

Kit de survie - Logique

François SCHWARZENTRUBER

Préparation à l'option informatique de l'agrégation de mathématiques
ÉNS Rennes

Table des matières

I	Logique propositionnelle	5
1	Logique propositionnelle et problème SAT	7
1.1	Motivation : problème de coloration	7
1.2	Un modèle : une valuation	7
1.3	Langage	8
1.3.1	Syntaxe	8
1.3.2	Sémantique	8
1.4	Théories	9
1.5	Systèmes de connecteurs complets	9
1.6	Problèmes de décision	9
1.7	Application pratique	9
2	Formes normales	11
2.1	Forme normale conjonctive	11
2.2	Transformation de Tseitin ([BA12], p. 91)	11
2.3	Fragments syntaxiques basés sur les FNC	12
2.3.1	Formules de Horn ([DPV16], p. 157)	12
2.3.2	2-formes normales	13
3	Résolution en logique propositionnelle	15
3.1	Règle de résolution	15
3.2	Arbre de preuve	15
3.3	Correction et complétude	16
4	Théorème de compacité	17
II	Logique des prédicats du premier ordre	19
5	Syntaxe et sémantique	21
5.1	Modèles	21
5.2	Langage	22
5.2.1	Syntaxe	22
5.2.2	Sémantique	22
5.3	Variables libres/liées	23
5.4	Satisfiable, valide, conséquence sémantique	23
5.5	Model checking	24
5.6	Problème de la satisfiabilité et problème de la validité	24
6	Théories	25
6.1	Définitions	25
6.2	Exemples de théories	26
6.2.1	Théorie de l'égalité	26
6.2.2	Théorie des groupes ([Lal90], p. 139) ([DNRC01], p. 105)	26
6.2.3	Théorie des ordres denses ([DNRC01], p. 130)	27
6.2.4	Théorie des corps clos ([DNRC01], p. 133)	27
6.2.5	Arithmétique de Presburger ([DNRC01], p. 136)	27
6.2.6	Arithmétique de Peano ([DNRC01], p. 111)	27
6.2.7	Arithmétique vraie sur \mathbb{N}	28
6.3	Résultats	28

7	Déduction naturelle	29
7.1	Substitution	29
7.2	Règles de la déduction naturelle ([DNRC01], p. 25)	30
7.3	Arbres de preuve	31
7.4	Correction et complétude	32
7.4.1	Énoncé	32
7.4.2	Idée de la démonstration	32
7.5	Conséquences	33
7.5.1	Problème de validité dans RE	33
7.5.2	Théorème de compacité	34
7.5.3	Théorème de Lowenheim-Skolem	34
8	Résolution en logique du premier ordre	35
8.1	Skolémisation ([BA12], p. 174)	35
8.2	Résolution en logique du premier ordre	37
8.2.1	Unification ([LDR93], p. 86) ([BA12], p. 189)	37
8.2.2	Règle de résolution ([DNRC01], p. 265)	37
8.2.3	Contraction ([DNRC01], p. 265)	37
8.3	Modèles de Herbrand	38
8.4	Correction et complétude	39
9	Calcul des séquents	41
9.1	Motivation	41
9.2	Règles du calcul des séquents ([DNRC01], p. 187)	41
9.3	Correction et complétude	43
9.4	Élimination de la règle de la coupure	43

Première partie
Logique propositionnelle

Chapitre 1

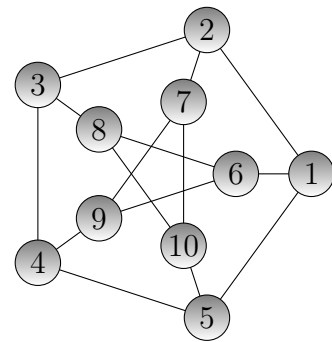
Logique propositionnelle et problème SAT

Points du programme de l'agrégation

Calcul propositionnel : syntaxe et sémantique. Tables de vérité. Tautologies.

1.1 Motivation : problème de coloration

On souhaite trouver une 3-coloration d'un graphe G non orienté. L'idée est d'exprimer les contraintes de coloriage avec une formule de la logique propositionnelle.



1.2 Un modèle : une valuation

Soit AP un ensemble dénombrable de **propositions atomiques**. Un modèle de la logique propositionnelle est une valuation. Formellement :

Définition 1 (valuation)

Une **valuation** V est une fonction de AP dans $\{0, 1\}$.

Exemple 2 Pour toute sommet s et toute couleur c , on introduit la proposition atomique

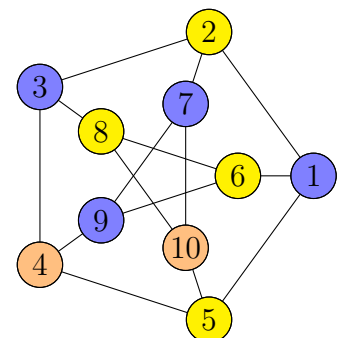
$$p_{s,c}$$

qui signifie intuitivement que

la couleur du sommet s est c .

Une valuation représente une 3-coloration. La 3-coloration donnée sur le graphe est représentée par la valuation V définie par :

- $V(p_{1,\bullet}) = V(p_{2,\bullet}) = \dots = 1$;
- $V(p_{1,\bullet}) = V(p_{1,\bullet}) = \dots = 0$.



1.3 Langage

1.3.1 Syntaxe

Définition 3 (syntaxe du langage de la logique propositionnelle)

Le langage de la logique propositionnelle \mathcal{L} est défini par la grammaire suivante :

$$\varphi ::= \perp \mid p \mid \neg\varphi \mid (\varphi \vee \psi) \mid (\varphi \wedge \psi)$$

où p désigne une proposition atomique dans AP .

On introduit les abréviations suivantes :

- $(\varphi \rightarrow \psi)$ pour $(\neg\varphi \vee \psi)$;
- $(\varphi \leftrightarrow \psi)$ pour $((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi))$.

On omet les parenthèses quand elles sont évidentes.

Exemple 4 On écrit $p \vee q \vee r$ au lieu de $(p \vee (q \vee r))$.

1.3.2 Sémantique

Définition 5 (conditions de vérité)

$V \models \varphi$ est défini par induction structurelle sur φ :

- $V \not\models \perp$;
- $V \models p$ si $V(p) = 1$;
- $V \models \neg\varphi$ si $\text{not } V \models \varphi$;
- $V \models (\varphi \vee \psi)$ si $V \models \varphi$ ou $V \models \psi$;
- $V \models (\varphi \wedge \psi)$ si $V \models \varphi$ et $V \models \psi$.

Tables de vérité

Dans une table de vérité, chaque ligne correspond à une valuation V , et on inscrit 1 dans la colonne pour φ si $V \models \varphi$ et 0 si $V \not\models \varphi$.

p	q	$\neg q$	$p \vee \neg q$
0	0	1	1
0	1	0	0
1	0	1	1
1	1	0	1

Définition 6 (satisfiable)

φ est **satisfiable**

s'il existe une valuation V telle que $V \models \varphi$.

	φ
.	.
.	1
.	.
.	.

Définition 7 (valide)

φ est **valide** (ou est une **tautologie**)

si pour toute valuation V , on a $V \models \varphi$.

	φ
.	1
.	1
.	1
.	1
.	1

1.4 Théories

Définition 8 (théorie)

Une **théorie** T est un ensemble de formules.

Définition 9 (notation $V \models T$)

On écrit $V \models T$ pour dire que pour toute formule ψ de T , on a $V \models \psi$.

Définition 10 (conséquence sémantique)

φ est **conséquence sémantique** d'une théorie T , noté $T \models \varphi$,
si pour toute valuation V , on a $V \models T$ implique $V \models \varphi$.

1.5 Systèmes de connecteurs complets

Définition 11 (formules équivalentes)

φ et ψ sont **équivalentes** si pour toute valuation V , ($V \models \varphi$ si et seulement $V \models \psi$).

Définition 12 (système de connecteurs complet)

Un système de connecteurs est **complet** si toute formule est équivalente à une formule qui ne contient que ces connecteurs là.

Proposition 13 Les système de connecteurs $\{\neg, \wedge\}$, $\{\neg, \rightarrow\}$, $\{\neg, \vee\}$ sont complets.

1.6 Problèmes de décision

Définition 14 (problème SAT)

- entrée : φ ;
- sortie : oui si φ est satisfiable ; non, sinon.

Définition 16 (problème VALIDE)

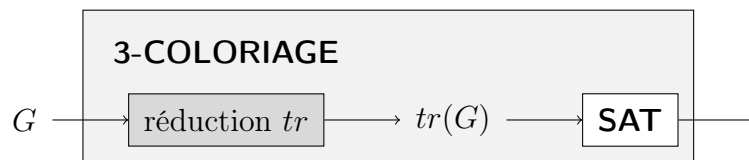
- entrée : φ ;
- sortie : oui si φ est valide ; non, sinon.

Théorème 15 SAT est NP-complet.

Théorème 17 VALIDE est coNP-complet.

1.7 Application pratique

On réduit le problème de 3-coloriage au problème SAT :



Chapitre 2

Formes normales

Points du programme de l'agrégation

Formes normales, forme clause.

2.1 Forme normale conjonctive

Définition 18 (littéral)

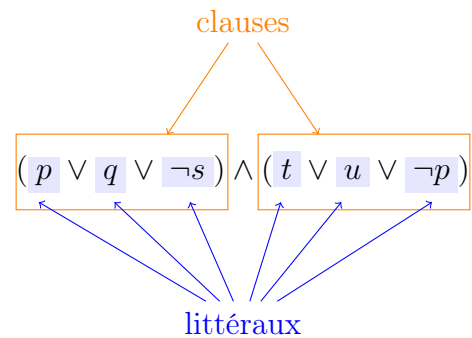
Un **littéral** est une proposition atomique ou la négation d'une proposition atomique.

Définition 19 (forme normale conjonctive)

Une **forme normale conjonctive** (FNC) est une formule de la forme $\bigwedge_{i=1}^n \bigvee_{j=1}^{m_i} \ell_{i,j}$ où les $\ell_{i,j}$ sont des littéraux.

Théorème 20 Toute formule est équivalente à une FNC

...potentiellement exponentiellement plus longue.



Exemple 21 $(p \wedge q) \vee (r \wedge s) \equiv ((p \wedge q) \vee r) \wedge ((p \wedge q) \vee s) \equiv (p \vee r) \wedge (q \vee r) \wedge (p \vee s) \wedge (q \vee s)$.

2.2 Transformation de Tseitin ([BA12], p. 91)

Définition 22 (équiasatisfiable)

φ et ψ est **équiasatisfiable** ssi (φ satisfiable ssi ψ satisfiable).

Théorème 23 Toute formule φ est équiasatisfiable à une FNC $tr(\varphi)$

...de taille $O(\varphi)$.

IDÉE DE LA DÉMONSTRATION.

1. Introduire une var. prop. α_ψ par sous-formules ψ de φ qui signifie ' ψ est vraie'.
2. Coder les conditions de vérité par des clauses.

$$\begin{aligned}
 & \alpha_{(p \vee (q \wedge r))} \wedge \\
 & (\alpha_{(p \vee (q \wedge r))} \rightarrow (\alpha_p \vee \alpha_{(q \wedge r)})) \wedge \\
 & (\alpha_p \rightarrow \alpha_{(p \vee (q \wedge r))}) \wedge (\alpha_{(q \wedge r)} \rightarrow \alpha_{(p \vee (q \wedge r))}) \wedge \\
 & (\alpha_{(q \wedge r)} \rightarrow \alpha_q) \wedge \\
 & (\alpha_{(q \wedge r)} \rightarrow \alpha_r) \wedge \\
 & ((\alpha_q \wedge \alpha_r) \rightarrow \alpha_{(q \wedge r)})
 \end{aligned}$$

est satisfiable ssi satisfiable.

