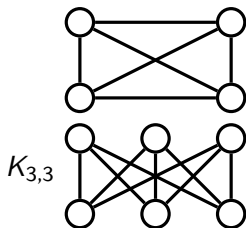
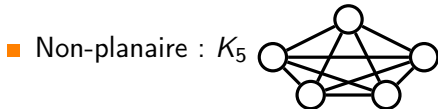
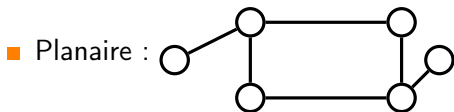
- Le calcul propositionnel reste très limité...
- Si on veut aller plus loin, on peut chercher à parler de choses plus générales que les fonctions booléennes.
 - ▶ On va se donner cette fois un ensemble Σ de formules.
 - Σ peut être fini ou infini.
 - ▶ On cherche à savoir quand on peut satisfaire toutes les formules de Σ .

Motivation

- Le calcul propositionnel reste très limité...
- Si on veut aller plus loin, on peut chercher à parler de choses plus générales que les fonctions booléennes.
 - ▶ On va se donner cette fois un ensemble Σ de formules.
 - Σ peut être fini ou infini.
 - ▶ On cherche à savoir quand on peut satisfaire toutes les formules de Σ .
- Le reste de cette section : la présentation d'un des grands résultats du calcul propositionnel, le théorème de compacité, via quelques digressions liées à une application.


Digression : Théorie des graphes.

- Un graphe est dit **planaire** s'il peut se représenter sur un plan sans qu'aucune arête n'en croise une autre.



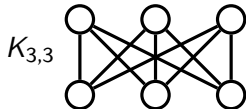
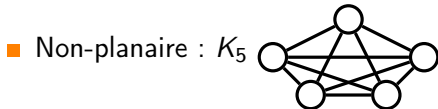
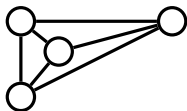
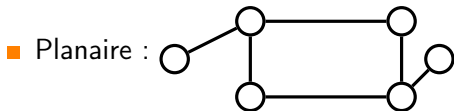
Théorème (Kuratowski-Wagner)

Un graphe fini est planaire ssi il ne contient pas de sous-graphe qui soit une expansion de K_5 ou de $K_{3,3}$.

- ▶ Une expansion consiste (grossièrement) à ajouter un ou plusieurs sommets sur une ou plusieurs arêtes (exemple : )


Digression : Théorie des graphes.

- Un graphe est dit **planaire** s'il peut se représenter sur un plan sans qu'aucune arête n'en croise une autre.



Théorème (Kuratowski-Wagner)

Un graphe fini est planaire ssi il ne contient pas de sous-graphe qui soit une expansion de K_5 ou de $K_{3,3}$.

- ▶ Une expansion consiste (grossièrement) à ajouter un ou plusieurs sommets sur une ou plusieurs arêtes (exemple : )

Digression : Coloriage de graphes.

- Le problème de **coloriage d'un graphe** : colorier les sommets d'un graphe de telle sorte qu'aucune arête n'ait ses extrémités d'une même couleur.



Un coloriage avec 4 couleurs

Théorème (Appel et Haken (76))

Tout graphe planaire est coloriable avec 4 couleurs.

- ▶ Preuve avec 1478 cas critiques.
- ▶ Robertson, Sanders, Seymour, Thomas, Gonthier, Werner...
- Digression : Le problème du coloriage de graphes est NP-complet (voir fin du cours).

Retour sur la logique propositionnelle

- On se donne un graphe $G = (V, E)$ et k couleurs.
- On considère $\mathcal{P} = \{A_{u,i}, u \in V, 1 \leq i \leq k\}$ un ensemble de variables propositionnelles.
- Idée : $A_{u,i}$ vraie ssi le sommet u est colorié avec la couleur i .
- Contraintes :

- ▶ Chaque sommet possède une couleur :

$$\Gamma_1 = \{A_{u,1} \vee \dots \vee A_{u,k} \mid u \in V\}.$$

- ▶ Chaque sommet n'a pas plus qu'une couleur :

$$\Gamma_2 = \{\neg(A_{u,i} \wedge A_{u,j}) \mid u \in V, 1 \leq i, j \leq k, i \neq j\}.$$

- ▶ Chaque arête n'a pas ses extrémités d'une même couleur :

$$\Gamma_3 = \{\neg(A_{u,i} \wedge A_{v,i}) \mid u \in V, 1 \leq i \leq k, (u, v) \in E\}.$$

- Un graphe est coloriable avec k couleurs si et seulement si on peut satisfaire toutes les formules de $\Gamma = \Gamma_1 \cup \Gamma_2 \cup \Gamma_3$.

