# Notes de cours préliminaires
# Cours de logique, premier semestre, première année, magistère STIC

Hubert Comon-Lundh & Ralf Treinen
{comon,treinen}@lsv.ens-cachan.fr

27 septembre 2005

# Chapitre 1

# Introduction

On peut distinguer 4 époques dans la logique (cette classification est aussi celle de M. Vardi, cf. `http://www.cs.rice.edu/~vardi/comp409/lec0.ps`) :

- L'âge de la réthorique (antiquité - 19ème siècle) au cours duquel la logique est une branche de la philosophie. Mais déjà dans l'antiquité, de nombreux paradoxes ont été mis à jour.
- L'âge de la logique symbolique (19ème) : avec l'introduction de notions comme la continuité, la convergence (simples ou uniformes) la nécéssité de formaliser est apparue.
- L'âge de la logique mathématique (début du 20ème). Le paradoxe de Russell, le problème des fondements des mathématiques et le programme de Hilbert. Simultanément d'autres problèmes se posent : l'interprétation des quantifications existentielles, l'axiome du tiers exclu, la définition de l'infini...
- L'âge de la logique informatique (fin 20ème - nos jours). L'automatisation, l'exécution sur machine, requiert un niveau supplémentaire de rigueur dans les énoncés, rigueur fournie par les formalismes de la logique mathématique. La difficulté intrinsèque de la résolution de problèmes se trouve intimement liée à la logique. Enfin, la correspondance de Curry-Howard montre les liens étroits entre logique et programmes : un programme est une preuve, un type de données est un énoncé et l'exécution d'un programme est une simplification de preuve d'existence en logique intuitioniste. Voir par exemple l'article (lisible par les élèves) : *On the unusual effectiveness of logic in computer science* `http://www.cs.rice.edu/~vardi/papers/aaas99.jsl.ps.gz`.

**Exercice 1 (6)**
Montrer qu'il existe deux nombres réels irrationnels $a, b$ tels que $a^b \in \mathbb{Q}$.

Le programme de Hilbert a donné lieu à des développements importants, qui ont culminé avec les théorèmes d'incomplétude de Gödel mais ont aussi permis de formaliser ce qui est faisable et ce qui ne l'est pas. Entre autres, A. Church, A. Turing, E. Post et bien d'autres ont, indépendemment, construit des modèles de calcul permettant de d'énoncer rigoureusement des résultats d'impossibilité de preuve. Sur le programme de Hilbert et ses suites, consulter par exemple l'ouvrage : *Computability, computable functions, logic, and the foundations of mathematics* par L. Epstein et A. Carnielli (Wadsworth & Brooks).

La logique mathématique s'est développée au cours du 20ème siècle en deux branches : la théorie des modèles (Voir par exemple le livre, difficile, *Model Theory*, par Chang & Keisler, 1973) et la théorie de la preuve. Cette dernière, de par sa pertinence en informatique a connu ces dernières 25 années de nombreux développements variés. Les résultats les plus célèbres sont ceux d'élimination des coupures, qui ont leur contrepartie dans les modèles de calcul comme théorèmes de normalisation forte (terminaison quelle que soit la stratégie d'exécution). Sur ce sujet, consulter par exemple *Proofs and Types* par J.-Y. Girard, Y. Lafont, P. Taylor (Cambridge University Press).

Nous nous interesserons ici aux rudiments les plus simples de théorie des modèles. Par la suite, si le temps le permet (ou au cours du 2ème semestre), nous développerons plus la théorie de la preuve et ses applications, par exemple en démonstration automatique.

# Chapitre 2

# Calcul propositionnel

C'est le formalisme logique le plus simple. Mais il est fondamental pour plusieurs raisons :

– Bien sûr, il sert d'introduction pédagogique.
– Plusieurs résultats en calcul des prédicats, en logique temporelle etc... s'obtiennent par "relèvement" de résultats du calcul propositionel.
– En fait, en pratique, il est très utilisé à cause de sa simplicité et de l'algorithmique relativement efficace qu'on peut mettre en oeuvre.

Il y a aussi plusieurs formalismes pour le calcul propositionnel. On commencera par le plus standard "à la Hilbert", puis on s'interessera au calcul des séquents, à la déduction naturelle (dans les deux cas, dans le cas classique et dans le cas intuitioniste), ainsi qu'à d'autres représentations comme les anneaux Booléens.

