Logique propositionnelle classique

MLO

Catherine Dubois, Julien Narboux (Strasbourg)

Le calcul des propositions (aussi appelé logique propositionnelle, ou bien CP0) est une des logiques les plus simples, elle ne comporte que des *variables* et des *connecteurs* logiques.

Premier volet : la syntaxe

Syntaxe

ou Comment écrire une formule de la logique des propositions ? Définition par induction

Soit V un ensemble dénombrable de symboles appelées *variables (propositionnelles)*.
L'ensemble des formules de la logique propositionnelle sur l'ensemble des variables V ($\subset (V \cup \{\bot, \wedge, \vee, \Rightarrow, (,), \neg\})^*$) est défini inductivement par :

- $\bot$ est une formule (lue *toujours faux*)
- une variable propositionnelle, élément de V, est une formule
- si F est une formule alors $\neg F$ est une formule
- si F et G sont deux formules alors $(F \wedge G)$ est une formule
- si F et G sont deux formules alors $(F \vee G)$ est une formule
- si F et G sont deux formules alors $(F \Rightarrow G)$ est une formule

Une formule de la logique propositionnelle est aussi appelée une *proposition*

Exemples de formules (avec $V = \{p, q, r\}$:
$((p \wedge q) \wedge \neg r))$, $(p \Rightarrow (\bot \vee q))$.

Exemples qui ne sont pas des formules:
$p \Rightarrow\Rightarrow p$, $p\neg q$

Dans la suite on s'autorisera à omettre les parenthèses en utilisant les règles de priorité et d'associativité classiques :

- Ordre des priorités: $\neg > \wedge > \vee > \Rightarrow$.
- Associativité:
  - $\vee$ et $\wedge$ sont associatifs à gauche,
  - $\Rightarrow$ est associatif à droite.

Ainsi la formule $((F_1 \wedge F_2) \wedge F_3)$ pourra s'écrire $F_1 \wedge F_2 \wedge F_3$.

Dans toute la suite des transparents p, q, r etc. désignent des variables propositionnelles.
F, G, H etc désignent des formules de la logique propositionnelle.

En OCaml : Les formules sont représentées à l'aide d'un type somme

```
type formule =
| Bottom
| Variable of string
| Non of formule
| Et of (formule * formule)
| Ou of (formule * formule)
| Implique of (formule * formule)
;;
```

La formule $(p \Rightarrow (\bot \vee q))$ est représentée par le terme Ocaml suivant :

```
Implique (Variable "p", Ou(Bottom, Variable "q"));;
```

Deuxième volet : la sémantique

Sémantique

ou Que signifie cette formule ?

Formule $\hookrightarrow$ valeur de vérité $\in \{1, 0\}$ (0 signifie faux et 1 signifie vrai)

I : interprétation : fonction de V dans $\{1, 0\}$
Par exemple $V = \{p, q, r\}, I(p) = 1, I(q) = 0 = I(r)$

On étend I à l'ensemble des formules de la façon suivante :

- si p est une variable alors $I(p)$ est sa valeur de vérité
- $I(\bot) = 0$ ($\bot$ est une formule fausse)
- $I(\neg F) = 0$ si $I(F) = 1$, $I(\neg F) = 1$ si $I(F) = 0$,
- $I(F \wedge G) = 0$ si $I(F) = 0$ ou $I(G) = 0$, $I(F \wedge G) = 1$ sinon
- $I(F \vee G) = 1$ si $I(F) = 1$ ou $I(G) = 1$, $I(F \wedge G) = 0$ sinon
- $I(F \Rightarrow G) = 1$ si $I(F) = 1$ et $I(G) = 1$ ou si $I(F) = 0$, $I(F \Rightarrow G) = 0$ sinon

Théorème

soit une formule F, soient deux interprétations I_1 et I_2 telles que pour toute variable propositionnelle v de F on a $I_1(v) = I_2(v)$ alors $I_1(F) = I_2(F)$

$\Longrightarrow$ Il suffit de connaître les valeurs de vérité des variables qui apparaissent dans une formule pour calculer sa valeur de vérité

La table de vérité d'une formule F est la fonction qui à chaque interprétation I possible (2^n si n est le nombre de variables de F) associe la valeur $I(F)$.

p	q	$p \Rightarrow q$	$\neg p \vee q$	$(p \Rightarrow q) \Rightarrow \neg p \vee q$
1	1	1	1	1
1	0	0	0	1
0	1	1	1	1
0	0	1	1	1

En OCaml :

- Les valeurs de vérité sont représentées par des valeurs de type bool : 1 par `true`, 0 par `false`.
- Une interprétation est représentée par une liste de couples (nom de variable, valeur de vérité) c'est-à-dire une liste de type `(string*bool) list`.
- `interp_formule : formule -> interpretation -> bool`

```
let rec interp_formule f i = match f with
| Bottom
| Variable v -> ....
```

A vous de jouer ...

- Si $I(F) = 1$ on dit que I satisfait la formule F et on écrit $I \models F$.
  Exemple : I tel que $I(p) = 1$, $I(q) = 0$ satisfait $p \vee q$.
- F est satisfaisable ssi il existe une interprétation I qui la rende vraie ($I \models F$)
  Exemple : $p \vee q$ est satisfiable.
- F est une tautologie (ou est valide) ssi elle est satisfaite par toute interprétation : $\models F$
  Exemple : $\models (p \Rightarrow q) \Rightarrow \neg p \vee q$
- F est une contradiction ssi elle n'est satisfaite par aucune interprétation
  Exemple : $p \wedge \neg p$ est une contradiction
  Théorème
  F est une contradiction ssi $\neg F$ est valide.