Définitions

- Soit Σ un ensemble de formules.
- Définitions :
 - ▶ Une valuation v **satisfait** Σ si elle satisfait chaque formule de Σ . On note alors $v \models \Sigma$. On dit aussi dans ce cas que cette valuation est **un modèle** de Σ .
 - ▶ Σ est dit **satisfiable**, ou **consistant**, s'il existe une valuation qui le satisfait. Σ est dit **inconsistant**, ou **contradictoire**, sinon.
- Exemples :
 - ▶ $\{p, \neg q, p \vee r\}$ est satisfiable.
 - ▶ $\{p, p \Rightarrow q, \neg q\}$ est inconsistant.
 - ▶ une valuation satisfait Γ ssi elle correspond à un k -coloriage.

Théorème de compacité

Supposons \mathcal{P} dénombrable.

Trois formulations équivalentes du théorème.

Théorème (Version 1)

Un ensemble Σ de formules est satisfiable si et seulement si toute partie finie de Σ est satisfiable.

Théorème (Version 2)

Un ensemble Σ de formules est inconsistant si et seulement si Σ possède une partie finie inconsistante.

Théorème (Version 3)

Une formule F est une conséquence d'un ensemble Σ de formules si et seulement si F est une conséquence d'une partie finie de Σ .

Une application du théorème : Coloriage de graphes

- Dans la preuve du théorème de Appel et Haken, il “suffit” de faire la preuve pour les graphes finis :

Théorème

Un graphe (fini ou infini) G est coloriable avec k couleurs si et seulement si chacun de ses sous-graphes est coloriable avec k couleurs.

- ▶ Sens \Rightarrow : trivial.
- ▶ Sens \Leftarrow : Pourquoi ?
 - Γ est satisfiable si et seulement si toute partie finie Γ_0 de Γ est satisfiable.
 - Soit Γ_0 une partie finie de Γ . Soient $V_0 = \{u_1, \dots, u_n\}$ les sommets u tels que $A_{u,i}$ figure dans une des formules de Γ_0 . Soit $G_0 = (V_0, E_0)$ le sous-graphe déterminé par V_0 .
 - Par hypothèse, G_0 est coloriable avec k couleurs, et donc Γ_0 est satisfiable.

Autres applications

- Le théorème de compacité est vrai pour des logiques plus générales.
- Autre application :
 - ▶ Lemme de König : tout arbre infini dénombrable de degré fini possède un chemin infini.
- ...il a surtout des applications dans des logiques plus générales.

Au menu

Calcul propositionnel

Calcul des prédicats

- Si l'on veut pouvoir raisonner sur des assertions mathématiques, il nous faut autoriser des constructions plus riches que celles du calcul propositionnel.
- Un énoncé comme

$$\forall x((Premier(x) \wedge x > 1 + 1) \Rightarrow Impair(x)).$$

n'est pas capturé par la logique propositionnelle :

- ▶ on a des **prédicats** comme $Premier(x)$ dont la valeur de vérité dépend d'une variable x ;
- ▶ on utilise des quantificateurs comme \exists , \forall .

Logique du premier ordre

- On va présenter seulement le **calcul des prédicats du premier ordre**.
 - ▶ En logique du **premier ordre**, on n'autorise que les quantifications sur les variables.

$$\forall x((Premier(x) \wedge x > 1 + 1) \Rightarrow Impair(x)).$$

- Un énoncé **du second ordre** (ou **d'ordre supérieur**) serait un énoncé où l'on autoriserait les quantifications sur les fonctions ou des relations.
 - ▶ Exemple :

$$\neg \exists f(\forall x(f(x) > f(x+1))).$$

Plus précisément

Calcul des prédicats
Syntaxe

Premières considérations

- Pour écrire une formule d'un langage du premier ordre, on utilise
 - ▶ certains symboles qui sont communs à tous les langages,
 - ▶ et certains symboles qui varient d'un langage à l'autre.

$$\forall x((Premier(x) \wedge x > 1 + 1) \Rightarrow Impair(x)).$$

■ Les symboles

- ▶ communs à tous les langages sont :
 - les connecteurs \neg , \vee , \wedge , \Rightarrow , \Leftrightarrow ;
 - les parenthèses (et) et la virgule , ;
 - le quantificateur universel \forall et le quantificateur existentiel \exists ;
 - un ensemble infini dénombrable de symboles \mathcal{V} de variables.
- ▶ qui peuvent varier d'un langage à l'autre sont :
 - capturés par la notion de **signature**.

Signature d'un langage du premier ordre

- La signature $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$ d'un langage du premier ordre est la donnée¹ :
 - ▶ d'un premier ensemble \mathcal{C} de **symboles de constantes** ;
 - ▶ d'un second ensemble \mathcal{F} de **symboles de fonctions**.
 - A chaque symbole de cet ensemble est associé un entier strictement positif, que l'on appelle **son arité** ;
 - ▶ d'un troisième ensemble \mathcal{R} de **symboles de relations**.
 - A chaque symbole de cet ensemble est associé un entier strictement positif, que l'on appelle **son arité**.