## 2.1 Syntaxe

La définition d'une logique passe par trois étapes : la définition des énoncés (syntaxe), la définition des modèles (sémantique) et enfin, la théorie de la preuve.

On suppose ici donné un ensemble de *variables propositionnelles* $\mathcal{P}$.

**Definition 2.1.1** *L'ensemble $\mathcal{F}_0(\mathcal{P})$ des formules du calcul propositionel est le plus petit ensemble tel que :*

– *les constantes $\top, \bot$ sont dans $\mathcal{F}_0(\mathcal{P})$*
– $\mathcal{P} \subseteq \mathcal{F}_0(\mathcal{P})$
– *Si $\phi \in \mathcal{F}_0(\mathcal{P})$ alors $\neg\phi \in \mathcal{F}_0(\mathcal{P})$*
– *Si $\phi, \psi \in \mathcal{F}_0(\mathcal{P})$, alors $\phi \vee \psi, \phi \wedge \psi, \phi \to \psi \in \mathcal{F}_0(\mathcal{P})$*

Dans cette définition, $\neg, \vee, \wedge, \to$ sont les *connecteurs logiques*.

**Exercice 2 (3)**

1. Montrer que la définition 2.1.1 a bien un sens, c'est à dire qu'il existe bien un (et un seul) plus petit ensemble (au sens de l'inclusion) qui satisfasse les conditions de la définition.

2. Montrer le principe de récurrence sur les formules : soit $R \subseteq \mathcal{F}_0(\mathcal{P})$. Si $\bot \in R, \top \in R, \mathcal{P} \subseteq R$ et que $\forall \phi, \psi \in R$, $\neg\phi, \phi \wedge \psi, \phi \vee \psi, \phi \rightarrow \psi \in R$, alors $R = \mathcal{F}_0(\mathcal{P})$.

**Exemple 2.1.1** Soit

$$\mathcal{P} = \{\texttt{La\_boîte\_1\_contient\_une\_bombe}, \ldots, \texttt{La\_boîte\_n\_contient\_une\_bombe}\}$$

un ensemble de $n$ variables propositionnelles. Voici des exemples de formules de $\mathcal{F}_0(\mathcal{P})$ :

$$\texttt{La\_boîte\_1\_contient\_une\_bombe} \wedge \texttt{La\_boîte\_2\_contient\_une\_bombe}$$
$$\texttt{La\_boîte\_1\_contient\_une\_bombe} \wedge \neg\texttt{La\_boîte\_1\_contient\_une\_bombe}$$

Pour que les formules ne prennent pas trop de place, on va abréger...

**Exemple 2.1.2** Soit $\mathcal{P} = \{A_n \mid n \in \mathbb{N}\}$. Sont des formules de $\mathcal{F}_0(\mathcal{P})$ :

$$A_2 \wedge A_2 \wedge (A_2 \vee \neg A_2)$$
$$A_2 \rightarrow (A_1 \rightarrow A_2)$$

N'est pas une formule :

$$A_1 \vee A_2 \vee \ldots \vee A_n \vee \ldots \quad \text{(disjonction infinie)}$$

Remarques :

1. Le parenthésage doit permettre de désambigüer. Habituellement la négation a priorité sur les autres connecteurs.
2. Le cas des disjonctions infinies sera (entre autres) étudié ultérieurement ; il s'agit d'une logique plus expressive que $\mathcal{F}_0(\mathcal{P})$.

## 2.2 Sémantique

Une *interprétation* est une application $I$ de $\mathcal{P}$ dans $\{0, 1\}$.

**Definition 2.2.1** *Une interprétation $I$* satisfait *une formule $\phi \in \mathcal{F}_0(\mathcal{P})$, ce que l'on note $I \models \phi$ ($\models \subseteq 2^{\mathcal{P}} \times \mathcal{F}_0(\mathcal{P})$), si*
- $\phi = \top$ *ou bien*
- $\phi \in \mathcal{P}$ *et* $I(\phi) = 1$ *ou bien*
- $\phi = \phi_1 \wedge \phi_2$ *et* $(I \models \phi_1 \text{ et } I \models \phi_2)$ *ou bien*
- $\phi = \phi_1 \vee \phi_2$ *et* $(I \models \phi_1 \text{ ou } I \models \phi_2)$ *ou bien*
- $\phi = \phi_1 \rightarrow \phi_2$ *et* $(\text{ si } I \models \phi_1 \text{ alors } I \models \phi_2)$ *ou bien*
- $\phi = \neg\psi$ *et* $I \not\models \psi$