■

2.3 Fragments syntaxiques basés sur les FNC

2.3.1 Formules de Horn ([DPV16], p. 157)

Définition 24 (clause de Horn)

Une **clause de Horn** est une clause de la forme $(p_1 \wedge \dots \wedge p_n) \rightarrow p$ ou $(p_1 \wedge \dots \wedge p_n) \rightarrow \perp$.



Définition 25 (formule de Horn)

Une **formule de Horn** est une conjonction de clauses de Horn.



Définition 26 (problème HORN-SAT)

Le **problème HORN-SAT** est le problème décision :

- Entrée : une formule de Horn ;
- Sortie : oui si elle est satisfiable ; non sinon.

Théorème 27 *Le problème HORN-SAT est dans P.*

IDÉE DE LA DÉMONSTRATION.

```

fonction satHorn( $\varphi$ )
   $V :=$  valuation où toutes les propositions atomiques sont fausses
  tant que il existe une clause  $\Gamma \rightarrow p$  avec  $V \not\models \Gamma \rightarrow p$  do
    |  $V := V[p := \top]$ 
  si une clause  $\Gamma \rightarrow \perp$  avec  $V \models \Gamma$  alors
    | retourner insatisfiable
  sinon
    | retourner  $V$ 

```

Lemme 28 *satHorn(φ) retourne une valuation V ssi φ est satisfiable.*

IDÉE DE LA DÉMONSTRATION.

- \Rightarrow La valuation V satisfait φ .
- \Leftarrow Soit V' telle que $V' \models \varphi$. La propriété ' $V \subseteq V'$ ' est un invariant. ■

Applications : calcul de premier, suivant en analyse syntaxique LL(1), des non-terminaux productifs d'une grammaire algébrique, des non-terminaux qui engendre ϵ [LS15].

2.3.2 2-formes normales

Définition 29 (problème 2SAT)

Le **problème 2SAT** est le problème décision :

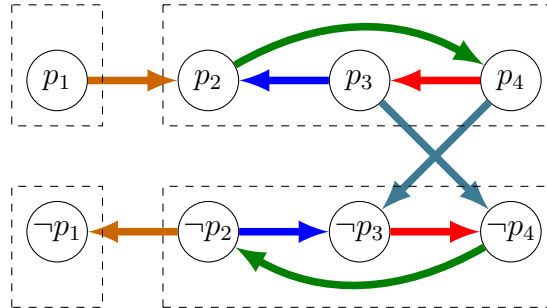
- Entrée : une FNC avec 2 littéraux par clause ;
- Sortie : oui si elle est satisfiable ; non sinon.

Définition 30 (graphe d'implication)

Soit φ une 2-CNF. Le **graphe d'implication** G_φ est le graphe où :

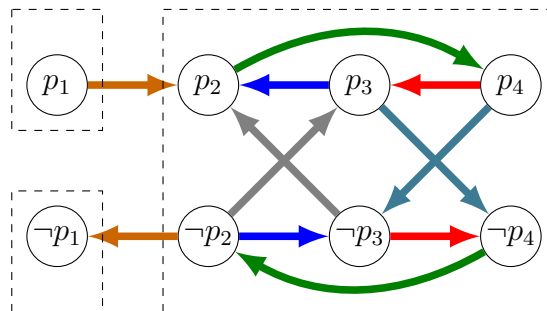
- les sommets sont les propositions atomiques de φ et leurs négations ;
- il y a un arc (α, β) si $\alpha \rightarrow \beta$ est équivalente à une clause de φ .

Exemple 31 $(p_3 \vee \neg p_4) \wedge (p_2 \vee \neg p_3) \wedge (p_4 \vee \neg p_2) \wedge (\neg p_1 \vee p_2) \wedge (\neg p_4 \vee \neg p_3)$ est satisfiable.



Exemple 32

$(p_3 \vee \neg p_4) \wedge (p_2 \vee \neg p_3) \wedge (p_4 \vee \neg p_2) \wedge (\neg p_1 \vee p_2) \wedge (\neg p_4 \vee \neg p_3) \wedge (p_3 \vee p_2)$ n'est pas satisfiable.



Théorème 33 Le problème 2-SAT est dans P.

IDÉE DE LA DÉMONSTRATION.

```

fonction sat2sat( $\varphi$ )
  Construire le graphe d'implication  $G_\varphi$ 
  Calculer les composantes fortement connexes de  $G_\varphi$ 
  si il existe  $p$  tel que  $p$  et  $\neg p$  sont dans la même composante fortement connexe alors
    | retourner insatisfiable
  sinon
    | retourner satisfiable
    
```

Lemme 34 $\text{sat2sat}(\varphi)$ retourne *satisfiable* ssi φ est satisfiable.

IDÉE DE LA DÉMONSTRATION.

(\Leftarrow) Soit V une valuation telle que $V \models \varphi$. Par l'absurde, supposons qu'il existe p et $\neg p$ dans la même composante fortement connexe (cfc). Sans perte de généralité, supposons que $V \models p$. Comme il y a un chemin de $p = \ell_0, \ell_1, \dots, \ell_n = \neg p$ dans G_φ , et comme $V \models \ell_i \rightarrow \ell_{i+1}$, on montre par récurrence sur i que $V \models \ell_i$ pour tout i . Donc $V \models \neg p$. Contradiction.

(\Rightarrow) Supposons que $\text{sat2sat}(\varphi)$ retourne *satisfiable*. Considérons l'algorithme suivant :

```

fonction construireValuation( $G$ )
  si le graphe  $G$  est vide alors
    | retourner valuation partielle vide
  sinon
    | Soit  $C$  une cfc finale de  $G$ 
    |  $V := \text{construireValuation}(G - (C \cup \{\neg \ell \mid \ell \in C\}))$ 
    | Mettre tous les littéraux de  $C$  à vrai dans  $V$ 
    | retourner  $V$ 

```

On considère la valuation $V := \text{construireValuation}(G_\varphi)$.

Fait 1 L'opération 'Mettre tous les littéraux de C à vrai dans V ' est bien définie.

IDÉE DE LA DÉMONSTRATION.

Comme p et $\neg p$ ne sont pas dans la même cfc, on donne une valeur unique à p . ■

Fait 2 V est une valuation totale sur les propositions apparaissant dans φ .

IDÉE DE LA DÉMONSTRATION.

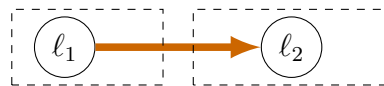
Car on considère tous les sommets de G_φ . ■

Fait 3 $V \models \varphi$.

IDÉE DE LA DÉMONSTRATION.

On considère une clause $\ell_1 \rightarrow \ell_2$ de φ . Montrons $V \models \ell_1 \rightarrow \ell_2$. Supposons que $V \models \ell_1$. Ainsi, ℓ_1 a été mis à vrai dans $\text{construireValuation}$: on avait $\ell_1 \in C_1$ où C_1 est finale dans un certain graphe G_1 .

- Si ℓ_1 et ℓ_2 dans une même cfc de G_φ , alors ℓ_2 est aussi mis à vraie, comme ℓ_1 .
- Sinon, dans G_φ :



Mais au moment, où ℓ_1 est affecté, la classe de ℓ_2 a déjà été supprimée car C_1 est finale :



Mais lorsque ℓ_2 a été supprimé, il n'était pas dans une classe initiale \bar{C} car $\ell_1 \rightarrow \ell_2$ était un arc entrant dans la classe de ℓ_2 . Ainsi, ℓ_2 était dans une classe finale C_2 et il a été affecté à vraie. Ainsi, $V \models \ell_2$.

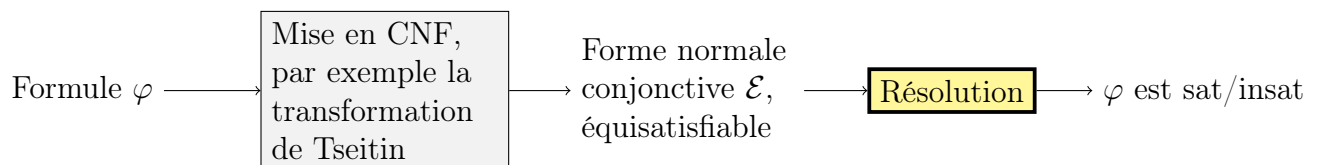
■ ■ ■

Chapitre 3

Résolution en logique propositionnelle

Points du programme de l'agrégation

Théorème de complétude du calcul propositionnel



3.1 Règle de résolution

Définition 35 (règle de résolution)

([BA12], p. 82) La **règle de résolution** est la règle

$$\frac{(p \vee \ell_1 \vee \dots \vee \ell_n) \quad (\neg p \vee \ell'_1 \vee \dots \vee \ell'_k)}{(\ell_1 \vee \dots \vee \ell_n \vee \ell'_1 \vee \dots \vee \ell'_k)}$$

à permutation près des littéraux et en supprimant les répétitions de littéraux¹.

La nouvelle clause obtenue $(\ell_1 \vee \dots \vee \ell_n \vee \ell'_1 \vee \dots \vee \ell'_k)$ s'appelle le **résolvant**.

Exemple 36 *Le modus ponens $\frac{p \quad (p \rightarrow q)}{q}$ en est un cas particulier.*

3.2 Arbre de preuve

Définition 37 (preuve par résolution)

Soit \mathcal{E} une forme normale conjonctive². Une **preuve par résolution** de φ pour \mathcal{E} est un arbre fini étiqueté par des clauses tel que :

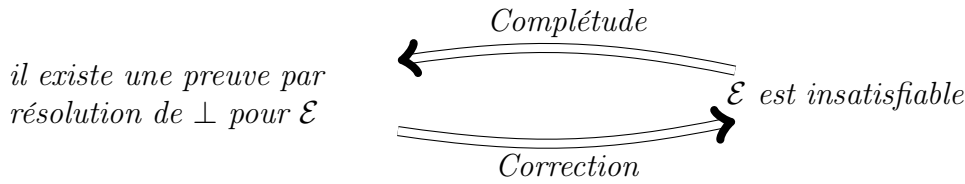
- Les feuilles sont des clauses de \mathcal{E} ;
- La racine est φ ;
- Chaque nœud interne correspond à l'application de la règle de résolution.

1. Une présentation plus bas niveau les clauses sont représentées des ensembles évite ce problème. Par exemple $(p \vee \neg q)$ est représentée par l'ensemble $\{p, \neg q\}$. Nous préférons ici une présentation haut niveau.

2. Certains auteurs [BA12] parlent d'ensemble de clauses.

3.3 Correction et complétude

Théorème 38 ([BA12], p. 82) Soit \mathcal{E} un forme normale conjonctive.



IDÉE DE LA DÉMONSTRATION.

\Rightarrow Par contraposée, supposons \mathcal{E} satisfiable, i.e. il existe une valuation V telle que $V \models \mathcal{E}$.

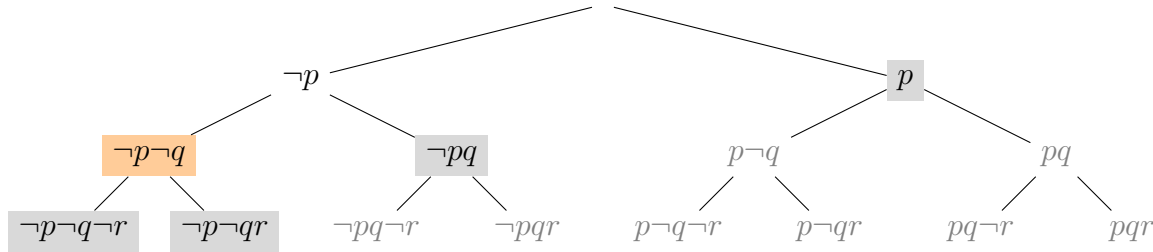
Lemme 39 Si $\frac{C_1 \quad C_2}{C}$, $V \models C_1$ et $V \models C_2$ alors $V \models C$.