1. On supposera que $\mathcal{V}, \mathcal{C}, \mathcal{F}, \mathcal{R}$ sont des ensembles disjoints deux à deux.

Exemples

■ Exemples de signatures :

- ▶ $\Sigma = (\{0, 1\}, \{s, +\}, \{Impair, Premier, =, <\})$ avec les symboles de constante 0 et 1, les symboles de fonctions s d'arité 1 et $+$ d'arité 2, les symboles de relations $Impairs$ et $Premier$ d'arité 1 et $=$ et $<$ d'arité 2.
- ▶ $\mathcal{L}_2 = (\{c, d\}, \{f, g, h\}, \{R\})$ avec c, d deux symboles de constante, f un symbole de fonction d'arité 1, g et h deux symboles de fonctions d'arité 2, R un symbole de relation d'arité 2.

- Une formule du premier ordre sera alors un mot sur l'alphabet

$$\mathcal{A}(\Sigma) = \mathcal{V} \cup \mathcal{C} \cup \mathcal{F} \cup \mathcal{R} \cup \{\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow, (,), ,, =, \forall, \exists\}.$$

- On va définir par étapes :

1. d'abord les **termes**,
 - qui visent à représenter des objets,
2. puis les **formules atomiques**,
 - qui visent à représenter des relations entre objets,
3. et enfin les **formules**.

■ Il est utile² de lire **le polycopié**.

▶ en particulier, le chapitre 5.

- Il est utile² de lire **le polycopié**.
 - ▶ en particulier, le chapitre 5.
- tout ce qui suit dans cette section précise la terminologie et les définitions mais reste sur le fond sans surprises...

- Et c'est pour cela que la suite va être subliminale . . . ,
...car le mieux est de le lire par soit-même à tête reposée

- Et c'est pour cela que la suite va être subliminale . . . ,
...car le mieux est de le lire par soit-même à tête reposée
 - ▶ puis de faire par exemple le quizz sur le moodle INF412 . . .

PARTIE SUBLIMINALE:

A LIRE ATTENTIVEMENT PAR SOI-MÊME

Termes

- Soit $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$ une signature.
- L'ensemble T des **termes** sur la signature Σ est le langage sur l'alphabet $\mathcal{A}(\Sigma)$ défini inductivement par :
 - (B) toute variable est un terme : $\mathcal{V} \subset T$;
 - (B) toute constante est un terme : $\mathcal{C} \subset T$;
 - (I) si f est un symbole de fonction d'arité n et si t_1, t_2, \dots, t_n sont des termes, alors $f(t_1, \dots, t_n)$ est un terme.
- Un **terme clos** est un terme sans variable.

Exemples

- (Convention : x, y, z, \dots désignent des variables, c-à-d des éléments de \mathcal{V}).
- Exemples :
 - ▶ $+(x, s(+ (1, 1)))$ est un terme sur la signature Σ précédente qui n'est pas clos. $+(+(s(1), +(1, 1)), s(s(0)))$ est un terme clos sur cette même signature.
 - ▶ $h(c, x)$, $h(y, z)$, $g(d, h(y, z))$ et $f(g(d, h(y, z)))$ sont des termes sur la signature \mathcal{L}_2 .

Formules atomiques

- Soit $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$ une signature.
- Une **formule atomique** sur la signature Σ est un mot sur l'alphabet $\mathcal{A}(\Sigma)$ de la forme $R(t_1, t_2, \dots, t_n)$, où $R \in \mathcal{R}$ est un symbole de relation d'arité n , et où t_1, t_2, \dots, t_n sont des termes sur Σ .

Formules atomiques

- Soit $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$ une signature.
- Une **formule atomique** sur la signature Σ est un mot sur l'alphabet $\mathcal{A}(\Sigma)$ de la forme $R(t_1, t_2, \dots, t_n)$, où $R \in \mathcal{R}$ est un symbole de relation d'arité n , et où t_1, t_2, \dots, t_n sont des termes sur Σ .
- Exemples :
 - ▶ $>(x, +(1, 0))$ est une formule atomique sur la signature précédente. $=(x, s(y))$ aussi.
 - ▶ $R(f(x), g(c, f(d)))$ est une formule atomique sur \mathcal{L}_2 .