**Definition 2.2.2** *Une interprétation $I$ satisfait un ensemble de formules $S$ (noté $I \models S$) si $I$ satisfait chacune des formules de $S$.*

*Un* modèle *d'un ensemble $S$ de formules est une interprétation $I$ telle que $I \models S$.*

*Une formule $\phi$ (resp. un ensemble de formules $S'$) est une* conséquence logique *de $\psi$ (resp. d'un ensemble de formules $S$) si tout modèle de $\psi$ (resp. tout modèle de $S$) est un modèle de $\phi$ (resp. est un modèle de l'une des formules de $S'$). On note alors $\psi \models \phi$ (resp. $S \models S'$).*

*Une formule est* satisfaisable *si elle a au moins un modèle.*

*Une formule $\phi$ est* valide *si toute interprétation est un modèle de $\phi$.*

*On dit que deux formules sont* logiquement équivalentes *lorsqu'elles ont les mêmes modèles.*

**Exemple 2.2.1** Reprenant l'exemple 2.1.1, L'interprétation ...

**Exercice 3 (1)**
Donner l'ensemble de tous les modèles de la formule $\phi \stackrel{\text{def}}{=} ((P \to Q) \vee (\neg P \to \neg Q)) \wedge (Q \wedge R \to \neg P)$ lorsque $\mathcal{P} = \{P, Q, R\}$.

**Exercice 4 (1)**
Montrer que :

1. $\phi$ est insatisfaisable si et seulement si $\neg\phi$ est valide
2. $\phi \models \psi$ si et seulement si $\phi \to \psi$ est valide.

**Exercice 5 (4)**
Montrer que, si $\mathcal{P}$ est fini, alors dans tout ensemble de formules fini de cardinal assez grand (on précisera cette borne), il existe deux formules logiquement équivalentes (i.e. qui ont même ensembles de modèles).

**Exercice 6 (5)**

1. Montrer que, lorsque $\mathcal{P}$ est fini, pour tout ensemble d'interprétations $S$, il existe un ensemble de formules $E$ tel que $S$ est exactement l'ensemble des modèles de $E$.
2. Montrer que ce résultat est faux lorsque $\mathcal{P}$ est infini.

**Exercice 7 (6)**
Donner un exemple d'un ensemble de formules dont l'ensemble des modèles est infini et dénombrable.

**Exercice 8 (5)**
**(théorème d'interpolation)** Soient $\phi, \psi$ telles que $\phi \models \psi$. Montrer que il existe une formule $\theta$ telle que $\phi \models \theta$, $\theta \models \psi$ et les variables propositionnelles apparaissant dans $\theta$, apparaissent aussi dans $\phi$ et dans $\psi$.

**Exercice 9 (6)**
**(théorème de compacité)** $\{0, 1\}$ est muni de la topologie pour laquelle tout sous-ensemble est un ouvert. $\{0, 1\}$ muni de cette topologie est ainsi un compact. L'ensemble $\{0, 1\}^A$ des interprétations des formules propositionnelles construites sur $A$ est alors muni de la topologie produit : les ouverts sont les unions de produits des ouverts de $\{0, 1\}$. Tout produit de compacts étant compact (ce qui est admis), l'espace $\mathcal{I}$ de toutes les interprétations est ainsi un compact.

1. Montrer que, pour toute formule $\phi$, l'ensemble des interprétations qui satisfont $\phi$ est un fermé de $\mathcal{I}$.
2. En déduire que tout ensemble de formules insatisfaisable contient un sous-ensemble fini insatisfaisable.

Les connecteurs logiques ne sont pas tous indépendants. Par exemple, pour toutes formules $\phi$ et $\psi$, $\phi \rightarrow \psi$ est logiquement équivalent à $\neg\phi \vee \psi$.

**Exercice 10 (1)**
Le démontrer.

Ainsi, $\rightarrow$ est *définissable* à l'aide de $\vee, \wedge, \neg$.

**Exercice 11 (2)**
Montrer que $\vee, \wedge, \neg$ sont définissables à l'aide du seul connecteur $\rightarrow$ et de la constante $\perp$. On dit alors que l'ensemble $\{\rightarrow, \perp\}$ est *fonctionnellement complet*.