On montre par induction structurale sur les preuves $\frac{\vdots}{\varphi}$ pour \mathcal{E} la propriété

$$\mathcal{P}\left(\frac{\vdots}{\varphi}\right) : V \models \varphi$$

Ainsi, il n'existe pas de preuve par résolution de \perp pour \mathcal{E} .

\Leftarrow Supposons \mathcal{E} insatisfiable. Considérons l'arbre de décision sur les propositions p_1, \dots, p_n apparaissant dans \mathcal{E} . Un nœud interne correspond à une valuation partielle et une feuille à une valuation totale sur p_1, \dots, p_n . Un **nœud d'échec** est un nœud le plus proche de la racine, dont la valuation partielle rend une des clauses de \mathcal{E} fausse. Un **nœud d'inférence** est un nœud dont les fils sont des nœuds d'échec.



Lemme 40 Si \mathcal{E} est insatisfiable, alors il existe un nœud d'inférence.

IDÉE DE LA DÉMONSTRATION.

Par l'absurde, supposons qu'il n'y a pas de nœud d'inférence. Alors on considère un nœud d'échec n_0 . Son frère n'est pas un nœud d'échec mais son sous-arbre en contient un strictement plus profond. On construit une suite infinie n_0, n_1, \dots de nœuds d'échec de plus en plus profond. Contradiction. ■

Lemme 41 Soit n un nœud d'inférence de fils n_1 et n_2 . Si C_1 est falsifié par n_1 et C_2 est falsifié par n_2 , alors on peut appliquer la règle de résolution $\frac{C_1 \quad C_2}{C}$ et n falsifie C .

L'algorithme suivant construit une preuve par résolution de \perp pour \mathcal{E} :

tant que \perp n'est pas produite **do**
 | Appliquer la règle de résolution sur un nœud d'inférence.

L'algorithme termine car le nombre de nœuds d'échec décroît strictement : avec $\mathcal{E} \wedge C$ à la place de \mathcal{E} , un ancêtre du nœud d'inférence considéré devient nœud d'échec. ■

Chapitre 4

Théorème de compacité

Théorème 42 Soit E un ensemble de formules de la logique propositionnelle. Si tout sous-ensemble fini de E est satisfiable, alors E l'est aussi.

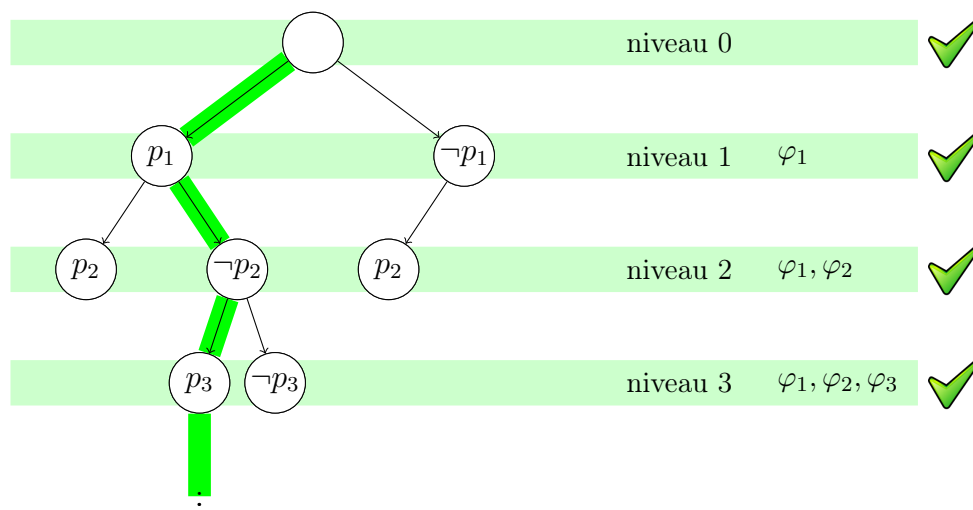
IDÉE DE LA DÉMONSTRATION.

On considère :

- $\varphi_1, \varphi_2, \dots$ une énumération des formules de E ;
- et p_1, p_2, \dots une énumération des propositions atomiques.

On construit l'arbre¹ suivant par récurrence.

- La racine est le nœud de niveau 0.
- Supposons que tous les nœuds de niveau $n - 1$ soient construits. On attache :
 - on attache un nœud p_n à une branche $\pm p_1, \dots, \pm p_{n-1}$ si $\{\pm p_1, \dots, \pm p_{n-1}, p_n, \varphi_1, \dots, \varphi_n\}$ est satisfiable ;
 - on attache un nœud $\neg p_n$ à une branche $\pm p_1, \dots, \pm p_{n-1}$ si $\{\pm p_1, \dots, \pm p_{n-1}, \neg p_n, \varphi_1, \dots, \varphi_n\}$ est satisfiable ;



Comme pour tout $n \in \mathbb{N}$, $\{\varphi_1, \dots, \varphi_n\}$ est satisfiable. On peut toujours continuer à attacher des nœuds. Ainsi, l'arbre est infini.

Comme l'arbre est infini et à branchement fini, d'après le **lemme de König**, il a une branche infinie. Cette branche définit une valuation qui satisfait T . ■

1. C'est un sous-arbre de l'arbre de décision.

Corollaire 43 (Théorème de De Bruijn-Erdős) *Un graphe G est 3-coloriable si et seulement si tout sous-graphe fini de G est 3-coloriable.*

IDÉE DE LA DÉMONSTRATION.

\Rightarrow Immédiat.

\Leftarrow Supposons que tout sous-graphe fini de G est 3-coloriable.

Soit S' un sous-ensemble de sommets de $G = (S, A)$. On note :

$$E_{S'} := \left\{ \left(\bigvee_{c \in \{\bullet, \circ, \diamond\}} p_{s,c} \right) \wedge \bigwedge_{c, c' \in \{\bullet, \circ, \diamond\}, c \neq c'} (p_{s,c} \rightarrow \neg p_{s,c'}) \mid s \in S' \right\} \\ \left\{ \bigwedge_{c \in \{\bullet, \circ, \diamond\}} (p_{s,c} \rightarrow \neg p_{t,c}) \mid s, t \in S' \text{ et } (s, t) \in A \right\}.$$

On a :

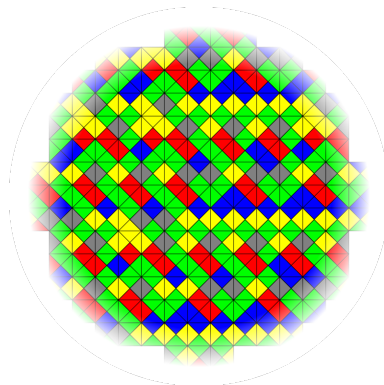
Lemme 44 $G|_{S'}$ est 3-coloriable ssi $E_{S'}$ est satisfiable.

Soit E' une partie finie de E_S . Il existe $S' \subseteq S$, S' fini, tel que $E' \subseteq E_{S'}$. Comme $G_{S'}$ est un graphe fini, il est 3-coloriable, et donc par le lemme 44, $E_{S'}$ est satisfiable. Comme $E' \subseteq E_{S'}$, E' est satisfiable.

D'après le **théorème de compacité de la logique propositionnelle**, E_S est satisfiable. D'après le lemme 44, $G = G|_S$ est 3-coloriable. ■



Corollaire 45 *Le plan est pavable par un ensemble de type de tuiles T si et seulement si tout carré fini est pavable par T .*



Deuxième partie

Logique des prédicats du premier ordre

Chapitre 5

Syntaxe et sémantique

Points du programme de l'agrégation

Logique du premier ordre : aspects syntaxiques. Langages, termes, formules. Variables libres et variables liées.
Logique du premier ordre : aspects sémantiques. Interprétation d'une formule dans un modèle. Validité, satisfiabilité.

But : écrire des propriétés et raisonner sur des structures

(base de données, groupes, arithmétiques, etc.).

5.1 Modèles

Définition 46 (signature)

Une **signature** Σ est un ensemble de symboles de fonctions et un ensemble de prédicats, munis de leurs arités.

Définition 47 (structure)

Une Σ -**structure** (ou Σ -modèle) est la donnée $\mathcal{M} = \langle D, \cdot^{\mathcal{M}} \rangle$ où :

- D est un ensemble non-vide appelé **domaine** ;
- $\cdot^{\mathcal{M}}$ est une fonction appelée **interprétation** qui :
 - à tout symbole de fonction f d'arité n dans Σ associe une fonction $f^{\mathcal{M}} : D^n \rightarrow D$;
 - à tout symbole de prédicat p d'arité n dans Σ associe une fonction $p^{\mathcal{M}} : D^n \rightarrow \{0, 1\}$.

Soit \mathcal{V} un ensemble dénombrable de **variables**.

Définition 48 (assignation)

Etant donnée une Σ -structure $\mathcal{M} = (D, \cdot^{\mathcal{M}})$, une **assignation** des variables v est une fonction de \mathcal{V} dans D .

5.2 Langage

5.2.1 Syntaxe

Définition 49 (terme)

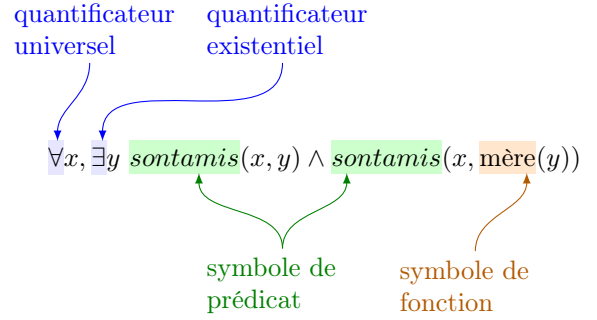
L'ensemble des Σ -termes est défini par induction :

- Une variable x de \mathcal{V} est un Σ -terme ;
- Pour tout symbole de fonction f d'arité n de Σ , et pour tous Σ -termes t_1, \dots, t_n ,
- $f(t_1, \dots, t_n)$ est un Σ -terme.

Définition 50 (formule)

L'ensemble des Σ -formules est défini par induction :

- Pour tout symbole de prédicat p d'arité n de Σ , et pour tous Σ -termes t_1, \dots, t_n ,
- $p(t_1, \dots, t_n)$ est une Σ -formule ;
- Pour toute Σ -formule φ ,
- $\neg\varphi$ est une Σ -formule ;
- Pour toutes formules φ et ψ ,
- $(\varphi \vee \psi)$ est une Σ -formule ;
- $(\varphi \wedge \psi)$ est une Σ -formule ;
- Pour toute variable x , toute Σ -formule φ ,
- $\forall x\varphi$ est une Σ -formule ;
- $\exists x\varphi$ est une Σ -formule.



Définition 51 (formule atomique)

Une **formule atomique** est une formule de la forme $p(t_1, \dots, t_n)$.

5.2.2 Sémantique

On va définir $\mathcal{M}, v \models \varphi$ qui signifie la Σ -formule φ est vraie dans \mathcal{M} avec l'assignation des variables v .

Définition 52 (assignation étendue aux termes)

D'abord, on étend v en $v^{\mathcal{M}}$ aux termes avec :

- $v^{\mathcal{M}}(x) = v(x)$;
- $v^{\mathcal{M}}(f(t_1, \dots, t_n)) = f^{\mathcal{M}}(v^{\mathcal{M}}(t_1), \dots, v^{\mathcal{M}}(t_n))$.

Définition 53 (Conditions de vérité)

- $\mathcal{M}, v \models p(t_1, \dots, t_n)$ si $p^{\mathcal{M}}(v^{\mathcal{M}}(t_1), \dots, v^{\mathcal{M}}(t_n)) = 1$;
- $\mathcal{M}, v \models \neg\varphi$ si $\mathcal{M}, v \not\models \varphi$;
- $\mathcal{M}, v \models (\varphi \vee \psi)$ si $\mathcal{M}, v \models \varphi$ ou $\mathcal{M}, v \models \psi$;
- $\mathcal{M}, v \models (\varphi \wedge \psi)$ si $\mathcal{M}, v \models \varphi$ et $\mathcal{M}, v \models \psi$;
- $\mathcal{M}, v \models \exists x\varphi$ s'il existe $d \in D$ tel que $\mathcal{M}, v[x := d] \models \varphi$.
- $\mathcal{M}, v \models \forall x\varphi$ si pour tout $d \in D$ on a $\mathcal{M}, v[x := d] \models \varphi$.