Formules atomiques

- Soit $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$ une signature.
- Une **formule atomique** sur la signature Σ est un mot sur l'alphabet $\mathcal{A}(\Sigma)$ de la forme $R(t_1, t_2, \dots, t_n)$, où $R \in \mathcal{R}$ est un symbole de relation d'arité n , et où t_1, t_2, \dots, t_n sont des termes sur Σ .
- Exemples :
 - ▶ $>(x, +(1,0))$ est une formule atomique sur la signature précédente. $=(x, s(y))$ aussi.
 - ▶ On convient parfois d'écrire $t_1 R t_2$ pour certains symboles binaires, comme $=, <, +$:
 - par exemple, on écrira $x > 1+1$ pour $>(x, +(1,1))$, ou $(s(1)+1)+s(s(0))$ pour $+(+(s(1),1),s(s(0)))$.
 - ▶ $R(f(x), g(c, f(d)))$ est une formule atomique sur \mathcal{L}_2 .

Formules

- Soit $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$ une signature.
- L'ensemble des formules sur la signature Σ est le langage sur l'alphabet $\mathcal{A}(\Sigma)$ défini inductivement par :
 - (B) toute formule atomique est une formule ;
 - (I) si F est une formule, alors $\neg F$ est une formule ;
 - (I) si F et G sont des formules, alors $(F \wedge G)$, $(F \vee G)$, $(F \Rightarrow G)$, et $(F \Leftrightarrow G)$ sont des formules ;
 - (I) si F est une formule, et si $x \in \mathcal{V}$ est une variable, alors $\forall xF$ est une formule, et $\exists xF$ aussi.

Exemples

■ Exemples :

- ▶ $\forall x((Premier(x) \wedge x > 1 + 1) \Rightarrow Impair(x))$ est une formule sur la signature Σ précédente.
- ▶ $\exists x(s(x) = 1 + 0 \vee \forall y x + y > s(x))$ aussi.
- ▶ Exemples de formules sur la signature \mathcal{L}_2 :
 - $\forall x \forall y \forall z((R(x, y) \wedge R(y, z) \Rightarrow R(x, z))$
 - $\forall x \exists y(g(x, y) = c \wedge g(y, x) = c)$;
 - $\forall x \neg f(x) = c$;
 - $\forall x \exists y \neg f(x) = c$.

Théorème de décomposition/lecture unique

Ce sont des définitions inductives non-ambigües :

Théorème (de décomposition/lecture unique)

- *Toute formule F est d'une, et exactement d'une, des formes suivantes :*
 1. *une formule atomique ;*
 2. *$\neg G$, où G est une formule ;*
 3. *$(G \wedge H)$ où G et H sont des formules ;*
 4. *$(G \vee H)$ où G et H sont des formules ;*
 5. *$(G \Rightarrow H)$ où G et H sont des formules ;*
 6. *$(G \Leftrightarrow H)$ où G et H sont des formules ;*
 7. *$\forall xG$ où G est une formule et x une variable ;*
 8. *$\exists xG$ où G est une formule et x une variable.*

- *De plus dans le premier cas, il y a une unique façon de "lire" la formule atomique. Dans chacun des autres cas, il y a unicité de la formule G et de la formule H avec cette propriété.*

Plus précisément

Variables libres, variables liées

Sémantique

Intuition

- L'intuition de ce qui va suivre est de distinguer les variables **liées** des variables qui ne le sont pas.
- Tout cela est en fait à propos de " $\forall x$ " et " $\exists x$ " qui sont des **lieurs** :

Intuition

- L'intuition de ce qui va suivre est de distinguer les variables **liées** des variables qui ne le sont pas.
- Tout cela est en fait à propos de “ $\forall x$ ” et “ $\exists x$ ” qui sont des **lieux** :

- D'autres lieux en mathématiques :
 - ▶ le symbole intégrale : dans l'expression $\int_a^b f(t)dt$, la variable t est une variable muette (liée). $\int_a^b f(u)du$ est exactement la même intégrale.

Intuition

- L'intuition de ce qui va suivre est de distinguer les variables liées des variables qui ne le sont pas.
- Tout cela est en fait à propos de " $\forall x$ " et " $\exists x$ " qui sont des **lieurs** :
 - ▶ lorsqu'on écrit $\forall xF$ ou $\exists xF$, x devient une variable liée ;
 - ▶ en d'autres termes, x est une variable "muette" de $\forall xF$.
 - ▶ on pourrait tout aussi bien écrire $\forall yF(y/x)$ (respectivement : $\exists yF(y/x)$) où $F(y/x)$ désigne intuitivement la formule que l'on obtient en remplaçant x par y dans F .
- D'autres lieurs en mathématiques :
 - ▶ le symbole intégrale : dans l'expression $\int_a^b f(t)dt$, la variable t est une variable muette (liée). $\int_a^b f(u)du$ est exactement la même intégrale.