- Si Σ est un ensemble de formules et I une interprétation, on dit que I satisfait Σ ($I \models \Sigma$) si $I \models F$ pour toute formule F de Σ
  Exemple : soit I telle que $I(p) = 0, I(q) = 1$, on a $I \models \{p \Rightarrow q, q\}$
- Un ensemble de formules est contradictoire s'il n'existe aucune interprétation qui le satisfasse.
  Exemple : $\{p \wedge q, \neg p\}$ est contradictoire
- Une formule F est une conséquence sémantique d'un ensemble de formules Σ : $\Sigma \models F$ ssi toute interprétation I qui satisfait Σ satisfait aussi F
  Exemple : $\{p \Rightarrow q, p\} \models q$
- Deux formules F et G sont sémantiquement équivalentes (noté $F \equiv G$) si l'un est conséquence sémantique de l'autre et vice-versa ($\{F\} \models G$ et $\{G\} \models F$).
  Autre caractérisation : F et G ont la même table de vérité.
  Exemple : $\neg(p \vee q) \equiv \neg p \wedge \neg q$

Un petit problème

Un psychiatre pour logiciens écoute un de ses patients énumérer ses sentiments à propos de deux charmantes collègues :

- J'aime Marie ou j'aime Jeanne
- Si j'aime Marie alors j'aime Jeanne

Le psychiatre conclut que le logicien aime Jeanne. Pourquoi ?

Un petit problème : modélisation

Soit m la proposition 'J'aime Marie'. Soit j la proposition 'j'aime Jeanne'.
La première proposition s'écrit $m \vee j$. La seconde s'écrit $m \Rightarrow j$.
On veut montrer que j est conséquence logique de $m \vee j$ et $m \Rightarrow j$, i.e.

$$m \vee j, m \Rightarrow j \models j$$

On s'intéresse aux interprétations où les deux propositions sont vraies.
Deux interprétations sont possibles :

$$I_0(m) = I_0(j) = 1$$

et

$$I_1(m) = 0, I_1(j) = 1$$

Dans les deux cas, la valeur de vérité de j est 1.

Théorème

$\Sigma \models F \Rightarrow G$ ssi $\Sigma, F \models G$ (prop 8.1)

Proof.

- Hypothèse $\Sigma \models F \Rightarrow G$ - Montrons $\Sigma, F \models G$

Soit I une interprétation telle que $I \models \Sigma, F$. Montrons qu'elle satisfait G.
I satisfait Σ donc I satisfait $F \Rightarrow G$ (hyp)
De plus on a $I(F) = 1$ donc $I(F \Rightarrow G) = 1 = I(G)$ cqfd

- (Réciproque) Hypothèse : $\Sigma, F \models G$ - Montrons $\Sigma \models F \Rightarrow G$

Soit I interprétation telle que $I \models \Sigma$. Montrons que $I(F \Rightarrow G) = 1$.
Si $I(F) = 1$ alors I satisfait Σ et F donc par hypothèse I satisfait G. Et donc $I(F \Rightarrow G) = I(G) = 1$
Si $I(F) = 0$ alors $I(F \Rightarrow G) = 1$
Dans les deux cas on $I \models F \Rightarrow G$. cqfd □

Théorème

$\Sigma \models F$ ssi $\Sigma, \neg F$ est un ensemble contradictoire (prop 8.2)

Proof.

- Hypothèse $\Sigma \models F$ - Montrons $\Sigma, \neg F$ est un ensemble contradictoire

Supposons que $\Sigma, \neg F$ n'est pas contradictoire. Donc il existe une interprétation I qui satisfait Σ et $\neg F$.
On a $I(\neg F) = 1$ donc $I(F) = 0$. Or d'après l'hypothèse puisque I satisfait Σ alors I satisfait F, soit $I(F) = 1$.

- Hypothèse : $\Sigma, \neg F$ contradictoire - Montrons $\Sigma \models F$

Soit I interprétation telle que $I \models \Sigma$. Montrons que $I(F) = 1$.
Si $I(F) = 0$ alors $I(\neg F) = 1$. Alors I satistait Σ et $\neg F$. Ce qui est impossible de par l'hypothèse.
Donc $I(F) = 1$. cqfd □

Equivalences et tautologies par substitutions

Substitution

Si F et G sont des formules et p une variable propositionnelle, on définit par induction la formule $F[p := G]$ obtenue à partir de F en substituant G à p dans F.

- $\bot[p := G] = \bot$
- $q[p := G] = G$ si $q = p, q$ sinon
- $(\neg F_1)[p := G] = \neg(F_1[p := G])$
- $(F_1 \wedge F_2)[p := G] = (F_1[p := G]) \wedge (F_2[p := G])$
- $(F_1 \vee F_2)[p := G] = (F_1[p := G]) \vee (F_2[p := G])$
- $(F_1 \Rightarrow F_2)[p := G] = (F_1[p := G]) \Rightarrow (F_2[p := G])$

Exemple : Soit G la formule $p \vee \neg q$.
$(r \wedge \neg r \wedge q)[r := G] = (p \vee \neg q) \wedge \neg(p \vee \neg q) \wedge q$

Théorème

Soit I une interprétation. Soit I_0 l'interprétation définie par $I_0(p) = I(G)$ et $I_0(q) = I(q)$ pour tout $q \neq p$. Alors $I(F[p := G]) = I_0(F)$ (prop. 9)

Proof.