Remarque 54 Dans le contexte de la logique du premier ordre égalitaire, le symbole de prédicats = est interprété par l'égalité :

- $\mathcal{M}, v \models t = t'$ si $v(t) = v(t')$.

5.3 Variables libres/liées

Définition 55 (occurrence libre)

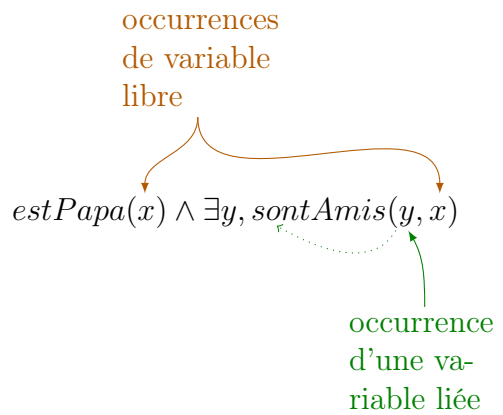
Une occurrence d'une variable x est libre si elle n'est pas sous la portée d'un quantificateur.

Définition 56 (occurrence liée)

Une occurrence est liée si elle n'est pas libre.

Définition 57 (variable libre)

x est une variable libre dans φ s'il existe une occurrence libre de x dans φ .



Notation 58 On note $\varphi(x_1, \dots, x_n)$ pour dire que les variables libres de φ sont dans $\{x_1, \dots, x_n\}$.

Définition 59 (terme clos)

Un terme est **clos** s'il est sans variables libres.

Définition 60 (formule close)

Une formule est **close** si elle est sans variables libres.

Définition 61 (clôture universelle)

La **clôture universelle** de $\varphi(x_1, \dots, x_n)$ est la formule $\forall x_1 \dots \forall x_n \varphi$.

Notation 62 Si φ est close, $\mathcal{M}, v \models \varphi$ ne dépend pas de v . On note alors $\mathcal{M} \models \varphi$.

5.4 Satisfiable, valide, conséquence sémantique

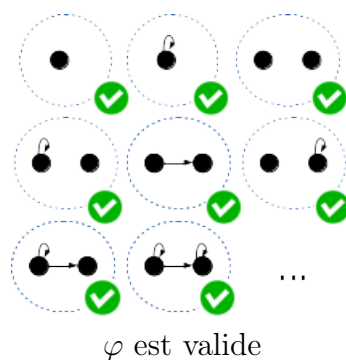
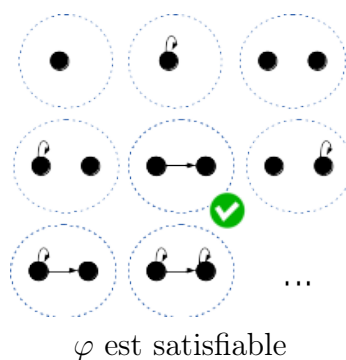
On ne s'intéresse qu'aux formules closes ([BA12], p. 138).

Définition 63 (satisfiable)

Une formule φ close est **satisfiable** s'il existe un modèle \mathcal{M} telle que $\mathcal{M} \models \varphi$.

Définition 64 (valide)

Une formule φ close est **valide** (ou est une tautologie) si pour tout modèle \mathcal{M} , on a $\mathcal{M} \models \varphi$.



5.5 Model checking

Définition 65 (problème de model checking en logique du premier ordre)

Le problème de model checking est :

- Entrée : un modèle fini \mathcal{M} , une formule close φ ;
- Sortie : oui si $\mathcal{M} \models \varphi$, non sinon.

Proposition 66 *Le problème du model checking en logique du premier ordre est PSPACE-complet.*

5.6 Problème de la satisfiabilité et problème de la validité

Définition 67 (problème de la satisfiabilité)

Le problème de la satisfiabilité est :

- Entrée : une formule close φ ;
- Sortie : oui si φ est satisfiable, non sinon.

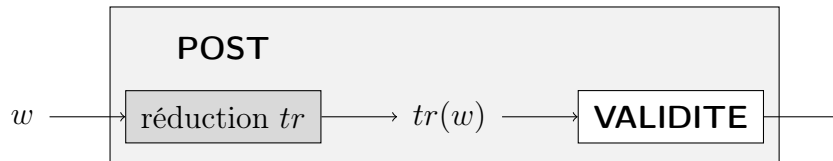
Définition 68 (problème de la validité)

Le problème de la validité est :

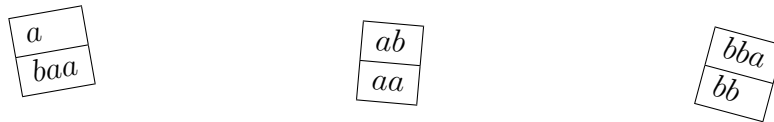
- Entrée : une formule close φ ;
- Sortie : oui si φ est valide, non sinon.

Proposition 69 ([GLM01], p. 205) *Le problème de la satisfiabilité et le problème de la validité en logique du premier ordre sont indécidables.*

IDÉE DE LA DÉMONSTRATION.



Considérons une instance w **POST** ne contenant pas de tuile $\begin{array}{|c|} \hline \epsilon \\ \hline \epsilon \\ \hline \end{array}$:



On construit la formule $tr(w) = (\varphi \rightarrow \psi)$ où :

- φ est la conjonction de
 - $p(\epsilon, \epsilon)$ où ϵ est un symbole de constante ;
 - $\forall x, y, p(x, y) \rightarrow p(u_i(x), v_i(y))$ pour toute tuile $\begin{array}{|c|} \hline u_i \\ \hline v_i \\ \hline \end{array}$ où, si $m = a_1 \dots a_n$ est un mot, on note $m(\cdot) = a_n(\dots a_1(\cdot) \dots)$;
- $\psi := \exists x, p(a(x), a(x)) \vee p(b(x), b(x))$.

On a :

- $tr(w)$ est calculable à partir de w ;
- w est une instance positive de **POST** ssi $tr(w)$ est valide.

■

Chapitre 6

Théories

Points du programme de l'agrégation

Théories cohérentes, théories complètes. Théories décidables, indécidables. Exemples de théories : égalité, arithmétique de Peano.

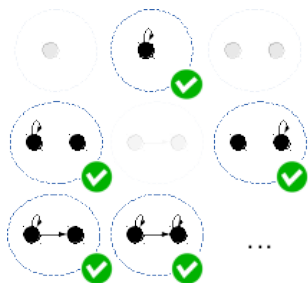
6.1 Définitions

Définition 70 (Théorie)

Une **théorie** T est un ensemble de formules closes.

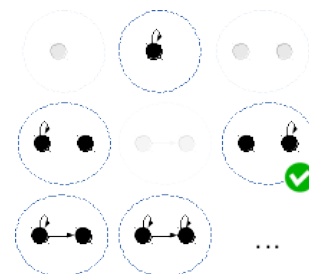
Définition 71 (T -valide¹)

φ close est **T -valide**, noté $T \models \varphi$, si pour tout modèle \mathcal{M} , on a $\mathcal{M} \models T$ implique $\mathcal{M} \models \varphi$.



Définition 72 (T -satisfiable)

Une formule φ est **T -satisfiable** s'il existe un modèle \mathcal{M} tel que $\mathcal{M} \models T$ et $\mathcal{M} \models \varphi$.



Le problème de la T -validité est :

- Entrée : une formule close φ ;
- Sortie : oui si φ est T -valide, non sinon.

Le problème de la T -satisfiabilité est :

- Entrée : une formule close φ ;
- Sortie : oui si φ est T -satisfiable, non sinon.

Définition 73 (théorie décidable)

Une théorie T est **décidable** si le problème de T -validité est décidable.

ou de manière équivalente le problème de T -satisfiabilité est décidable.

Définition 74 (théorie cohérente)

Une théorie T est **cohérente** si elle est satisfiable.

Définition 75 (théorie (sémantiquement) complète)

Une théorie T est **(sémantiquement) complète**

si pour toute formule φ , on a $T \models \varphi$ ou $T \models \neg\varphi$.

1. Ou conséquence sémantique de T .

6.2 Exemples de théories

6.2.1 Théorie de l'égalité

$$T_{eq} \begin{cases} \forall x, x = x \\ \forall x, y, (x = y) \rightarrow (y = x) \\ \forall x, y, z, (x = y \wedge y = z) \rightarrow x = z \\ \forall x_1, \dots, x_n, y_1, \dots, y_n, (\bigwedge_i (x_i = y_i)) \rightarrow f(\vec{x}) = f(\vec{y}) \\ \quad \text{pour tout symbole de fonction } f \text{ d'arité } n \\ \forall x_1, \dots, x_n, y_1, \dots, y_n, (\bigwedge_i (x_i = y_i)) \rightarrow (p(\vec{x}) \leftrightarrow p(\vec{y})) \\ \quad \text{pour tout symbole de prédicat } p \text{ d'arité } n \end{cases}$$

Proposition 76 *Si φ est T_{eq} -satisfiable ssi φ est satisfiable dans un modèle où le symbole $=$ est interprété par l'égalité.*

IDÉE DE LA DÉMONSTRATION.

(\Leftarrow) Soit \mathcal{M} un modèle où le symbole $=$ est interprété par l'égalité tel que $\mathcal{M} \models \varphi$. Par ailleurs, on peut montrer que $\mathcal{M} \models T_{eq}$, donc φ est T_{eq} -satisfiable.

(\Rightarrow) Soit $\mathcal{M} = (D, \cdot^{\mathcal{M}})$ un modèle tel que $\mathcal{M} \models T_{eq}$ et $\mathcal{M} \models \varphi$. Comme $\mathcal{M} \models \forall x, x = x$, $\mathcal{M} \models \forall x, y, (x = y) \rightarrow (y = x)$ et $\mathcal{M} \models \forall x, y, z, (x = y \wedge y = z) \rightarrow x = z$, la relation $=^{\mathcal{M}}$ est une relation d'équivalence.

Soit $\mathcal{M}' = (D', \cdot^{\mathcal{M}'})$ tel que

1. $D' = D / =^{\mathcal{M}}$;
2. Pour tout symbole de fonction f d'arité n ,

$$\begin{aligned} f^{\mathcal{M}'} : D'^n &\rightarrow D' \\ ([t_1], \dots, [t_n]) &\mapsto [f^{\mathcal{M}}(t_1, \dots, t_n)] \end{aligned}$$

3. Pour tout symbole de prédicat p d'arité n ,

$$\begin{aligned} p^{\mathcal{M}'} : D'^n &\rightarrow \{0, 1\} \\ ([t_1], \dots, [t_n]) &\mapsto p^{\mathcal{M}}(t_1, \dots, t_n) \end{aligned}$$

$f^{\mathcal{M}'}$ est bien définie car $\mathcal{M} \models \forall x_1, \dots, x_n, y_1, \dots, y_n, (\bigwedge_i (x_i = y_i)) \rightarrow f(\vec{x}) = f(\vec{y})$.

$p^{\mathcal{M}'}$ est bien définie car $\mathcal{M} \models \forall x_1, \dots, x_n, y_1, \dots, y_n, (\bigwedge_i (x_i = y_i)) \rightarrow (p(\vec{x}) \leftrightarrow p(\vec{y}))$.

Enfin, on démontre que pour toute formule ψ ,

$$\mathcal{P}(\psi) : \mathcal{M}, v \models \psi \text{ ssi } \mathcal{M}', v' \models \psi$$

où $v'(x) = [v(x)]$.