Le cas des termes

- Les variables libres d'un terme sont les variables qui apparaissent dans ce terme.
- Si on préfère : l'ensemble $\ell(t)$ des **variables libres d'un terme** t se définit inductivement par :

$$(B) \quad \ell(v) = \{v\} \text{ pour } v \in \mathcal{V};$$

$$(B) \quad \ell(c) = \emptyset \text{ pour } c \in \mathcal{C};$$

$$(I) \quad \ell(f(t_1, \dots, t_n)) = \ell(t_1) \cup \dots \cup \ell(t_n).$$

Le cas des formules

- L'ensemble $\ell(t)$ des **variables libres d'une formule** F se définit inductivement par :

$$(B) \ell(R(t_1, \dots, t_n)) = \ell(t_1) \cup \dots \cup \ell(t_n);$$

$$(I) \ell(\neg G) = \ell(G);$$

$$(I) \ell(G \vee H) = \ell(G \wedge H) = \ell(G \Rightarrow H) = \ell(G \Leftrightarrow H) = \ell(G) \cup \ell(H);$$

$$(I) \ell(\forall x F) = \ell(\exists x F) = \ell(F) \setminus \{x\}.$$

- Une formule F est dite **close** si elle ne possède pas de variables libres.

- Exemple :

▶ La formule $\forall x \forall z (R(x, z) \Rightarrow \exists y (R(y, z) \vee y = z))$ est close.

Plus précisément

Variables libres, variables liées

Sémantique

- Nous pouvons maintenant parler du sens que l'on donne aux formules.
- Pour donner un sens aux formules, il faut fixer un sens aux symboles de la signature, et c'est l'objet de la notion de structure.

Structures

- Soit $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$ une signature.
- Une **structure** \mathfrak{M} de signature Σ est la donnée :
 - ▶ d'un ensemble non-vide M , appelé **ensemble de base**, ou **domaine** de la structure ;
 - ▶ d'un élément de M , noté $c^{\mathfrak{M}}$, pour chaque symbole de constante $c \in \mathcal{C}$;
 - ▶ d'une fonction, notée $f^{\mathfrak{M}}$, de $M^n \rightarrow M$ pour chaque symbole de fonction $f \in \mathcal{F}$ d'arité n ;
 - ▶ d'un sous-ensemble, noté $R^{\mathfrak{M}}$, de M^n pour chaque symbole de relation $R \in \mathcal{R}$ d'arité n .
- On dit que la constante c (respectivement la fonction f , la relation R) est **interprétée par** $c^{\mathfrak{M}}$ (resp. $f^{\mathfrak{M}}$, $R^{\mathfrak{M}}$).
- Une structure est parfois aussi appelée une **réalisation**.

Exemples

■ Exemples :

- ▶ On peut obtenir une réalisation de la signature Σ précédente en prenant comme ensemble de base les entiers, 0 interprété par l'entier 0, 1 par l'entier 1, s par la fonction qui à l'entier x associe $x + 1$, $+$ par la fonction addition, *Impair* par les entiers impairs, *Premier* par les entiers premiers, $=$ par l'égalité, et $<$ par la relation $\{(x, y) | x < y\}$.

- On peut la noter $(\mathbb{N}, =, <, \textit{Impair}, \textit{Premier}, s, +, 0, 1)$.

- ▶ On peut obtenir une réalisation de la signature \mathcal{L}_2 en considérant l'ensemble de base \mathbb{R} des réels, en interprétant R comme la relation d'ordre \leq sur les réels, la fonction f comme la fonction qui à x associe $x + 1$, les fonctions g et h comme l'addition et la multiplication, les constantes c et d comme 0 et 1.

- On peut la noter $(\mathbb{R}, \leq, s, +, \times, 0, 1)$.

- On va ensuite utiliser la notion de structure pour interpréter
 1. les termes,
 2. les formules atomiques,
 3. puis inductivement les formules,

comme on peut s'y attendre.

- Une **valuation** v est une fonction de l'ensemble des variables \mathcal{V} dans le domaine M de la structure.
- Etant donnée une valuation v , l'interprétation :
 - ▶ d'un terme est un élément de l'ensemble de base de la structure :
 - ▶ d'une formule atomique est un objet qui s'interprète soit par **vrai** soit par **faux**.
 - ▶ d'une formule est un objet qui s'interprète soit par **vrai** soit par **faux**.

- Une **valuation** v est une fonction de l'ensemble des variables \mathcal{V} dans le domaine M de la structure.
- Etant donnée une valuation v , l'interprétation :
 - ▶ d'un terme est un élément de l'ensemble de base de la structure :
 - les termes désignent donc des éléments de la structure.
 - ▶ d'une formule atomique est un objet qui s'interprète soit par **vrai** soit par **faux**.

 - ▶ d'une formule est un objet qui s'interprète soit par **vrai** soit par **faux**.