Par induction sur F (on applique le principe d'induction structurelle)

1. $I(\bot[p := G]) = I(\bot) = 0 = I_0(\bot)$
2. soit q une variable propositionnelle.
   si $p = q$, $I(q[p := G] = I(G) = I_0(G)$ par construction de I_0
   si $p \neq q$, $I(q[p := G] = I(q) = I_0(q)$ par construction de I_0
3. hyps d'induction : $I(F_1[p := G]) = I_0(F_1)$ et $I(F_2[p := G]) = I_0(F_2)$.
   $I((F_1 \wedge F_2)[p := G]) = I(F_1[p := G] \wedge F_2[p := G])$
   $= I(F_2[p := G])$ si $I(F_1[p := G]) = 1$, 0 sinon.
   $= I_0(F_1 \wedge F_2)$
4. de même pour F de la forme $F_1 \vee F_2$
5. de même pour F de la forme $F_1 \Rightarrow F_2$
6. de même pour F de la forme $\neg F_1$ (1 seule hypothèse d'induction)

Corollaires :

1. Si $\models F$ alors $\models F[p := G]$
2. Si $F \equiv F'$ alors $F[p := G] \equiv F'[p := G]$
3. Si $G \equiv G'$ alors $F[p := G] \equiv F[p := G']$

Il en découle les équivalences suivantes :

$F \wedge F \equiv F$	$F \vee F \equiv F$	3.1
$F \wedge G \equiv G \wedge F$	$F \vee G \equiv G \vee F$	3.2
$F \wedge (G \wedge H) \equiv (F \wedge G) \wedge H$	$F \vee (G \vee H) \equiv (F \vee G) \vee H$	3.3
$F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$	$F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$	3.4
$\neg(F \wedge G) \equiv \neg F \vee \neg G$	$\neg(F \vee G) \equiv \neg F \wedge \neg G$	3.5
$F \Rightarrow G \equiv \neg F \vee G$	$\neg(F \Rightarrow G) \equiv F \wedge \neg G$	3.6
$\neg\neg F \equiv F$		3.7

En effet,

p	$p \wedge p$
1	1
0	0

Donc $p \equiv p \wedge p$ et donc par le corrolaire précédent on a $p[p := F] \equiv (p \wedge p)[p := F]$ d'où $F \wedge F \equiv F$.

Décidabilité

Les notions de validité et de satisfaisabilité en calcul des propositions sont décidables.

Algorithme (naïf) :
etant donnée une formule F ayant n variables propositionnelles.
Calculer les 2^n interprétations possibles.
Pour chacune d'entre elles calculer la valeur de vérité de F.
Si toutes les valeurs de vérité de F obtenues sont toutes égales à 1 alors F est valide.
Si au moins une est égale à 1 alors F est satisfaisable.

(cf TP Caml)

Mise sous forme normale conjonctive

- Un littéral: une variable ou une négation de variable
  p, $\neg p$
- Une clause: une disjonction de littéraux
  $p \vee \neg q \vee r$
- Formule en FNC: une conjonction de clauses
  $(p \vee q \vee r) \wedge (\neg p \vee t) \wedge (\neg r \vee \neg p)$

- Exemples de formules en forme normale conjonctive :
  $(p \vee \neg q) \wedge (\neg r \vee p)$, p, $p \wedge q$
- Exemples de formules qui ne sont pas en forme normale :
  $\neg(p \wedge q)$, $p \Rightarrow q$

- Théorème
  Pour toute formule propositionnelle, il existe une formule en FNC logiquement équivalente

Démonstration = Méthode

1. On élimine les $\Rightarrow$ en transformant $F \Rightarrow G$ par $\neg F \vee G$.
2. On propage les négations vers les feuilles avec les règles:
   - $\neg(F \vee G)$ devient $\neg F \wedge \neg G$
   - $\neg(F \wedge G)$ devient $\neg F \vee \neg G$
3. On simplifie les double-négations en transformant $\neg\neg F$ en F.
4. On distribue le $\wedge$ sur le $\vee$ avec les règles:
   - $F \vee (G \wedge H)$ devient $(F \vee G) \wedge (F \vee H)$
   - $(F \wedge G) \vee H$ devient $(F \vee H) \wedge (G \vee H)$
5. On simplifie.

Exemple

$$\neg(p \Rightarrow q \wedge q \Rightarrow p)$$

Exemple

$$\neg(p \Rightarrow q \wedge q \Rightarrow p)$$

$$\neg((\neg p \vee q) \wedge (\neg q \vee p))$$

Exemple

$$\neg(p \Rightarrow q \wedge q \Rightarrow p)$$

$$\neg((\neg p \vee q) \wedge (\neg q \vee p))$$

$$(\neg(\neg p \vee q)) \vee (\neg(\neg q \vee p))$$

Exemple

$$\neg(p \Rightarrow q \wedge q \Rightarrow p)$$

$$\neg((\neg p \vee q) \wedge (\neg q \vee p))$$

$$(\neg(\neg p \vee q)) \vee (\neg(\neg q \vee p))$$

$$(p \wedge \neg q) \vee (q \wedge \neg p)$$

Exemple

$$\neg(p \Rightarrow q \wedge q \Rightarrow p)$$

$$\neg((\neg p \vee q) \wedge (\neg q \vee p))$$

$$(\neg(\neg p \vee q)) \vee (\neg(\neg q \vee p))$$

$$(p \wedge \neg q) \vee (q \wedge \neg p)$$

$$(p \vee (q \wedge \neg p)) \wedge (\neg q \vee (q \wedge \neg p))$$

Exemple

$$\neg(p \Rightarrow q \wedge q \Rightarrow p)$$

$$\neg((\neg p \vee q) \wedge (\neg q \vee p))$$

$$(\neg(\neg p \vee q)) \vee (\neg(\neg q \vee p))$$

$$(p \wedge \neg q) \vee (q \wedge \neg p)$$

$$(p \vee (q \wedge \neg p)) \wedge (\neg q \vee (q \wedge \neg p))$$

$$(p \vee (q \wedge \neg p)) \wedge (\neg q \vee (q \wedge \neg p))$$

Exemple

$$\neg(p \Rightarrow q \wedge q \Rightarrow p)$$

$$\neg((\neg p \vee q) \wedge (\neg q \vee p))$$

$$(\neg(\neg p \vee q)) \vee (\neg(\neg q \vee p))$$

$$(p \wedge \neg q) \vee (q \wedge \neg p)$$

$$(p \vee (q \wedge \neg p)) \wedge (\neg q \vee (q \wedge \neg p))$$

$$(p \vee (q \wedge \neg p)) \wedge (\neg q \vee (q \wedge \neg p))$$

$$((p \vee q) \wedge (p \vee \neg p)) \wedge ((\neg q \vee q) \wedge (\neg q \vee \neg p))$$