On peut aussi définir de nouveaux connecteurs logiques, par exemple

$$\phi \leftrightarrow \psi \stackrel{\text{def}}{=} (\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi)$$

ou

$$\phi \oplus \psi \stackrel{\text{def}}{=} (\phi \wedge \neg\psi) \vee (\neg\phi \wedge \psi)$$

**Exercice 12 (3)**
Plus généralement, les connecteurs logiques peuvent être vus comme des fonctions Booléennes. Si $F$ est un ensemble de fonctions Booléennes, on note $A(F)$ l'ensemble de toutes les fonctions Booléennes obtenues à l'aide des fonctions de $F$ et de la composition et des projections (fonctions $\pi_n^i(x_1, \ldots, x_n) \stackrel{\text{def}}{=} x_i$).

Pour tout entier $n \geq 1$ on note $d_n$ (resp. $c_n$) la fonction Booléenne à $n$ arguments qui renvoie 0 (resp. 1) si et seulement si tous ses arguments valent 0 (resp. 1).

1. Montrer que, pour tous $n, m, k \geq 2$, $A(c_n, f_\neg) = A(d_m, f_\neg)$ contient toutes les fonctions Booléennes à $k$ arguments.
2. Montrer que $f_\neg$ n'est pas dans $A(f_\vee, f_\wedge, f_\rightarrow, f_\leftrightarrow)$

**Exercice 13 (4)**
Donner un connecteur logique binaire qui est, seul, fonctionnellement complet.

**Exercice 14 (5)**
Montrer que $\{\leftrightarrow, \neg\}$ n'est pas fonctionnellement complet.

**Exercice 15 (6)**
Un ensemble de formules $E$ est *indépendant* si, pour toute formule $\phi \in E$, $E \setminus \{\phi\} \not\models \phi$.

1. Montrer que, pour tout ensemble fini de formules $E$, il existe un sous-ensemble fini $E' \subseteq E$ indépendant tel que, pour tout $\phi \in E$, $E' \models \phi$.

2. Montrer que, pour tout ensemble dénombrable $E$ de formules, il existe un ensemble $E'$ de formules tel que $E'$ est indépendant et, pour toute formule $\phi \in E'$, $E \models \phi$, pour toute formule $\psi \in E$, $E' \models \psi$.
3. Montrer qu'il n'est pas toujours possible d'avoir (en plus) $E' \subseteq E$.

**Exercice 16 (8)**
On considère $n$ coffres, chacun contenant un trésor ou une bombe. Le problème est de déterminer le contenu exact de chacun des coffres. Pour cela, on peut poser par écrit une liste de $N$ questions (formules du calcul propositionnel, les variables propositionelles étant le contenu des coffres). On obtient, une fois la liste complète des questions établies, la réponse (i.e. l'interprétation) aux $N$ questions. Mais il est possible que (au plus) $k$ des $N$ réponses soient incorrectes.

Etant donnés $n, k$, on s'intéresse au problème de trouver le $N$ minimal, et les questions correspondantes, de manière à déterminer à coup sûr le contenu des coffres.

Donner le $N$ minimal (et les questions correspondantes) dans les cas suivants.

1. $k = 0$ et $n$ quelconque
2. $n = k = 1$
3. $n \leq 5$, $k = 1$
4. $k = 1$ et $n$ quelconque

Prendre soin dans chaque cas de justifier la réponse.

Parmi les théorèmes célèbres (en calcul des prédicats), le théorème de compacité, énoncé ici dans le cas propositionnel, permet de ramener l'insatisfaisabilité à l'insatisfaisabilité finie (mais ne sera d'aucune utilité dans le cadre du calcul propositionnel).

**Théorème 2.2.1 (compacité)** *Un ensemble de formules du calcul propositionnel sur $\mathcal{P} = \{A_n \mid n \in \mathbb{N}\}$ est insatisfaisable si et seulement si il contient un sous-ensemble fini de formules insatisfaisable.*

Preuve:
Soit $\geq$ la relation d'ordre sur $\mathcal{P}$ définie par $A_n \geq A_m$ si et seulement si $n \geq m$. Une *interprétation partielle* est une fonction de $\mathcal{P}$ dans $\{0, 1\}$ dont le domaine de définition est un ensemble $\{Q \in \mathcal{P} \mid Q < P\}$ (on notera en indice de l'interprétation partielle la borne supérieure de son domaine de définition). L'ensemble des interprétations partielles est alors ordonné par prolongement : $I_{P_1} \leq I_{P_2}$ si $P_1 \leq P_2$ et $I_{P_2}$ restreinte aux variables propositionelles inférieures à $P_1$ coïncide avec $I_{P_1}$.