- Une **valuation** ν est une fonction de l'ensemble des variables \mathcal{V} dans le domaine M de la structure.

- Etant donnée une valuation ν , l'interprétation :
 - ▶ d'un terme est un élément de l'ensemble de base de la structure :
 - les termes désignent donc des éléments de la structure.

 - ▶ d'une formule atomique est un objet qui s'interprète soit par **vrai** soit par **faux**.
 - les formules atomiques désignent donc des relations entre éléments de la structure.

 - ▶ d'une formule est un objet qui s'interprète soit par **vrai** soit par **faux**.

Formellement : interprétation des termes

- Soit \mathfrak{M} une structure de signature $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$ et ν une valuation.

Définition

L'interprétation $t^{\mathfrak{M}}$ du terme t en ν , aussi notée $t^{\mathfrak{M}}$ est définie inductivement de la façon suivante :

- (B) toute variable est interprétée par sa valeur dans la valuation :*
- (B) toute constante est interprétée par son interprétation dans la structure :*
- (I) chaque symbole de fonction est interprété par son interprétation dans la structure.*

Formellement : interprétation des termes

- Soit \mathfrak{M} une structure de signature $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$ et v une valuation.

Définition

L'interprétation $t^{\mathfrak{M}}$ du terme t en v , aussi notée $t^{\mathfrak{M}}$ est définie inductivement de la façon suivante :

- (B) *toute variable est interprétée par sa valeur dans la valuation :*
 - *c-à-d : si t est la variable $x_i \in \mathcal{V}$, alors $t^{\mathfrak{M}}$ est $v(x_i)$;*
- (B) *toute constante est interprétée par son interprétation dans la structure :*
- (I) *chaque symbole de fonction est interprété par son interprétation dans la structure.*

Formellement : interprétation des termes

- Soit \mathfrak{M} une structure de signature $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$ et v une valuation.

Définition

L'interprétation $t^{\mathfrak{M}}$ du terme t en v , aussi notée $t^{\mathfrak{M}}$ est définie inductivement de la façon suivante :

- (B) *toute variable est interprétée par sa valeur dans la valuation :*
 - *c-à-d : si t est la variable $x_i \in \mathcal{V}$, alors $t^{\mathfrak{M}}$ est $v(x_i)$;*
- (B) *toute constante est interprétée par son interprétation dans la structure :*
 - *c-à-d : si t est la constante $c \in \mathcal{C}$, alors $t^{\mathfrak{M}}$ est $c^{\mathfrak{M}}$;*
- (I) *chaque symbole de fonction est interprété par son interprétation dans la structure.*

Formellement : interprétation des termes

- Soit \mathfrak{M} une structure de signature $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$ et v une valuation.

Définition

L'*interprétation* $t^{\mathfrak{M}}$ du terme t en v , aussi notée $t^{\mathfrak{M}}$ est définie inductivement de la façon suivante :

- (B) toute variable est interprétée par sa valeur dans la valuation :
 - c-à-d : si t est la variable $x_i \in \mathcal{V}$, alors $t^{\mathfrak{M}}$ est $v(x_i)$;
- (B) toute constante est interprétée par son interprétation dans la structure :
 - c-à-d : si t est la constante $c \in \mathcal{C}$, alors $t^{\mathfrak{M}}$ est $c^{\mathfrak{M}}$;
- (I) chaque symbole de fonction est interprété par son interprétation dans la structure.
 - c-à-d : si t est le terme $f(t_1, \dots, t_n)$, alors $t^{\mathfrak{M}}$ est $f^{\mathfrak{M}}(t_1^{\mathfrak{M}}, \dots, t_n^{\mathfrak{M}})$, où $t_1^{\mathfrak{M}}, \dots, t_n^{\mathfrak{M}}$ sont les interprétations respectives des termes t_1, \dots, t_n .

Exemples

■ Exemples :

- ▶ Soit \mathcal{N} la structure $(\mathbb{N}, \leq, s, +, \times, 0, 1)$ de signature $\mathcal{L}_2 = (\{c, d\}, \{f, g, h\}, \{R\})$.
 - l'interprétation du terme $h(d, x)$ pour une valuation telle que $v(x) = 2$ est 2.
 - l'interprétation du terme $f(g(d, h(y, z)))$ pour une valuation telle que $v(y) = 2, v(z) = 3$ est 8.

Interprétation des formules atomiques

- Soit \mathfrak{M} une structure de signature $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$ et v une valuation.

Définition

La valuation v *satisfait la formule atomique* $R(t_1, t_2, \dots, t_n)$ de variables libres x_1, \dots, x_k si

$$(t_1^{\mathfrak{M}}, t_2^{\mathfrak{M}}, \dots, t_n^{\mathfrak{M}}) \in R^{\mathfrak{M}},$$

où $R^{\mathfrak{M}}$ est l'interprétation du symbole R dans la structure.