Exemple

$$\neg(p \Rightarrow q \wedge q \Rightarrow p)$$

$$\neg((\neg p \vee q) \wedge (\neg q \vee p))$$

$$(\neg(\neg p \vee q)) \vee (\neg(\neg q \vee p))$$

$$(p \wedge \neg q) \vee (q \wedge \neg p)$$

$$(p \vee (q \wedge \neg p)) \wedge (\neg q \vee (q \wedge \neg p))$$

$$(p \vee (q \wedge \neg p)) \wedge (\neg q \vee (q \wedge \neg p))$$

$$((p \vee q) \wedge (p \vee \neg p)) \wedge ((\neg q \vee q) \wedge (\neg q \vee \neg p))$$

$$(p \vee q) \wedge (\neg q \vee \neg p)$$

Attention !

La formule peut grandir de manière exponentielle.

Le problème SAT

- Entrée : une formule propositionnelle F en forme normale conjonctive
- Sortie : F est-elle satisfaisable?
  Si oui, fournir un modèle (ie une interprétation qui satisfait F).
- Pourquoi en FNC?
  - Forme normale utilisée par les algorithmes
  - F est satisfaite ssi chaque clause a au moins un littéral vrai
    $(p \vee q \vee r) \wedge (\neg p \vee t) \wedge (\neg r \vee \neg p)$
  - Ensemble de clauses = ensemble de contraintes à satisfaire

Utilité pratique de SAT

- Encoder un problème en logique propositionnelle
- Utiliser un solveur SAT
- Retranscrire le modèle pour trouver une solution au problème

Application : coloriage de graphes, planification, modélisation de circuits, vérification de modèles (model-checking, algo/protocole)
$\Longrightarrow$ on a très vite des centaines de variables
problème de complexité

En chiffres :

Taille du problème	n	n^2	n^3	$(2^n)/2$
1	1ms	1ms	1ms	1ms
10	10ms	100ms	1s	512ms
20	20ms	400ms	8s	8min44s
30	30ms	900ms	27s	6j5h
100	100ms	10s	16min40s	20Md de Md d'années

On ne connaît pas d'algorithme polynomial pour la résolution du problème SAT, et on ne sait pas s'il peut en exister.

Algorithmes incomplets

- Avantages : possible de trouver un modèle rapidement si le problème est satisfaisable
- Inconvénients :
  - Pas sûr de trouver un modèle, même si la formule est SAT
  - Si la formule est non-SAT, aucune réponse
  - A utiliser si on pense que la formule est SAT, si on a besoin d'un modèle

Algorithmes complets

- Ils donnent toujours une réponse (si assez de temps et d'espace)
- algorithme DP, algorithme DPLL, algorithmes de décomposition arborescente

Etude en TP de DP/DPLL

Troisième volet : le raisonnement

Preuve formelle et règles de déduction

Jusqu'à présent, caractérisation des formules en se ramenant à leur interprétation.
Désormais on ne va faire que des manipulations syntaxiques pour déduire qu'une formule est vraie ou non.

But de ce 3ème volet : quand dirons nous qu'une proposition se déduit des propositions F_1, F_2 $\ldots F_n$?
Pour justifier une déduction, on montrera une *preuve*.

$\Longrightarrow$ **Au lieu de s'intéresser à ce qui est vrai, on s'intéresse à ce qui est prouvable**

Une preuve ou déduction sera un assemblage de raisonnements suffisamment élémentaires pour paraître évidents.

Les raisonnements élémentaires sont formalisées au moyen de règles d'inférence.
Ici : système d'inférence de la déduction naturelle (il en existe d'autres)

Un séquent est un couple noté $\Gamma \vdash F$ où Γ est un ensemble fini de formules et F une formule.
Γ appelé contexte du séquent
F est appelée conclusion du séquent.

Les séquents sont les objets manipulés dans les déductions/preuves.

Règles de déduction : généralités

Les règles de déduction sont présentées de la manière suivante :

$$\frac{\Delta_1 \vdash F_1 \quad \ldots \quad \Delta_k \vdash F_k}{\Delta \vdash F}$$

Une telle règle se lit *si on peut déduire F_1 des hypothèses Δ_1, . . . , si on peut déduire F_k des hypothèses Δ_k, alors on peut déduire F des hypothèses Δ.*

On peut aussi lire cette règle en *mode arrière* de la façon suivante : *pour prouver F à partir des hypothèses Δ, il suffit de prouver F_1 avec les hypothèses Δ_1, . . . et de prouver F_k à partir des hypothèses Δ_k.*

Séquents au dessus du trait horizontal : les prémisses de la règle
Séquent en dessous du trait : conclusion de la règle

La règle comprend des méta-variables : on les notera A, B : elles peuvent être remplacées par n'importe quelle formule.

Exemple : $\dfrac{\Delta \vdash A \Rightarrow B \qquad \Delta \vdash A}{\Delta \vdash B}$

Notion de Preuve

Une règle sans prémisses est un axiome

Une preuve de $\Gamma \vdash F$ est une suite d'applications de règles d'inférence commençant par $\Gamma \vdash F$ et se terminant par des axiomes.
Autre définition : une preuve du séquent s est un arbre dont la racine est le séquent à prouver s, les noeuds les séquents obtenus en appliquant les règles d'inférence. Les feuilles de l'arbre sont des instances des axiomes.