■

6.2.2 Théorie des groupes ([Lal90], p. 139) ([DNRC01], p. 105)

$$T_{groupes} \begin{cases} \text{Théorie de l'égalité} \\ \forall x, (x \times e = x) \\ \forall x, x \times x^{-1} = e \\ \forall x, y, z, ((x \times y) \times z) = (x \times (y \times z)) \end{cases}$$

Proposition 77 $T_{groupes} \models \varphi$ ssi pour tout groupe (G, \cdot) , on a $(G, \cdot) \models \varphi$.

6.2.3 Théorie des ordres denses ([DNRC01], p. 130)

$$T_O \left\{ \begin{array}{l} \text{Théorie de l'égalité} \\ \forall x, y, \neg(x < y \wedge y < x) \\ \forall x, y, z, ((x < y \wedge y < z) \rightarrow x < z) \\ \forall x, y, (x < y \vee x = y \vee y < x) \\ \forall x, y, \exists z, (x < y \rightarrow (x < z \wedge z < y)) \\ \forall x, \exists y, (x < y) \\ \forall x, \exists y, (y < x) \end{array} \right.$$

Proposition 78 $T_O \models \varphi$ ssi $(\mathbb{Q}, =, <) \models \varphi$ ssi $(\mathbb{R}, =, <) \models \varphi$.

6.2.4 Théorie des corps clos ([DNRC01], p. 133)

$$T_{CC} \left\{ \begin{array}{l} \text{Théorie de l'égalité} \\ \forall x, y, z, (x + y) + z = x + (y + z) \\ \forall x, y, x + y = y + x \\ \forall x, x + 0 = x \\ \forall x, x + (-x) = 0 \\ \forall x, y, z, (x \times y) \times z = x \times (y \times z) \\ \forall x, y, x \times y = y \times x \\ \forall x, x \times 1 = x \\ \forall x, (x \neq 0) \rightarrow \exists y, x \times y = 1 \\ \forall x, y, z, x \times (y + z) = x \times y + x \times z \\ 0 \neq 1 \\ \forall x, y, (x \leq y \wedge y \leq x) \rightarrow x = y \\ \forall x, y, z, (x \leq y \wedge y \leq z) \rightarrow x \leq z \\ \forall x, y, (x \leq y) \vee (y \leq x) \\ \forall x, y, z, x \leq y \rightarrow (x + z \leq y + z) \\ \forall x, y, (x \leq 0 \wedge y \leq 0) \rightarrow x \times y \leq 0 \\ \forall x \exists y, (x = y \times y) \vee (x = -y \times y) \\ \forall x_0, \dots, x_{n-1}, \exists y, y^n + x_{n-1}y^{n-1} + \dots + x_1y + x_0 = 0 \text{ pour tout nombre impair } n \end{array} \right.$$

Proposition 79 $T_{CC} \models \varphi$ ssi $(\mathbb{R}, =, 0, 1, +, \times) \models \varphi$.

6.2.5 Arithmétique de Presburger ([DNRC01], p. 136)

$$T_{Pres} \left\{ \begin{array}{l} \text{Théorie de l'égalité} \\ \forall x, x+1 \neq 0 \\ \forall x, (x = 0) \vee \exists y, x = y+1 \\ \forall x, y, x+1 = y+1 \rightarrow x = y \\ \forall x, x + 0 = x \\ \forall x, y, x + (y+1) = (x + y) + 1 \\ ((\varphi(0) \wedge (\forall y, \varphi(y) \rightarrow \varphi(y+1))) \rightarrow \forall x, \varphi(x)) \text{ pour toute formule } \varphi(x) \end{array} \right.$$

Proposition 80 $T_{Pres} \models \varphi$ ssi $(\mathbb{N}, =, 0, 1, +) \models \varphi$.

6.2.6 Arithmétique de Peano ([DNRC01], p. 111)

$$PA \left\{ \begin{array}{l} \text{Arithmétique de Presburger} \\ \forall x, x \times 0 = x \\ \forall x, y, x \times (y+1) = (x \times y) + x \end{array} \right.$$

Proposition 81 $PA \models \varphi$ implique $(\mathbb{N}, =, 0, 1, +, \times) \models \varphi$.

6.2.7 Arithmétique vraie sur \mathbb{N}

Soit $\Sigma = \{0, 1, +, \times\}$.

$T_{\mathbb{N}} = \{\varphi \mid \varphi \text{ est une } \Sigma\text{-formule et } (\mathbb{N}, =, 0, 1, +, \times) \models \varphi\}$.

Proposition 82 $T_{\mathbb{N}} \models \varphi$ ssi $(\mathbb{N}, =, 0, 1, +, \times) \models \varphi$.

6.3 Résultats

	Théorie com- plète?	SAT	SAT d'une formule existentielle	SAT d'une conjonction existentielle
\emptyset	✗	indéc, dans co-RE	?	?
Théorie de l'égalité	✗	indéc, dans co-RE	?	?
Théorie de l'égalité (avec que des symboles de fonction)	✗	indéc [??]	NP-complet	dans P [KS08]
Théorie de l'égalité (sans autres symboles de fonction et symboles de prédicats) ([DNRC01], p. 132)	✗	PSPACE-complet [SM73]	NP-complet	dans P [KS08]
Théorie des ordres denses ([DNRC01], p. 130) ([Har09], p. 333)	✓	PSPACE-complet	NP-complet	dans P
Théorie des corps clos ([DNRC01], p. 133)	✓	dans EXPSPACE [BOKR86], PSPACE-dur	NP-dur dans PSPACE [Can88]	?
Arithmétique linéaire sur \mathbb{R}	✓		NP-complet	dans P
Arithmétique linéaire sur \mathbb{N} (de Presburger) ([DNRC01], p. 136) ([Har09], p. 336) ([Car08])	✓	dans 3EXPTIME [Opp78], 2EXPTIME-dur [FFR74]	NP-complet	NP-complet
Arithmétique de Robinson ([CL93], p. 73)	✗	indéc, dans co-RE	?	?
Arithmétique de Peano ([DNRC01], p. 123)	✗	indéc, dans co-RE	indéc [?]	indéc [?]
Arithmétique sur \mathbb{N} (théorie non récursive)	✓	indéc, ni dans RE, ni dans co-RE	indéc, dans RE	indéc[Mat03], dans RE

Chapitre 7

Déduction naturelle

Points du programme de l'agrégation

... substitutions, capture de variables.

Logique du premier ordre : systèmes formels de preuve. Déduction naturelle. Théorème de complétude du calcul des prédicats du premier ordre.

7.1 Substitution

Définition 83 (substitution ([BA12], p. 187))

Une **substitution** est un ensemble de la forme

$$[x_1 := t_1, \dots, x_n := t_n]$$

où chaque x_i est une variable et chaque t_i est un terme.

Définition 84 (instantiation)

La formule $\varphi[x_1 := t_1, \dots, x_n := t_n]$ est la formule φ dans laquelle on a remplacé simultanément les occurrences libres x_i par le terme t_i .

Attention, on autorise uniquement les **substitutions licites**. Par exemple

$$\underbrace{(\forall x, x < y)}_{\varphi}[y := \overbrace{x-1}^t] = \forall x, x < x-1 \quad \times$$

n'est pas licite. On parle de **capture de variables**. Sans perte de généralité, on renomme les variables liées de φ par des variables fraîches afin qu'elles n'apparaissent pas dans t ([DNRC01], p. 20-22) :

$$(\forall x', x' < y)[y := x-1] = \forall x', x' < x-1 \quad \checkmark$$

7.2 Règles de la déduction naturelle ([DNRC01], p. 25)

Définition 85 (séquent en déduction naturelle ([DNRC01], p. 24))

Un **séquent** est un couple (Γ, φ) où Γ est un ensemble fini de formules et φ une formule. Il se note $\Gamma \vdash \varphi$ et se lit « à partir des hypothèses Γ , j'ai prouvé la formule φ ».

Définition 86 (règles de la déduction naturelle)

Les **règles de la déduction naturelle** sont données ci-dessous :

$$\text{axiome} \frac{}{\Gamma, A \vdash A} \quad \text{affaiblissement} \frac{\Gamma \vdash A}{\Gamma, B \vdash A} \quad \text{absurde} \frac{\Gamma, \neg A \vdash \perp}{\Gamma \vdash A}$$

	Règles d'introduction	Règles d'élimination
\rightarrow	$\frac{\Gamma, A \vdash B}{\Gamma \vdash (A \rightarrow B)}$	$\frac{\Gamma \vdash A \quad \Gamma \vdash (A \rightarrow B)}{\Gamma \vdash B}$
\wedge	$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash (A \wedge B)}$	$\frac{\Gamma \vdash (A \wedge B)}{\Gamma \vdash A} \quad \frac{\Gamma \vdash (A \wedge B)}{\Gamma \vdash B}$
\vee	$\frac{\Gamma \vdash A}{\Gamma \vdash (A \vee B)} \quad \frac{\Gamma \vdash B}{\Gamma \vdash (A \vee B)}$	$\frac{\Gamma \vdash (A \vee B) \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}$
\neg	$\frac{\Gamma, A \vdash \perp}{\Gamma \vdash \neg A}$	$\frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash \perp}$
\exists	$\frac{\Gamma \vdash A[x := t]}{\Gamma \vdash \exists x A}$	$\frac{\Gamma \vdash \exists x A \quad \Gamma, A \vdash C}{\Gamma \vdash C}$ où x non libre dans Γ, C
\forall	$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x A}$ où x non libre dans Γ	$\frac{\Gamma \vdash \forall x A(x)}{\Gamma \vdash A[x := t]}$
$=$	$\frac{}{\Gamma \vdash (t = t)}$	$\frac{\Gamma \vdash \varphi(x := t) \quad \Gamma \vdash (t = u)}{\Gamma \vdash \varphi(x := u)}$

Exemple 87 (règle d'introduction du \forall)

$$\frac{p(x) \vdash p(x)}{p(x) \vdash \forall x, p(x)} \quad \text{!}$$

$$\frac{\vdash p(x)}{\vdash \forall x, p(x)} \quad \checkmark$$

Exemple 88 (règle d'élimination du \exists)

$$\frac{p(x) \vdash \exists x, q(x) \quad p(x), q(x) \vdash r(x)}{p(x) \vdash r(x)} \quad \text{!}$$

$$\frac{\vdash \exists x, p(x) \quad p(x) \vdash q}{\vdash q} \quad \checkmark$$

7.3 Arbres de preuve

Définition 89 (arbre de preuve en déduction naturelle)

Une (arbre de) preuve (en déduction naturelle) de $\Gamma \vdash \varphi$ est un arbre fini tel que :

- La racine est $\Gamma \vdash \varphi$;
- Chaque nœud correspond à l'application d'une des règles de la déduction naturelle.

Définition 90 (existence d'un arbre de preuve ([DNRC01], p. 80))

Soit T une théorie. Soit φ une formule close. On note $T \vdash_{DN} \varphi$ s'il¹ existe un arbre de preuve de $\Gamma \vdash \varphi$ avec Γ fini et $\Gamma \subseteq T$.

Définition 91 (théorie consistante)

Soit T une théorie. T est **consistante** si $T \not\vdash_{DN} \perp$.

Définition 92 (théorie syntaxiquement complète)

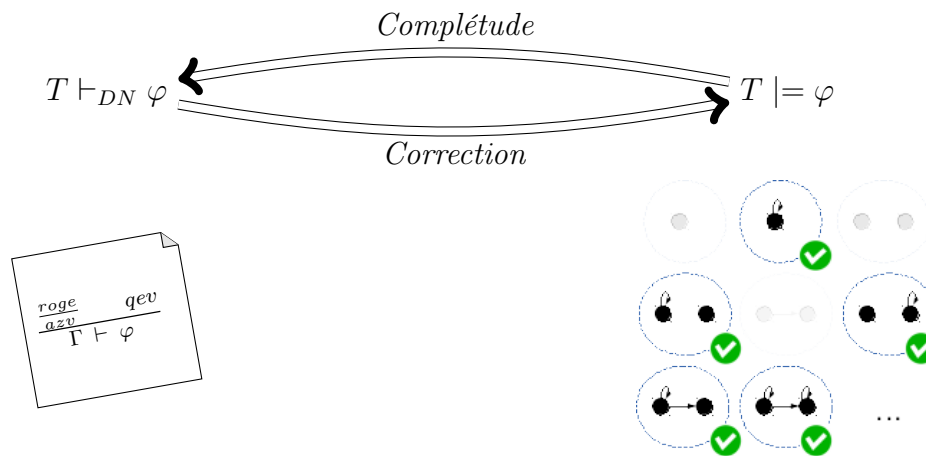
Soit T une théorie. T est **syntaxiquement complète** si pour toute formule close φ , $T \vdash_{DN} \varphi$ ou $T \vdash_{DN} \neg\varphi$.