Exemples

- Exemples :

- ▶ Sur la structure Σ précédente $x < 1 + 1$ s'interprète par vrai en une valuation telle que $v(x) = 1$, et par faux en une valuation telle que $v(x) = 5$. La formule atomique $0 = s(0)$ s'interprète par faux.
- ▶ Sur la structure \mathcal{N} , $R(f(c), h(c, f(d)))$ s'interprète par faux.

Interprétation des formules

- Soit \mathfrak{M} une structure de signature $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$ et v une valuation.

Définition

L'expression "la valuation v satisfait la formule $F = F(x_1, \dots, x_k)$ ", notée $v \models F$, se définit inductivement de la façon suivante :

- (B) elle a déjà été définie pour une formule atomique ;
 - (I) $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$ sont interprétés exactement comme dans le calcul propositionnel.
-
- (I) $\exists x$ et $\forall x$ sont interprétés comme des quantifications existentielles et universelles :
 - ▶ si F est de la forme $\forall x_0 G(x_0, x_1, \dots, x_k)$, alors $v \models F$ ssi pour tout $a_0 \in M$, $v' \models G$, où v' est la valuation telle que $v'(x_0) = a_0$, et $v'(x) = v(x)$ pour tout $x \neq x_0$.
 - ▶ si F est de la forme $\exists x_0 G(x_0, x_1, \dots, x_k)$, alors $s \models F$ ssi pour un certain $a_0 \in M$, $v' \models G$, où v' est la valuation telle que $v'(x_0) = a_0$, et $v'(x) = v(x)$ pour tout $x \neq x_0$.

Interprétation des formules

- Soit \mathfrak{M} une structure de signature $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$ et v une valuation.

Définition

L'expression "la valuation v satisfait la formule $F = F(x_1, \dots, x_k)$ ", notée $v \models F$, se définit inductivement de la façon suivante :

(B) elle a déjà été définie pour une formule atomique ;

(I) $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$ sont interprétés exactement comme dans le calcul propositionnel.

- exemple du \vee : si F est de la forme $(G \vee H)$, alors $v \models F$ ssi $v \models G$ ou $v \models H$;

(I) $\exists x$ et $\forall x$ sont interprétés comme des quantifications existentielles et universelles :

- ▶ si F est de la forme $\forall x_0 G(x_0, x_1, \dots, x_k)$, alors $v \models F$ ssi pour tout $a_0 \in M$, $v' \models G$, où v' est la valuation telle que $v'(x_0) = a_0$, et $v'(x) = v(x)$ pour tout $x \neq x_0$.
- ▶ si F est de la forme $\exists x_0 G(x_0, x_1, \dots, x_k)$, alors $s \models F$ ssi pour un certain $a_0 \in M$, $v' \models G$, où v' est la valuation telle que $v'(x_0) = a_0$, et $v'(x) = v(x)$ pour tout $x \neq x_0$.

- 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} .

Au menu

Exemples de théories du premier ordre

Le prochain épisode : le monde est beau

Plus précisément

Exemples de théories du premier ordre

La notion de théorie

Groupes

Corps

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.

Plus précisément

Exemples de théories du premier ordre

La notion de théorie

Groupes

Corps

Groupe

- Un groupe est un modèle égalitaire³ de la théorie constituée des deux formules :

$$\forall x \forall y \forall z \ x * (y * z) = (x * y) * z \quad (1)$$

$$\exists e \forall x \ (x * e = e * x = x \wedge \exists y (x * y = y * x = e)) \quad (2)$$

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

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

Plus précisément

Exemples de théories du premier ordre

La notion de théorie

Groupes

Corps

Corps

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

$$\forall x \forall y \forall z (x + (y + z) = (x + y) + z) \quad (3)$$

$$\forall x \forall y (x + y = y + x) \quad (4)$$

$$\forall x (x + 0 = x) \quad (5)$$

$$\forall x \exists y (x + y = 0) \quad (6)$$

$$\forall x \forall y \forall z x * (y + z) = x * y + x * z \quad (7)$$

$$\forall x \forall y \forall z ((x * y) * z) = (x * (y * z)) \quad (8)$$

$$\forall x \forall y (x * y = y * x) \quad (9)$$

$$\forall x (x * 1 = x) \quad (10)$$

$$\forall x \exists y (x = 0 \vee x * y = 1) \quad (11)$$

$$\neg 1 = 0 \quad (12)$$

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

Au menu

Exemples de théories du premier ordre

Le prochain épisode : le monde est beau

Le prochain épisode : le monde est beau

- 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 (Validité)

*Soit \mathcal{T} une théorie. Soit F une formule close.
Si $\mathcal{T} \vdash F$ alors $\mathcal{T} \models F$.*

Théorème (Complétude)

*Soit \mathcal{T} une théorie. Soit F une formule close.
Si $\mathcal{T} \models F$ alors $\mathcal{T} \vdash F$.*

Exprimez vous.