Un théorème est une formule prouvable.
"F est un théorème" sera noté $\vdash F$, cela signifie qu'*il existe une preuve du séquent* $\vdash F$ *(pas d'hypothèses).*

Déduction naturelle

Il y a trois sortes de règles :

- les règles élémentaires (la règle dite de l'axiome et celle de l'affaiblissement)
- pour chaque connecteur, une ou plusieurs règles d'introduction
  Le connecteur apparaît quand on lit la règle de haut en bas.
  Exemple : $\dfrac{\Delta, A \vdash B}{\Delta \vdash A \Rightarrow B}$
- pour chaque connecteur, une ou plusieurs règles d'élimination
  Le connecteur disparaît quand on lit la règle de haut en bas.
  Exemple : $\dfrac{\Delta \vdash A \Rightarrow B \qquad \Delta \vdash A}{\Delta \vdash B}$

Déduction naturelle : les règles élémentaires

$$(ax) \qquad \Delta, A \vdash A$$

$$(aff) \qquad \frac{\Delta \vdash A}{\Delta, B \vdash A}$$

Déduction naturelle : élimination et introduction de $\Rightarrow$, $\wedge$

$$(\Rightarrow_i) \quad \frac{\Delta, A \vdash B}{\Delta \vdash A \Rightarrow B}$$

$$(\Rightarrow_e) \quad \frac{\Delta \vdash A \Rightarrow B \qquad \Delta \vdash A}{\Delta \vdash B}$$

$$(\wedge i) \quad \frac{\Delta \vdash A \qquad \Delta \vdash B}{\Delta \vdash A \wedge B}$$

$$(\wedge e_g) \quad \frac{\Delta \vdash A \wedge B}{\Delta \vdash A}$$

$$(\wedge e_d) \quad \frac{\Delta \vdash A \wedge B}{\Delta \vdash B}$$

Déduction naturelle : élimination et introduction de $\vee$, /

$$(\vee i_g) \quad \frac{\Delta \vdash A}{\Delta \vdash A \vee B}$$

$$(\vee i_d) \quad \frac{\Delta \vdash B}{\Delta \vdash A \vee B}$$

$$(\vee e) \quad \frac{\Delta \vdash A \vee B \qquad \Delta, A \vdash C \qquad \Delta, B \vdash C}{\Delta \vdash C}$$

$$(\neg i) \quad \frac{\Delta, A \vdash \bot}{\Delta \vdash \neg A}$$

$$(\neg e) \quad \frac{\Delta \vdash \neg A \qquad \Delta \vdash A}{\Delta \vdash \bot}$$

Déduction naturelle : Absurdité classique

$$(\bot_c)\ \frac{\Delta, \neg A \vdash \bot}{\Delta \vdash A}$$

Exemple : $F \wedge G \Rightarrow G \wedge F$ est un théorème
Montrons que l'on peut dériver le séquent $F \wedge G \Rightarrow G \wedge F$ à partir des règles d'inférence précédentes.

$$\frac{}{F \wedge G \vdash F \wedge G}\,ax$$

Exemple : $F \wedge G \Rightarrow G \wedge F$ est un théorème
Montrons que l'on peut dériver le séquent $F \wedge G \Rightarrow G \wedge F$ à partir des règles d'inférence précédentes.

$$\dfrac{\dfrac{}{F \wedge G \vdash F \wedge G}\,ax}{F \wedge G \vdash G}\,\wedge_{e_d}$$

Exemple : $F \wedge G \Rightarrow G \wedge F$ est un théorème
Montrons que l'on peut dériver le séquent $F \wedge G \Rightarrow G \wedge F$ à partir des règles d'inférence précédentes.

$$\dfrac{\dfrac{}{F \wedge G \vdash F \wedge G}\,ax}{F \wedge G \vdash G}\,\wedge_{e_d} \qquad \dfrac{\dfrac{}{F \wedge G \vdash F \wedge G}\,ax}{F \wedge G \vdash F}\,\wedge_{e_g}$$

Exemple : $F \wedge G \Rightarrow G \wedge F$ est un théorème
Montrons que l'on peut dériver le séquent $F \wedge G \Rightarrow G \wedge F$ à partir des règles d'inférence précédentes.

$$\dfrac{\dfrac{\dfrac{}{F \wedge G \vdash F \wedge G}\,ax}{F \wedge G \vdash G}\,\wedge_{e_d} \qquad \dfrac{\dfrac{}{F \wedge G \vdash F \wedge G}\,ax}{F \wedge G \vdash F}\,\wedge_{e_g}}{F \wedge G \vdash G \wedge F}\,\wedge_i$$

Exemple : $F \wedge G \Rightarrow G \wedge F$ est un théorème
Montrons que l'on peut dériver le séquent $F \wedge G \Rightarrow G \wedge F$ à partir des règles d'inférence précédentes.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{F \wedge G \vdash F \wedge G}\,ax}{F \wedge G \vdash G}\,\wedge_{e_d} \qquad \dfrac{\dfrac{}{F \wedge G \vdash F \wedge G}\,ax}{F \wedge G \vdash F}\,\wedge_{e_g}}{F \wedge G \vdash G \wedge F}\,\wedge_i}{\vdash (F \wedge G) \Rightarrow (G \wedge F)}\,\Rightarrow_i$$

Exemple : $F \wedge G \Rightarrow G \wedge F$ est un théorème
Montrons que l'on peut dériver le séquent $F \wedge G \Rightarrow G \wedge F$ à partir des règles d'inférence précédentes.

Il peut être plus facile de construire la dérivation *en remontant* (en chaînage arrière).

Exemple : $F \wedge G \Rightarrow G \wedge F$ est un théorème
Montrons que l'on peut dériver le séquent $F \wedge G \Rightarrow G \wedge F$ à partir des règles d'inférence précédentes.

Il peut être plus facile de construire la dérivation *en remontant* (en chaînage arrière).

$$\frac{}{\vdash (F \wedge G) \Rightarrow (G \wedge F)} \Rightarrow_i$$

Exemple : $F \wedge G \Rightarrow G \wedge F$ est un théorème
Montrons que l'on peut dériver le séquent $F \wedge G \Rightarrow G \wedge F$ à partir des règles d'inférence précédentes.