On peut représenter graphiquement cet ordre sous forme d'un arbre des interprétations partielles (cf. figure 2.1).

Soit maintenant un ensemble $S$ insatisfaisable. On peut supposer sans perdre de généralité que $S$ ne contient pas deux formules logiquement équivalentes. Si l'ensemble des variables propositionnelles intervenant dans les formules de $S$ est fini, alors $S$ est fini (cf. exercice 5). On peut donc supposer sans perdre de

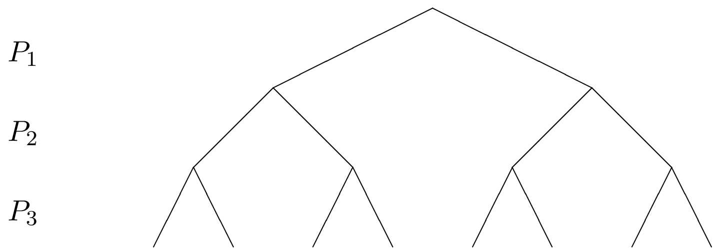


FIG. 2.1 – arbre des interprétations partielles

généralité que l'ensemble $\mathcal{P}$ est infini et que toute variable de $\mathcal{P}$ apparaît dans au moins une formule de $S$.

Une interprétation partielle $I$ *falsifie* une formule $\phi \in S$ si les variables de $\phi$ sont dans le domaine de définition de $I$ et $I \not\models \phi$.

Considérons l'arbre des interprétations partielles qui ne falsifient aucune formule de $S$. Formellement : si $I$ ne falsifie aucune formule de $S$ et $J \leq I$, alors $J$ ne falsifie aucune formule de $S$. Si cet arbre était infini, alors, comme il est à branchement fini, il contiendrait un chemin infini (lemme de König). Mais un tel chemin infini définit une interprétation qui satisfait $S$, ce qui est absurde. Il en résulte que l'arbre est fini et donc que le sous-ensemble de $S$ qui ne contient que les variables propositionnelles correspondantes est fini, chacune de ses extensions étant insatisfaisable. □

**Exercice 17 (3)**
Montrer qu'un graphe est coloriable avec $k$ couleurs si et seulement si chacun de ses sous-graphes finis est coloriable avec $k$ couleurs.

**Exercice 18 (5)**
Soit $E$ un ensemble de formules du calcul propositionnel sur $\mathcal{P}$. On dira que $E$ est *maximal cohérent* si $E$ est satisfaisable et que, pour toute formule $\phi$ du calcul propositionnel, ou bien $\phi \in E$ ou bien $E \cup \{\phi\}$ est insatisfaisable.

1. Supposant que $\mathcal{P}$ est fini, montrer que tout ensembe de formules $E$ satisfaisable est contenu dans un ensemble maximal cohérent.
2. Montrer que cet ensemble maximal cohérent n'est pas unique : donner (toujours dans le cas où $\mathcal{P}$ est fini) un ensemble $E$ et deux ensembles maximaux cohérents distincts contenant $E$.
3. Que devient le résultat de la première question lorsque $\mathcal{P}$ est infini dénombrable ?

**Exercice 19 (7)**
Soit $\Sigma$ un ensemble de formules de $\mathcal{F}_0(\mathcal{P})$. On dit que $\Sigma$ est *préservé par intersections finies* si, l'intersection de deux modèles de $\Sigma$ est un modèle de $\Sigma$. $\Sigma$ est *préservé par intersections* si toute intersection de modèles de $\Sigma$ est un modèle de $\Sigma$. $\Sigma$ est *axiomatisé* par $\Gamma$ si, pour tout $\phi \in \mathcal{F}_0(\mathcal{P})$, $\Gamma \models \phi$ si et seulement si $\Sigma \models \phi$.

1. Montrer que $\Sigma$ est préservé par intersections finies si et seulement si $\Sigma$ est préservé par intersections.
2. Une *clause* est une formule

$$A_1 \vee \ldots \vee A_n$$

   dans laquelle les $A_i$ sont des variables propositionnelles (appelés *littéraux positifs*) ou des négations de variables propositionnelles (appelées *littéraux négatifs*). Une *clause de Horn* est une clause contenant au plus un littéral positif.

   Montrer que $\Sigma$ est axiomatisable par un ensemble de clauses de Horn si et seulement si $\Sigma$ est stable par intersections. (On pourra supposer, sans perte de généralité, que $\Sigma$ est un ensemble de clauses).