Page du cours.



Commentaires, avis
sur les cours et les PCs.

- Page du cours:
<https://moodle.polytechnique.fr/course/view.php?id=14459>.
- Commentaires, avis sur les cours et les PCs.
www.enseignement.polytechnique.fr/informatique/INF412/AVIS.

ANNEXES

ANNEXE

Le prochain épisode : le monde est beau
Preuves du théorème de compacité

- Démonstration par la topologie (du sens non-trivial de la version 1 du théorème de compacité).
 - ▶ L'espace topologique $\{0,1\}^{\mathcal{P}}$ (muni de la topologie produit) est un espace compact, car il s'obtient comme un produit de compacts (Théorème de Tychonoff).
 - ▶ Pour chaque formule propositionnelle $F \in \Sigma$, l'ensemble \overline{F} des valuations qui la satisfont est un ouvert dans $\{0,1\}^{\mathcal{P}}$, car la valeur de vérité d'une formule ne dépend que d'un nombre fini de variables, celles qui apparaissent dans la formule.
 - ▶ Il est également fermé puisque celles qui ne satisfont pas F sont celles qui satisfont $\neg F$.
 - ▶ Dire que $\{0,1\}^{\mathcal{P}}$ est compact est équivalent à dire que de toute famille de fermés dont l'intersection est vide on peut extraire une famille finie dont l'intersection est aussi vide ((complémentaire de la) propriété de Borel-Lebesgue).
 - ▶ L'hypothèse du théorème entraîne que toute intersection d'un nombre fini de \overline{F} pour $F \in \Sigma$ est non-vide.
 - ▶ L'intersection de tous les \overline{F} pour $F \in \Sigma$ est donc non vide, ce qui prouve le résultat.

■ Démonstration sans topologie du théorème de compacité :

- ▶ Considérons $\mathcal{P} = \{p_1, p_2, \dots, p_k, \dots\}$ une énumération de \mathcal{P} .
- ▶ Lemme : supposons qu'il existe une application v de $\{p_1, p_2, \dots, p_n\}$ dans $\{0, 1\}$ telle que tout sous-ensemble fini de Σ ait un modèle dans lequel p_1, \dots, p_n prennent les valeurs $v(p_1), \dots, v(p_n)$. Alors on peut étendre v à $\{p_1, p_2, \dots, p_{n+1}\}$ avec la même propriété.
 - En effet, si $v(p_{n+1}) = 0$ ne convient pas, alors il existe un ensemble fini U_0 de Σ qui ne peut pas être satisfait quand p_1, \dots, p_n, p_{n+1} prennent les valeurs respectives $v(p_1), \dots, v(p_n)$ et 0.
 - Si U est un sous-ensemble fini quelconque de Σ , alors d'après l'hypothèse faite sur v , $U_0 \cup U$ a un modèle dans lequel p_1, \dots, p_n prennent les valeurs $v(p_1), \dots, v(p_n)$.
 - Dans ce modèle, la proposition p_{n+1} prend donc la valeur 1. Autrement dit, tout sous-ensemble fini U de Σ a un modèle dans lequel p_1, \dots, p_n, p_{n+1} prennent les valeurs respectives $v(p_1), \dots, v(p_n)$ et 1.
 - Dit encore autrement, soit $v(p_{n+1}) = 0$ convient auquel cas on peut fixer $v(p_{n+1}) = 0$, soit $v(p_{n+1}) = 0$ ne convient pas auquel cas on peut fixer $v(p_{n+1}) = 1$ qui convient.

- ▶ En utilisant ce lemme, on définit ainsi une valuation v telle que, par récurrence sur n , pour chaque n , tout sous-ensemble fini de Σ a un modèle dans lequel p_1, \dots, p_n prennent les valeurs $v(p_1), \dots, v(p_n)$.
- ▶ Il en résulte que v satisfait Σ :
 - En effet, soit F une formule de Σ .
 - F ne dépend que d'un ensemble fini $p_{i_1}, p_{i_2}, \dots, p_{i_k}$ de variables propositionnelles (celles qui apparaissent dans F).
 - En considérant $n = \max(i_1, i_2, \dots, i_k)$, chacune de ces variables p_{i_j} est parmi $\{p_1, \dots, p_n\}$.
 - Nous savons alors que le sous ensemble fini $\{F\}$ réduit à la formule F admet un modèle dans lequel p_1, \dots, p_n prennent les valeurs $v(p_1), \dots, v(p_n)$, i.e. F est satisfaite par v .