Il peut être plus facile de construire la dérivation *en remontant* (en chaînage arrière).

$$\dfrac{\dfrac{}{F \wedge G \vdash G \wedge F}\wedge_i}{\vdash (F \wedge G) \Rightarrow (G \wedge F)}\Rightarrow_i$$

Exemple : $F \wedge G \Rightarrow G \wedge F$ est un théorème
Montrons que l'on peut dériver le séquent $F \wedge G \Rightarrow G \wedge F$ à partir des règles d'inférence précédentes.

Il peut être plus facile de construire la dérivation *en remontant* (en chaînage arrière).

$$\dfrac{\dfrac{\dfrac{}{F \wedge G \vdash G}\wedge_{e_d}}{F \wedge G \vdash G \wedge F}\wedge_i}{\vdash (F \wedge G) \Rightarrow (G \wedge F)}\Rightarrow_i$$

Exemple : $F \wedge G \Rightarrow G \wedge F$ est un théorème
Montrons que l'on peut dériver le séquent $F \wedge G \Rightarrow G \wedge F$ à partir des règles d'inférence précédentes.

Il peut être plus facile de construire la dérivation *en remontant* (en chaînage arrière).

$$\dfrac{\dfrac{\dfrac{}{F \wedge G \vdash F \wedge G}\,ax}{F \wedge G \vdash G}\,\wedge_{e_d}}{F \wedge G \vdash G \wedge F}\,\wedge_i$$
$$\dfrac{}{\vdash (F \wedge G) \Rightarrow (G \wedge F)}\,\Rightarrow_i$$

Exemple : $F \wedge G \Rightarrow G \wedge F$ est un théorème
Montrons que l'on peut dériver le séquent $F \wedge G \Rightarrow G \wedge F$ à partir des règles d'inférence précédentes.

Il peut être plus facile de construire la dérivation *en remontant* (en chaînage arrière).

$$\dfrac{\dfrac{\dfrac{\dfrac{}{F \wedge G \vdash F \wedge G}\,ax}{F \wedge G \vdash G}\,\wedge_{e_d} \qquad \dfrac{\dfrac{}{F \wedge G \vdash F \wedge G}\,ax}{F \wedge G \vdash F}\,\wedge_{e_g}}{F \wedge G \vdash G \wedge F}\,\wedge_i}{\vdash (F \wedge G) \Rightarrow (G \wedge F)}\,\Rightarrow_i$$

Exemple : $F \wedge G \Rightarrow G \wedge F$ est un théorème
Montrons que l'on peut dériver le séquent $F \wedge G \Rightarrow G \wedge F$ à partir des règles d'inférence précédentes.

Il peut être plus facile de construire la dérivation *en remontant* (en chaînage arrière).

$$\dfrac{\dfrac{\dfrac{\dfrac{}{F \wedge G \vdash F \wedge G}\,ax}{F \wedge G \vdash G}\,\wedge_{e_d} \qquad \dfrac{\dfrac{}{F \wedge G \vdash F \wedge G}\,ax}{F \wedge G \vdash F}\,\wedge_{e_g}}{F \wedge G \vdash G \wedge F}\,\wedge_i}{\vdash (F \wedge G) \Rightarrow (G \wedge F)}\,\Rightarrow_i$$

Encore un autre exemple : démontrons que $(F \Rightarrow G) \Rightarrow F \Rightarrow G$ est un théorème.

Encore un autre exemple : démontrons que $(F \Rightarrow G) \Rightarrow F \Rightarrow G$ est un théorème.

$$\dfrac{}{\vdash (F \Rightarrow G) \Rightarrow (F \Rightarrow G)} \Rightarrow_i$$

Encore un autre exemple : démontrons que $(F \Rightarrow G) \Rightarrow F \Rightarrow G$ est un théorème.

$$\dfrac{\dfrac{}{(F \Rightarrow G) \vdash F \Rightarrow G}\,ax}{\vdash (F \Rightarrow G) \Rightarrow (F \Rightarrow G)}\,\Rightarrow_i$$

Encore un autre exemple : démontrons que $(F \Rightarrow G) \Rightarrow F \Rightarrow G$ est un théorème.

$$\dfrac{\dfrac{}{(F \Rightarrow G) \vdash F \Rightarrow G}\,ax}{\vdash (F \Rightarrow G) \Rightarrow (F \Rightarrow G)}\,\Rightarrow_i$$

ou encore

Encore un autre exemple : démontrons que $(F \Rightarrow G) \Rightarrow F \Rightarrow G$ est un théorème.

$$\dfrac{\dfrac{}{(F \Rightarrow G) \vdash F \Rightarrow G}\,ax}{\vdash (F \Rightarrow G) \Rightarrow (F \Rightarrow G)}\,\Rightarrow_i$$

ou encore

$$\dfrac{\dfrac{}{(F \Rightarrow G) \vdash F \Rightarrow G}\,\Rightarrow_i}{\vdash (F \Rightarrow G) \Rightarrow (F \Rightarrow G)}\,\Rightarrow_i$$

Encore un autre exemple : démontrons que $(F \Rightarrow G) \Rightarrow F \Rightarrow G$ est un théorème.

$$\dfrac{\dfrac{}{(F \Rightarrow G) \vdash F \Rightarrow G}\,ax}{\vdash (F \Rightarrow G) \Rightarrow (F \Rightarrow G)}\,\Rightarrow_i$$

ou encore

$$\dfrac{\dfrac{\dfrac{}{(F \Rightarrow G), F \vdash G}\,\Rightarrow_e}{(F \Rightarrow G) \vdash F \Rightarrow G}\,\Rightarrow_i}{\vdash (F \Rightarrow G) \Rightarrow (F \Rightarrow G)}\,\Rightarrow_i$$