1. Certains livres surchargent la notation et écrivent \vdash .

7.4 Correction et complétude

7.4.1 Énoncé

Théorème 93 Soit T un ensemble de formules closes et φ une formule close.



IDÉE DE LA DÉMONSTRATION.

⇒ On démontre, par induction sur π , que pour tout arbre de preuve π , on a

$\mathcal{P}(\pi)$: Si π est une preuve de $\Gamma \vdash \varphi$, alors pour tout modèle \mathcal{M} , pour tout assignation v , $\mathcal{M}, v \models \Gamma$ implique que $\mathcal{M}, v \models \varphi$.

⇐

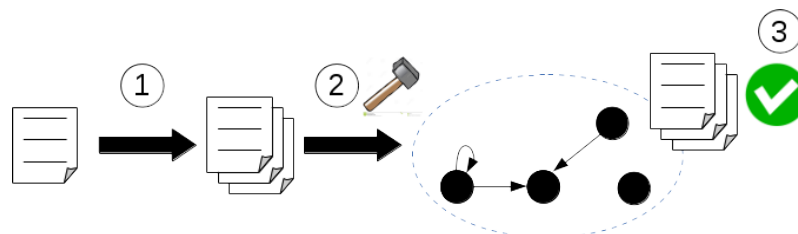
$T \models \varphi$	ssi	$T \cup \{\neg\varphi\}$ insatisfiable	
	implique	$T \cup \{\neg\varphi\}$ inconsistante	(par le lemme 94
	ssi	$T \vdash_{DN} \varphi$	

■

7.4.2 Idée de la démonstration

Lemme 94 ([DNRC01], p. 83) Δ est consistante alors Δ est satisfiable.

IDÉE DE LA DÉMONSTRATION.



- On étend Δ en Δ' tel que :
 - Pour toute formule $\psi(x)$, on introduit un symbole de constante c_ψ tel que

$$\Delta' \vdash_{DN} (\exists x \psi(x) \rightarrow \psi(c_\psi)).$$

Un tel c_ψ s'appelle un **témoin de Henkin**.

- Δ' soit une théorie syntaxiquement complète.

2. On construit le modèle \mathcal{M} :
- Le domaine D est l'ensemble des termes clos² ;
 - Si f est un symbole de fonction d'arité n ,

$$f^{\mathcal{M}} : D^n \rightarrow D$$

$$([t_1], \dots, [t_n]) \mapsto [f(t_1, \dots, t_n)]$$

- Si p est un symbole de prédicats n -aire,

$$p^{\mathcal{M}} : D^n \rightarrow \{0, 1\}$$

$$([t_1], \dots, [t_n]) \mapsto 1 \text{ si } \Delta' \vdash_{DN} p(t_1, \dots, t_n)$$

$$\mapsto 0 \text{ sinon.}$$

3. On montre :

Lemme 95 (lemme de la vérité)

Soit $\varphi(x_1, \dots, x_n)$ une formule et t_1, \dots, t_n des termes clos. On a :

$$\mathcal{M}[x_1 := [t_1], \dots, x_n := [t_n]] \models \varphi \text{ ssi } \Delta' \vdash_{DN} \varphi(t_1, \dots, t_n)$$

■

7.5 Conséquences

7.5.1 Problème de validité dans RE

Théorème 96 *Le problème de validité en logique du premier ordre est dans RE.*

IDÉE DE LA DÉMONSTRATION.

Voici une machine qui accepte le langage des formules valides :

```

procédure valide( $\varphi$ )
  pour toute preuve  $\pi$ 
  |   si  $\pi$  est une preuve de  $\vdash \varphi$  alors
  |   |   accepter

```

■

Théorème 97 *Si $T \in RE$, le problème de T -validité en logique du premier ordre est dans RE.*

IDÉE DE LA DÉMONSTRATION.

Soit ψ_1, ψ_2, \dots une énumération effective de T . Voici une machine qui accepte le langage des formules T -valides :

```

procédure Tvalide( $\varphi$ )
  pour tout  $n = 0, 1, \dots$ 
  |   Énumérer les formules  $\psi_1, \dots, \psi_n$ 
  |   pour toute preuve  $\pi$  de longueur au plus  $n$ 
  |   |   si  $\pi$  est une preuve de  $\{\psi_1, \dots, \psi_n\} \vdash \varphi$  alors
  |   |   |   accepter

```

■

2. Certaines personnes ([DNRC01], p. 83) quotientent l'ensemble des termes clos avec la relation d'équivalence \sim défini par $t \sim t'$ ssi $\Delta' \vdash (t = t')$ car le symbole de prédicat $=$ s'interprète par l'égalité. Aussi ils ont rajouté les règles correspondantes à $=$.

7.5.2 Théorème de compacité

Théorème 98 (Compacité de la logique du premier ordre ([DNRC01], p. 86))

Soit T un ensemble de formules closes.

Si toute partie finie de T est satisfiable alors T satisfiable.

IDÉE DE LA DÉMONSTRATION.

Par contraposée.

T insatisfiable **implique** T inconsistante (par le lemme 94)
 implique il existe une preuve de $\Gamma \vdash \perp$ avec Γ fini et $\Gamma \subseteq T$
 implique il existe Γ fini et $\Gamma \subseteq T$ et Γ insatisfiable (par correction).

■

Corollaire 99 *Il n'existe pas de formule φ de la logique du premier ordre tel que*

$$\mathcal{M} \models \varphi \text{ ssi le domaine de } \mathcal{M} \text{ est fini.}$$

IDÉE DE LA DÉMONSTRATION.

Par l'absurde. Soit φ une telle formule et posons

$$T = \{\varphi\} \cup \bigcup_{n \in \mathbb{N}} \{\exists x_1 \dots x_n, \bigwedge_{i,j \in \{1, \dots, n\}, i \neq j} x_i \neq x_j\}.$$

Toute partie finie de T est satisfiable mais T est insatisfiable.

Contradiction avec le théorème de compacité. ■

Corollaire 100 (modèle non-standard de l'arithmétique vraie)

$T_{\mathbb{N}} = \{\varphi \mid \varphi \text{ est une } \Sigma\text{-formule et } (\mathbb{N}, =, 0, 1, +, \times) \models \varphi\}$ admet un modèle non isomorphe³ à $(\mathbb{N}, =, 0, 1, +, \times)$.

IDÉE DE LA DÉMONSTRATION.

Soit c un symbole frais de constante. Soit $T = T_{\mathbb{N}} \cup \{i < c \mid i \in \mathbb{N}\}$. Toute partie finie de T est satisfiable. D'après le théorème de compacité, T est satisfiable. ■

7.5.3 Théorème de Lowenheim-Skolem

Théorème 101 (Lowenheim-Skolem ([DNRC01], p. 99) ([BA12], p. 228))

Si T est satisfiable dans un modèle infini alors T est satisfiable dans un modèle infini dénombrable.

IDÉE DE LA DÉMONSTRATION.

On pose $T' = T \cup \{c_i \neq c_j \mid i, j \in \mathbb{N}, i \neq j\}$ où c_0, c_1, \dots sont des nouveaux symboles de constante.

T' satisfiable implique T' consistante
 implique T' est satisfiable dans le modèle à l'étape 2
 de la démonstration du lemme 94.

■

Corollaire 102 (modèle dénombrable pour la théorie des corps-clos)

La théorie des corps clos admet un modèle infini dénombrable.

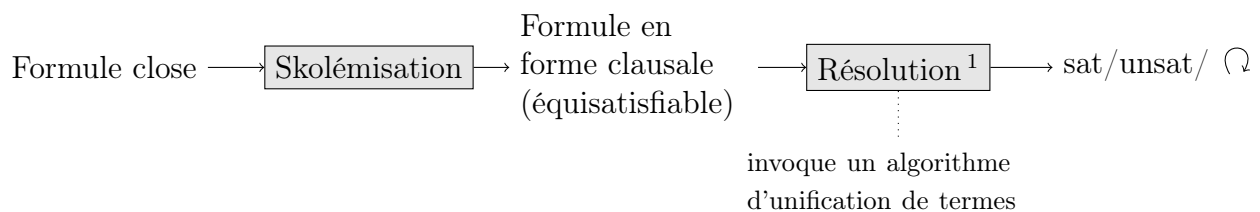
3. que l'on appelle non-standard.

Chapitre 8

Résolution en logique du premier ordre

Points du programme de l'agrégation

Algorithme d'unification des termes. Preuves par résolution.



8.1 Skolémisation ([BA12], p. 174)

Définition 103 (formule prénexe)

Une **formule prénexe** est une formule close de la forme $Q_1x_1 \dots Q_nx_n\psi$ où chaque Q_i est un quantificateur et ψ est sans quantificateur.

Définition 104 (forme normale prénexe universelle)

Une **forme prénexe universelle** est une formule close qui est de la forme $\forall_1x_1 \dots \forall_nx_n\psi$ où ψ est sans quantificateur.

Définition 105 (littéral)

Un **littéral** est une formule atomique ou la négation d'une formule atomique.

Définition 106 (forme normale conjonctive)

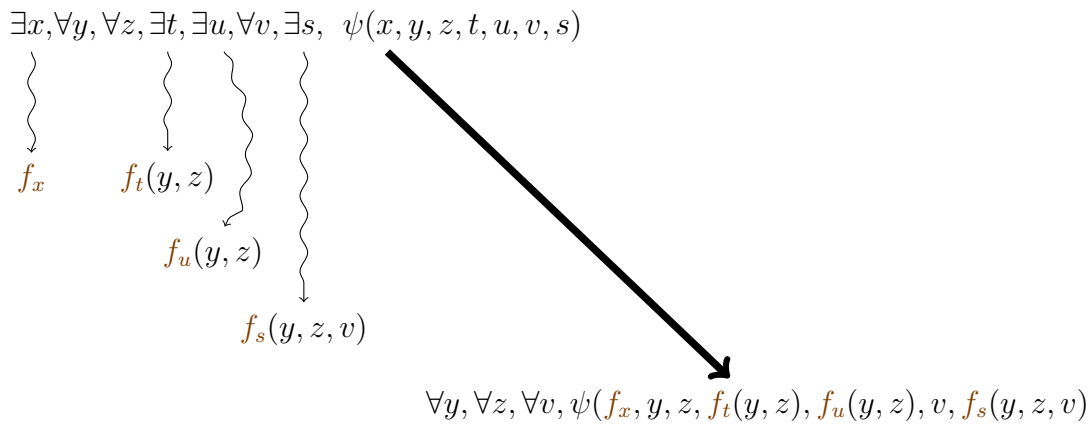
Par abus, on dit qu'une formule est une **forme normale conjonctive** si elle est de la forme $\forall x_1 \dots \forall x_n\psi$ où ψ est une formule sans quantificateur qui est une forme normale conjonctive, c'est-à-dire une conjonction de disjonctions de littéraux.

1. Attention, ce n'est pas un algorithme.

Définition 107 (fonctions de Skolem)

Soit φ une formule prénexe.

On appelle **fonction de Skolem** un symbole de fonction f_x d'arité n pour un quantificateur $\exists x$ qui dépend des n variables quantifiées universellement qui précède $\exists x$ dans φ .