Encore un autre exemple : démontrons que $(F \Rightarrow G) \Rightarrow F \Rightarrow G$ est un théorème.

$$\dfrac{\dfrac{}{(F \Rightarrow G) \vdash F \Rightarrow G}\,ax}{\vdash (F \Rightarrow G) \Rightarrow (F \Rightarrow G)}\,\Rightarrow_i$$

ou encore

$$\dfrac{\dfrac{\dfrac{}{F \Rightarrow G, F \vdash F \Rightarrow G}\,ax}{(F \Rightarrow G), F \vdash G}\,\Rightarrow_e}{(F \Rightarrow G) \vdash F \Rightarrow G}\,\Rightarrow_i}{\vdash (F \Rightarrow G) \Rightarrow (F \Rightarrow G)}\,\Rightarrow_i$$

Encore un autre exemple : démontrons que $(F \Rightarrow G) \Rightarrow F \Rightarrow G$ est un théorème.

$$\dfrac{\dfrac{}{(F \Rightarrow G) \vdash F \Rightarrow G}\,ax}{\vdash (F \Rightarrow G) \Rightarrow (F \Rightarrow G)}\,\Rightarrow_i$$

ou encore

$$\dfrac{\dfrac{\dfrac{}{F \Rightarrow G, F \vdash F \Rightarrow G}\,ax \qquad \dfrac{}{F \Rightarrow G, F \vdash F}\,ax}{(F \Rightarrow G), F \vdash G}\,\Rightarrow_e}{(F \Rightarrow G) \vdash F \Rightarrow G}\,\Rightarrow_i}{\vdash (F \Rightarrow G) \Rightarrow (F \Rightarrow G)}\,\Rightarrow_i$$

Encore un autre exemple : démontrons que $(F \Rightarrow G) \Rightarrow F \Rightarrow G$ est un théorème.

$$\dfrac{\dfrac{}{(F \Rightarrow G) \vdash F \Rightarrow G}\,ax}{\vdash (F \Rightarrow G) \Rightarrow (F \Rightarrow G)}\,\Rightarrow_i$$

ou encore

$$\dfrac{\dfrac{\dfrac{}{F \Rightarrow G, F \vdash F \Rightarrow G}\,ax \qquad \dfrac{}{F \Rightarrow G, F \vdash F}\,ax}{(F \Rightarrow G), F \vdash G}\,\Rightarrow_e}{(F \Rightarrow G) \vdash F \Rightarrow G}\,\Rightarrow_i}{\vdash (F \Rightarrow G) \Rightarrow (F \Rightarrow G)}\,\Rightarrow_i$$

$\Longrightarrow$ Pas unicité de la preuve d'un séquent

Exercices

Prouver que:

- $\vdash A \vee B \Rightarrow B \vee A$
- $\vdash A \Rightarrow \neg\neg A$

Solutions

$$\dfrac{\dfrac{}{A \vee B \vdash A \vee B} \quad \dfrac{\dfrac{}{A \vee B, A \vdash A}}{A \vee B, A \vdash B \vee A}\ \text{Intro}\ \vee_d \quad \dfrac{\dfrac{}{A \vee B, B \vdash B}}{A \vee B, B \vdash B \vee A}\ \text{Intro}\ \vee_g}{\dfrac{A \vee B \vdash B \vee A}{\vdash A \vee B \Rightarrow B \vee A}\ \text{Intro}\ \Rightarrow}\ \text{Elim}\ \vee$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A, \neg A \vdash A} \quad \dfrac{}{A, \neg A \vdash \neg A}}{A, \neg A \vdash \bot}\ \text{Elim}\ \neg}{A \vdash \neg\neg A}\ \text{Intro}\ \neg}{\vdash A \Rightarrow \neg\neg A}\ \text{Intro}\ \Rightarrow$$

Règles dérivées

Quand on doit démontrer des résulats sur le ssytème d'inférence (apr exempel sa correction), c'est un atout d'avoir un petit nombre de règles. Les règles précédentes sont élémentaires, si on utilise que celles-ci dans les démonstrations, ces dernières peuvent être longues.

On peut introduire des règles dérivées (des utilitaires) qui vont permettre de raccourcir les preuves.

Une règle dérivée se démontre à l'aide des règles de base (ou d'autres règles dérivées déjà démontrées).

Pour démontrer une règle dérivée, on doit exhiber un arbre de dérivation dont la racine est le séquent conclusion de la règle dérivée et les feuilles non fermées (non instances d'axiomes) les prémisses de la règle dérivée.

Exemple : la coupure

$$\frac{H, A \vdash B \quad H \vdash A}{H \vdash B}\,cut$$

Démonstration

$$\dfrac{\dfrac{H, A \vdash B}{H \vdash A \Rightarrow B}\Rightarrow_i \quad H \vdash A}{H \vdash B}\Rightarrow_e$$

Exemple : manipuler les hypothèses

Pour *casser* un $\wedge$ dans une hypothèse

$$\frac{H, A, B \vdash C}{H, A \wedge B \vdash C}$$

Démonstration : au tableau.

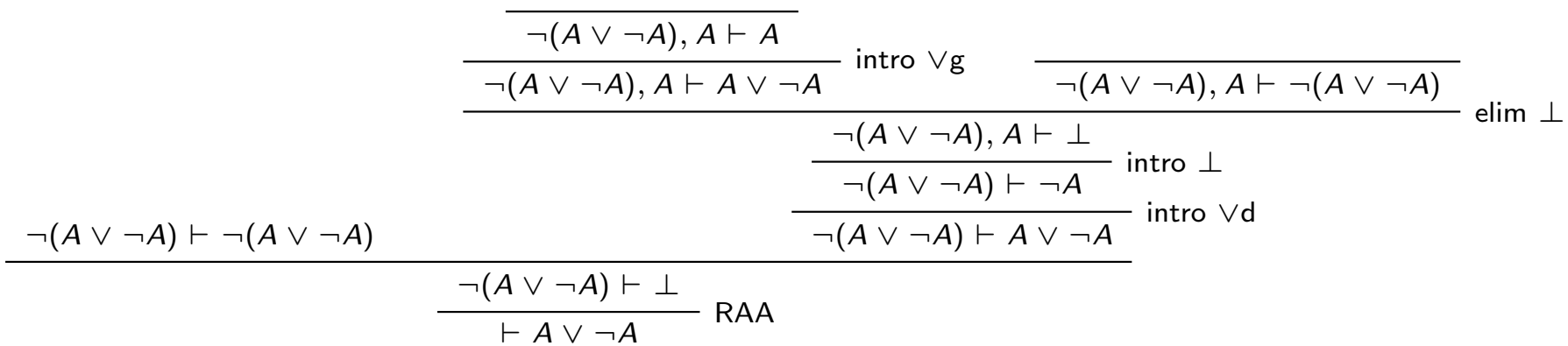
Exercices

1. $\vdash \neg\neg\neg A \Rightarrow A$
2. $\vdash A \vee \neg A$
3. $\vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A$

Solution I

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\neg A, \neg A \vdash \neg\neg A} \quad \dfrac{}{\neg\neg A, \neg A \vdash \neg A}}{\neg\neg A, \neg A \vdash \bot}\ \text{elim } \neg}{\neg\neg A \vdash A}\ \text{RAA}}{\vdash \neg\neg A \Rightarrow A}\ \text{intro } \Rightarrow$$

Solution II


¬(A ∨ ¬A), A ⊢ A
¬(A ∨ ¬A), A ⊢ A ∨ ¬A
intro ∨g
¬(A ∨ ¬A), A ⊢ ¬(A ∨ ¬A)
elim ⊥
¬(A ∨ ¬A), A ⊢ ⊥
intro ⊥
¬(A ∨ ¬A) ⊢ ¬A
intro ∨d
¬(A ∨ ¬A) ⊢ A ∨ ¬A
¬(A ∨ ¬A) ⊢ ¬(A ∨ ¬A)
¬(A ∨ ¬A) ⊢ ⊥
RAA
⊢ A ∨ ¬A

Solution III

$$\dfrac{\dfrac{\dfrac{}{(A \Rightarrow B) \Rightarrow A, \neg A \vdash \neg A} \qquad \dfrac{\dfrac{\dfrac{}{(A \Rightarrow B) \Rightarrow A, \neg A \vdash (A \Rightarrow B) \Rightarrow A} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, \neg A, A \vdash A} \qquad \dfrac{}{\Gamma, \neg A, A \vdash \neg A}}{(A \Rightarrow B) \Rightarrow A, \neg A, A \vdash \bot}\ \text{elim } \neg}{(A \Rightarrow B) \Rightarrow A, \neg A, A \vdash B}\ \text{elim } \bot}{(A \Rightarrow B) \Rightarrow A, \neg A \vdash A \Rightarrow B}\ \text{intro } \Rightarrow}{(A \Rightarrow B) \Rightarrow A, \neg A \vdash A}\ \text{elim } \Rightarrow}{(A \Rightarrow B) \Rightarrow A, \neg A \vdash \bot}\ \text{elim } \bot}{(A \Rightarrow B) \Rightarrow A \vdash A}\ \text{RAA}}{\vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A}\ \text{Intro } \Rightarrow$$

Faire des preuves sur ordinateur

Démonstration avec Coq : voir le TP

On fait la preuve à l'aide tactiques : certaines correspondent directement à des règles de la déduction naturelle, d'autres sont des règles dérivées.

Correction et complétude

Lien entre sémantique et raisonnement.
Lien entre sémantique et raisonnement.

Théorème d'adéquation/correction

Si $\vdash A$ alors $\models A$

Théorème de complétude

Si $\models A$ alors $\vdash A$

Théorème de la déduction

$A \vdash B$ ssi $\vdash A \Rightarrow B$

Quelques cas de la preuve de correction

On démontre un théorème plus général : si $H \vdash A$ alors $H \models A$
Démonstration par induction sur la forme de la démonstration $H \vdash A$ (autant de cas qu'il y a de règles d'inférence de base).

• Cas 1 : La démonstration $H \vdash A$ est une instance de ax

On en déduit que $A \in H$.
Soit I une interprétation qui satisfait H. Il faut montrer que I satisfait A.
I satisfait H, donc I satisfait toutes les formules de H donc en particulier A, cqfd.

• Cas 2 : La démonstration $H \vdash A$ est une instance de $\wedge_i$

On en déduit que A est de la forme $F \wedge G$ et que l'on a une preuve de $H \vdash F$ et une preuve de $H \vdash G$.
Les hypothèses de récurrence sont : (hyp1) $H \models F$ et (hyp2) $H \models G$.
Soit I une interprétation qui satisfait H. Il faut montrer que I satisfait $F \wedge G$.
I satisfait H, donc I satisfait F (d'après hyp1) et I satisfait G (d'après hyp2). Et donc I satisfait $F \wedge G$ cqfd.

• Cas 3 : La démonstration $H \vdash A$ est une instance de $\Rightarrow_e$

On en déduit qu'il existe une proposition G telle que l'on a une preuve de $H \vdash G \Rightarrow A$ et une preuve de $H \vdash G$. *(C'est ici que c'était faux au tableau)*.

Les hypothèses de récurrence sont : (hyp1) $H \models G \Rightarrow A$ et (hyp2) $H \models G$.

Soit I une interprétation qui satisfait H. Il faut montrer que I satisfait A.

I satisfait H, donc I satisfait $G \Rightarrow A$ (d'après hyp1) et I satisfait G (d'après hyp2). Et donc I satisfait A (définition de la vérité de $\Rightarrow$)cqfd.

etc.