Théorème 108 (de Skolem ([BA12], p. 172)) *Toute formule φ admet une forme normale conjonctive équisatisfiable.*

IDÉE DE LA DÉMONSTRATION.

1. Renommer les variables liées afin que chaque quantification porte sur une variable différente.
2. Éliminer les opérateurs booléens autre que \wedge et \vee
3. Mettre les négations à l'intérieur cf. loi de Morgan
4. Mettre en forme prénexe
5. Mettre la matrice en FNC
6. Introduire² des **fonctions de Skolem** pour chaque $\exists x$.

■

Exemple 109 ([BA12], p. 174)

$$[\forall x(p(x) \rightarrow q(x))] \rightarrow [(\forall x p(x)) \rightarrow (\forall x q(x))]$$

2. Étape qui fait que l'on obtient une formule équisatisfiable et pas forcément équivalente.

8.2 Résolution en logique du premier ordre

8.2.1 Unification ([LDR93], p. 86) ([BA12], p. 189)

Définition 110 (unificateur)

Soit $\{\psi_1, \dots, \psi_i\}$ un ensemble de formules atomiques. Un **unificateur** de $\{\psi_1, \dots, \psi_i\}$ est une substitution σ telle que $\psi_1\sigma = \dots = \psi_k\sigma$.

Définition 111 (unificateur principal)

Soit $\{\psi_1, \dots, \psi_i\}$ un ensemble de formules atomiques. Un **unificateur principal** (**most general unifier**) de $\{\psi_1, \dots, \psi_i\}$ est un unificateur de cet ensemble tel que pour tout unificateur α , il existe une substitution β telle que $\alpha = \sigma\beta$.

Exemple 112

$\sigma := [x := f(a), z := y]$ est un unificateur principal de $\{p(f(x), g(y)), p(f(f(a)), g(z))\}$.
 $\alpha := [x := f(a), y := f(g(a)), z := f(g(a))]$ en est un unificateur et s'écrit $\sigma[y := f(g(a))]$.

8.2.2 Règle de résolution ([DNRC01], p. 265)

Définition 113 (règle de résolution)

La règle de résolution en logique du premier ordre est

$$\text{res} \frac{(\psi \vee l_1 \vee \dots \vee l_n) \quad (\neg\psi' \vee l'_1 \vee \dots \vee l'_k)}{(l_1\sigma \vee \dots \vee l_n\sigma \vee l'_1\sigma \vee \dots \vee l'_k\sigma)}$$

où :

- $l_1, \dots, l_n, \dots, l'_1, \dots, l'_k$ sont des littéraux ;
- ψ, ψ' sont des formules atomiques ;
- les clauses $(\psi \vee l_1 \vee \dots \vee l_n)$ et $(\neg\psi' \vee l'_1 \vee \dots \vee l'_k)$ n'ont pas de variables communes ;
- ψ et ψ' sont unifiables et σ en est un unificateur principal.

8.2.3 Contraction ([DNRC01], p. 265)

Définition 114 (règle de contraction)

La règle de contraction est

$$\text{contr} \frac{(\psi \vee \psi' \vee l_1 \vee \dots \vee l_n)}{(\psi\sigma \vee l_1\sigma \vee \dots \vee l_n\sigma)}$$

où :

- L, L', l_1, \dots, l_n sont des littéraux ;
- ψ, ψ' sont des formules atomiques ;
- ψ et ψ' sont unifiables et σ en est un unificateur principal.

Remarque 115 Certains auteurs ([BA12], p. 196) ([LDR93], p. 93) présentent une seule règle de résolution qui fusionne la règle de résolution ci-dessus et la règle de contraction :

$$\text{super-res} \frac{(\psi_1 \vee \dots \vee \psi_i \vee l_1 \vee \dots \vee l_n) \quad (\neg\psi'_1 \vee \dots \vee \neg\psi'_j \vee l'_1 \vee \dots \vee l'_k)}{(l_1\sigma \vee \dots \vee l_n\sigma \vee l'_1\sigma \vee \dots \vee l'_k\sigma)}$$

si $\{\psi_1, \dots, \psi_i, \psi'_1, \dots, \psi'_j\}$ sont unifiables et où σ en est un unificateur principal.

8.3 Modèles de Herbrand

Définition 116 (modèles de Herbrand)

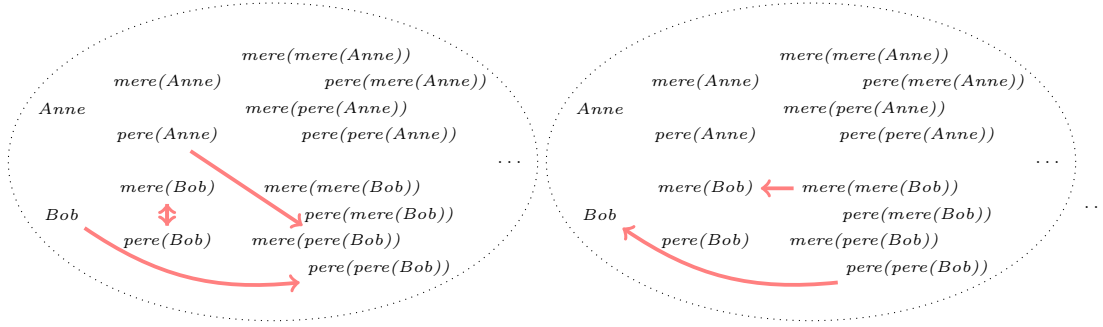
Un **modèle de Herbrand** est un modèle $\mathcal{H} = (D, \cdot^{\mathcal{H}})$ tel que :

- D = ensemble des termes clos ; (on suppose que l'on a toujours au moins un symbole de constante)
- Pour tout symbole de fonction f d'arité n , on a :

$$f^{\mathcal{H}} : D^n \rightarrow D$$

$$\vec{t} \mapsto f(\vec{t}).$$

Exemple 117 (quelques modèles de Herbrand)



Proposition 118 ([LDR93], p. 99) *Soit φ une formule en forme préfixe universelle.*

φ satisfiable ssi φ satisfiable dans un modèle de Herbrand.

IDÉE DE LA DÉMONSTRATION.

(\Leftarrow) Immédiat. (\Rightarrow) Soit \mathcal{M} un modèle tel que $\mathcal{M} \models \varphi$. On construit \mathcal{H} avec pour tout symbole de prédicat p d'arité n , on a :

$$p^{\mathcal{H}} : D^n \rightarrow \{0, 1\}$$

$$\vec{t} \mapsto \begin{cases} 1 & \text{si } \mathcal{M} \models p(\vec{t}) \\ 0 & \text{sinon} \end{cases}$$

On démontre alors, par induction sur toute formule sans quantificateur ψ , que la propriété suivante est vraie :

$$\mathcal{P}(\psi) : \mathcal{H}, [\vec{x} := \vec{t}] \models \psi \text{ ssi } \mathcal{M} \models \psi[\vec{x} := \vec{t}]$$

■

Définition 119 (théorie universelle)

Une théorie T est **universelle** si toutes les formules de T sont en forme préfixe universelle.

Notation 120 *Soit T une théorie universelle. On note $Inst(T)$ l'ensemble des instances des formules de T obtenues par substitution de termes clos.*

Théorème 121 ([LDR93], p. 99) *Soit T une théorie universelle.*

T est insatisfiable ssi il existe $T' \subseteq Inst(T)$, T' fini tel que T' insatisfiable en logique propositionnelle.

IDÉE DE LA DÉMONSTRATION.

(\Leftarrow) Immédiat.

(\Rightarrow)

T insatisfiable implique T n'a pas de modèle de Herbrand

implique $Inst(T)$ insatisfiable en logique prop.

implique qu'il existe $T' \subseteq Inst(T)$, T' fini, insatisfiable en logique prop.

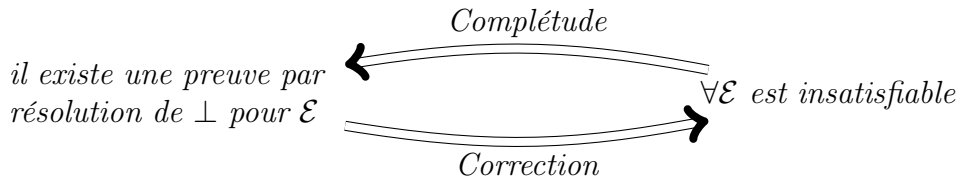
d'après le **théorème de compacité de la logique prop.**

■

8.4 Correction et complétude

Notation 122 (clotûre universelle) On note $\forall\varphi$ la clotûre universelle de φ .

Théorème 123 Soit \mathcal{E} une forme normale conjonctive.



IDÉE DE LA DÉMONSTRATION.

\Rightarrow ([CRK03], p. 270) ([BA12], p. 198) ([LDR93], p. 94-95)

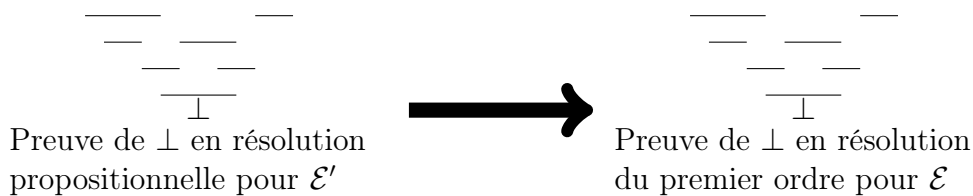
Par contraposée, soit $\mathcal{M} \models \forall\mathcal{E}$. La démonstration est similaire au cas propositionnel :

Lemme 124 si $\mathcal{M} \models \forall C_1$, $\mathcal{M} \models \forall C_2$ et $\text{res}\frac{C_1}{C} \frac{C_2}{C}$ alors $\mathcal{M} \models \forall C$.

Lemme 125 si $\mathcal{M} \models \forall C_1$ et $\text{contr}\frac{C_1}{C}$ alors $\mathcal{M} \models \forall C$.

\Leftarrow ([CRK03], p. 272) ([BA12], p. 199)

Supposons $\forall\mathcal{E}$ insatisfiable. D'après le théorème 121, il existe $\mathcal{E}' \subseteq \text{Inst}(\mathcal{E})$, \mathcal{E}' ensemble fini de clauses, insatisfiable en logique propositionnelle. Par **complétude de la résolution en logique propositionnelle**, il existe une preuve par résolution de \perp pour \mathcal{E}' en logique propositionnelle.



On démontre la propriété suivante par induction sur une preuve par résolution propositionnelle π' :

« Si π' est une preuve par résolution propositionnelle de C' pour \mathcal{E}'
 $\mathcal{P}(\pi')$: alors il existe une clause C , une preuve par résolution du premier
 ordre de C pour \mathcal{E} , une substitution σ tel que $C' = \sigma C$ ».

— Cas de base. Si $C' \in \mathcal{E}'$, alors par définition il existe $C \in \mathcal{E}$, σ tel que $C' = \sigma C$.

D'où $\mathcal{P}(C')$.

— Cas inductif. Supposons $\mathcal{P}(C'_1)$ et $\mathcal{P}(C'_2)$. On montre $\mathcal{P}(\text{res-prop}\frac{\overset{\cdot}{C}'_1}{C'} \frac{\overset{\cdot}{C}'_2}{C'})$ grâce à :

Lemme 126 Soit C_1 et C_2 deux clauses sans variables communes.

Soit σ_1 et σ_2 deux substitutions.

Si $\text{res-prop}\frac{\sigma_1 C_1}{C'} \frac{\sigma_2 C_2}{C'}$ alors il existe une substitution β et une clause C tel que

$\text{super-res}\frac{C_1}{C} \frac{C_2}{C}$ et $C' = \beta C$.

■

Chapitre 9

Calcul des séquents

Points du programme de l'agrégation
--

Calcul des séquents.

9.1 Motivation

- Règles du calcul des séquents plus symétriques que celles de la déduction naturelle ([DNRC01], p. 58).

éliminable
↓

- La créativité humaine est confinée dans les substitutions et la règle de coupure :
 - Propriété de la sous-formule. D'où la décidabilité de la logique propositionnelle ;
 - Calcul effectif d'un interpolant à partir d'un arbre de preuve ([DNRC01], p. 216).

9.2 Règles du calcul des séquents ([DNRC01], p. 187)

Définition 127 (séquent en calcul des séquents ([DNRC01], p. 186))

Un **séquent** est un couple (Γ, Δ) où Γ et Δ sont des multi-ensembles¹ finis de formules.

Il se note $\Gamma \vdash \Delta$ et se lit

« à partir de la conjonction des hypothèses Γ , j'ai prouvé la disjonction des formules de Δ ».

1. Il existe aussi des présentations avec des ensembles, cf. [BA12], p. 70.

Définition 128 (règles du calcul des séquents)

Les règles du calcul des séquents sont données ci-dessous :

$$\perp_g \frac{}{\perp \vdash} \quad \text{axiome} \frac{}{A \vdash A}$$

	Règles d'introduction à gauche	Règles d'introduction à droite
affaiblissement	$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}$	$\frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A}$
contraction	$\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}$	$\frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}$
\rightarrow	$\frac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, (A \rightarrow B) \vdash \Delta}$	$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash (A \rightarrow B), \Delta}$
\wedge	$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, (A \wedge B) \vdash \Delta}$	$\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash (A \wedge B), \Delta}$
\vee	$\frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, (A \vee B) \vdash \Delta}$	$\frac{\Gamma, \vdash \Delta, A, B}{\Gamma \vdash \Delta, (A \vee B)}$
\neg	$\frac{\Gamma \vdash \Delta, A}{\Gamma, \neg A \vdash \Delta}$	$\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}$
\exists	$\frac{\Gamma, A \vdash \Delta}{\Gamma, \exists x A \vdash \Delta}$ où x non libre dans Γ, Δ	$\frac{\Gamma \vdash A[x := t], \Delta}{\Gamma \vdash \exists x A, \Delta}$
\forall	$\frac{\Gamma, A[x := t] \vdash \Delta}{\Gamma, \forall x A \vdash \Delta}$	$\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash \forall x A, \Delta}$ où x non libre dans Γ, Δ

éliminable



$$\text{coupure} \frac{\Gamma \vdash A, \Delta \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

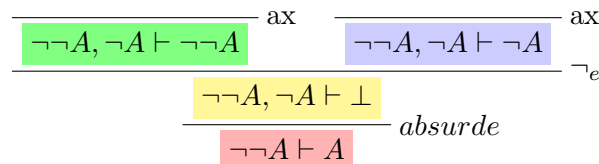
9.3 Correction et complétude

Théorème 129

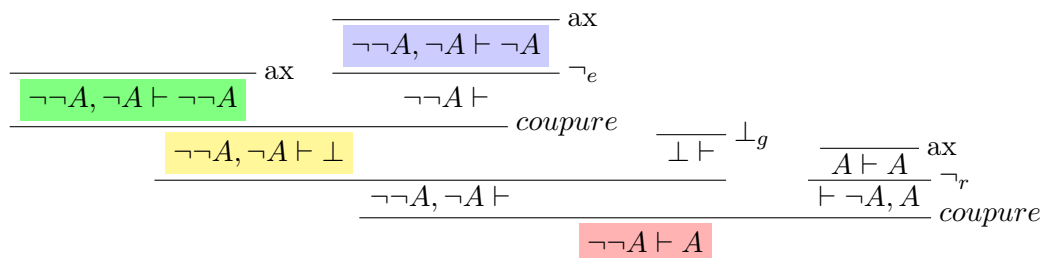
$\Gamma \vdash \varphi$ est prouvable
 en déduction naturelle *ssi* $\Gamma \vdash \varphi$ est prouvable
 en calcul des séquents.

IDÉE DE LA DÉMONSTRATION.

(\Rightarrow) ([DNRC01], p. 195) On transforme un arbre de preuve en déduction naturelle



en un arbre de preuve en calcul des séquents :



(\Leftarrow) On transforme un arbre de preuve du calcul des séquents en un arbre de la déduction naturelle ([DNRC01], p. 197).

■

9.4 Élimination de la règle de la coupure

Théorème 130

$\Gamma \vdash \varphi$ est prouvable
 en calcul des séquents *ssi* $\Gamma \vdash \varphi$ est prouvable
 en calcul des séquents
 sans utiliser la règle de la coupure.

IDÉE DE LA DÉMONSTRATION.

(\Leftarrow) Immédiat.
 (\Rightarrow) Voir ([DNRC01], p. 200-208)

■

Quizz sur la logique propositionnelle

Donner des exemples de formules satisfiables.	
Donner des exemples de formules insatisfiables.	
Donner des exemples de formules valides.	
Donner la complexité de SAT.	
Donner la complexité de VALIDE.	
Donner la complexité de HORN-SAT.	
Donner la complexité de 2-SAT.	
Donner la complexité de 3-SAT.	
Donner des exemples de formes normales conjonctives.	
Donner des exemples de formes normales disjonctives.	

Est-ce que $\exists x, p(x)$ et $p(c)$ sont des formules équivalentes ?	
Est-ce que $\exists x, p(x)$ est satisfiable ?	
Est-ce que $\exists x, p(x)$ est satisfiable dans un modèle fini ?	
Est-ce que $\exists x, p(x)$ est valide ?	
Décidabilité du model checking d'une formule de la logique du premier ordre dans un modèle fini ?	
Classe de la validité d'une formule de la logique du premier ordre ? (RE, co-RE)	
Classe de la satisfiabilité d'une formule de la logique du premier ordre ? (RE, co-RE)	
Classe de la validité d'une formule de la logique du premier ordre sur la classe des modèles finis ? (RE, co-RE)	
Classe de la satisfiabilité d'une formule de la logique du premier ordre dans un modèle fini ? (RE, co-RE)	
Est-ce que le théorème de compacité est toujours vrai si on remplace 'satisfiable' par 'satisfiable dans un modèle fini' ?	
Existe-t-il une formule φ tel que $\mathcal{M} \models \varphi$ implique que le domaine de \mathcal{M} est infini non dénombrable ?	
Donner un exemple de théorie indécidable.	
Donner un exemple de théorie décidable.	
Comment se lit le séquent $A, B \vdash C, D$ (en calcul des séquents) ?	

Indiquer s'il s'agit d'une formule, un terme ou une expression mal formée. Si c'est une formule, précisez si elle est atomique ou non. Précisez aussi si elle est close ou non. Si c'est un terme, précisez s'il est clos ou non.

Convention

	Notations
Variables	x, y, z , etc.
Symboles de constantes	c, d , etc., $0, 1$, etc.
Symboles de fonctions	f, g , etc. $+$, $-$, \times , etc.
Symboles de prédicats	p, q, r , etc.

x	
p	
$p(x)$	
$(x \vee y)$	
$1 + 1$	
$f(x)$	
$g(0, c)$	
$q(0, c)$	
$f(q(x))$	
$q(g(x), c)$	
$\forall x, x$	
$(q(g(x), c) \wedge p(x))$	
$p(x \vee f(0))$	
$\forall x, (q(g(x), c) \wedge p(x))$	

Bibliographie

- [BA12] Mordechai Ben-Ari. *Mathematical logic for computer science*. Springer Science & Business Media, 2012.
- [BOKR86] Michael Ben-Or, Dexter Kozen, and John Reif. The complexity of elementary algebra and geometry. *Journal of Computer and System Sciences*, 32(2) :251–264, 1986.
- [Can88] John Canny. Some algebraic and geometric computations in pspace. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 460–467. ACM, 1988.
- [Car08] Olivier Carton. *Langages formels, calculabilité et complexité*, volume 101. Vuibert, 2008.
- [CL93] René Cori and Daniel Lascar. Logique mathématique ii. fonctions récursives, théorème de gödel, théorie des ensembles, théorie des modèles, 1993.
- [CRK03] Lascar D CORI R and JL Krivine. Logique mathématique, tome 1 : Calcul propositionnel, algèbre de boole, calcul des prédicats, coll. *Sciences Sup, Dunod*, 2003.
- [DNRC01] René David, Karim Nour, Christophe Raffalli, and Pierre-Louis Curien. *Introduction à la logique : théorie de la démonstration : cours et exercices corrigés*. Dunod, 2001.
- [DPV16] Sanjoy Dasgupta, Christos H Papadimitriou, and Umesh Virkumar Vazirani. Algorithms. 2016.
- [FFR74] Michael Jo Fischer, Michael J Fischer, and Michael O Rabin. Super-exponential complexity of presburger arithmetic. 1974.
- [GLM01] Jean Goubault-Larrecq and Ian Mackie. *Proof theory and automated deduction*, volume 6. Springer Science & Business Media, 2001.
- [Har09] John Harrison. *Handbook of practical logic and automated reasoning*. Cambridge University Press, 2009.
- [KS08] Daniel Kroening and Ofer Strichman. *Decision procedures : an algorithmic point of view*. Springer Science & Business Media, 2008.
- [Lal90] René Lalement. Logique, réduction, résolution, 1990.
- [LDR93] Richard Lassaigne and Michel De Rougemont. Logique et fondements de l’informatique. *Hermes, Paris*, 1993.
- [LS15] Romain Legendre and François Schwarzentruher. *Compilation : Analyse lexicale et syntaxique du texte à sa structure en informatique*. Reference Sciences. Ellipses, 2015.
- [Mat03] Ju V Matijasevič. Enumerable sets are diophantine. In *Mathematical Logic In The 20th Century*, pages 269–273. 2003.
- [Opp78] Derek C Oppen. A $2^{2^{2^n}}$ upper bound on the complexity of presburger arithmetic. *Journal of Computer and System Sciences*, 16(3) :323–332, 1978.
- [SM73] Larry J Stockmeyer and Albert R Meyer. Word problems requiring exponential time (preliminary report). In *Proceedings of the fifth annual ACM symposium on Theory of computing*, pages 1–9. ACM, 1973.

Index

- 2SAT, 13
- arbre de preuve en déduction naturelle, 31
- assignation, 21

- capture de variables, 29
- clause de Horn, 12
- complet (système de connecteurs), 9
- complétude de la déduction naturelle, 32
- complétude de la résolution, 16
- complétude de la résolution en premier ordre, 39
- condition de vérité, 8
- consistante, 31
- conséquence sémantique, 9
- correction de la déduction naturelle, 32
- correction de la résolution, 16
- correction de la résolution en premier ordre, 39

- fonction de Skolem, 36
- forme normale conjonctive, 11, 35
- forme prénexe universelle, 35
- formule atomique, 22
- formule de Horn, 12
- formule de la logique du premier ordre, 22
- formule prénexe, 35

- instantiation, 29

- lemme de la vérité, 33
- littéral, 11, 35
- logique propositionnelle, 8

- modèle de Herbrand, 38

- occurrence libre, 23
- occurrence liée, 23

- preuve par résolution, 15
- proposition atomique, 7

- règle de contraction, 37
- règle de résolution, 15

- règle de résolution en logique du premier ordre, 37
- règles de la déduction naturelle, 30
- règles du calcul des séquents, 42

- satisfiable, 8
- signature, 21
- structure, 21
- substitution, 29
- substitution licite, 29
- syntactiquement complète, 31
- système de connecteurs, 9
- séquent, 30, 41

- table de vérité, 8
- tautologie, 8
- terme, 22
- théorie, 9
- théorie universelle, 38
- théorème de compacité, 17
- théorème de compacité de la logique du premier ordre, 34
- théorème de De Bruijn-Erdős, 18
- transformation de Tseitin, 11
- témoin de Henkin, 32

- unificateur, 37
- unificateur principal, 37

- valide, 8
- validité, 33
- valuation, 7
- variable, 21
- variable libre, 23

- équisatisfiable, 11
- équivalence de formules, 9