

LIFLC – Logique classique

Tactiques Coq et déduction naturelle

Licence informatique UCBL – Automne 2018–2019

Résumé

On montre le lien entre les tactiques Coq et les règles d'inférence de la déduction naturelle.

L'idée générale est qu'une tactique de Coq sur un but correspond à l'utilisation d'une règle de la déduction naturelle *lue de bas en haut*, c'est-à-dire qu'on réécrit le but de Coq en un ou plusieurs autres.

Dans chacune des sections suivantes, on va s'intéresser à un connecteur logique (\Rightarrow , \wedge , \vee , \neg) et voir quelles tactiques Coq correspondent aux règles de déduction naturelle d'*introduction* et d'*élimination*.

Pour l'utilisation de tactiques sur les hypothèses (appelée aussi le contexte, noté Γ dans les règles) dans Coq, l'équivalence avec les règles d'élimination est un peu moins immédiate, on montrera alors que les règles de Coq sont correctes (on dit *admissibles*).

Table des matières

1 Règles Coq de l'axiome	2
2 Règles Coq de l'implication	2
2.1 Introduction de l'implication	2
2.2 Utilisation de l'implication en hypothèse	2
3 Règles Coq de la négation	3
4 Règles Coq de la disjonction	3
4.1 Introduction de la disjonction	3
4.2 Destruction de disjonction en hypothèse	4
5 Règles Coq de la conjonction	5
5.1 Introduction de la conjonction	5
5.2 Destruction de conjonction en hypothèse	5
6 Un exemple de preuve en Coq et en déduction naturelle	6
6.1 La preuve en Coq	6
6.2 La preuve en déduction naturelle	6

1 Règles Coq de l'axiome

Supposant qu'on a une preuve de A , nommons la H , alors, si on cherche à prouver que A , on peut simplement donner H et terminer la preuve : c'est ce que vont faire les tactiques `assumption` ou `trivial`.

Ces tactiques correspondent directement à la règle d'inférence (ax) : comme cette règle n'a pas d'hypothèse, alors la preuve du but est terminée et Coq affiche `No more subgoals`.

```
H : A
----- (1/1)
A
```

No more subgoals.

$$\frac{}{\Gamma, A \vdash A} (ax)$$

Règle d'inférence (ax)

Tactique `assumption`

2 Règles Coq de l'implication

2.1 Introduction de l'implication

La tactique `intros H0 H1 ...` correspond directement à la règle (\Rightarrow_i)

```
..... (1/1)
A -> B
```

```
...
HA : A
----- (1/1)
B
```

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

Règle d'inférence (\Rightarrow_i)

`intros HA`

2.2 Utilisation de l'implication en hypothèse

La tactique `apply H` correspond presque à la règle (\Rightarrow_e). La règle de Coq n'est pas une règle de la déduction naturelle, par contre, on peut prouver que cette nouvelle règle, nommons-la ($\Gamma \Rightarrow$), est correcte, car toute preuve qui l'utilise peut être réécrite en utilisant uniquement des règles de la

déduction naturelle.

$$\begin{array}{c} \dots \\ H : A \rightarrow B \\ \hline B \end{array} (1/1)$$

$$\begin{array}{c} \dots \\ H : A \rightarrow B \\ \hline A \end{array} (1/1)$$

$$\frac{\Gamma, A \Rightarrow B \vdash A}{\Gamma, A \Rightarrow B \vdash B} (\Gamma \Rightarrow)$$

Règle d'inférence associée

apply H

Correction de la règle $(\Gamma \Rightarrow)$.

$$\frac{\frac{}{\Gamma, A \Rightarrow B \vdash A \Rightarrow B} (ax) \quad \Gamma, A \Rightarrow B \vdash A}{\Gamma, A \Rightarrow B \vdash B} (\Rightarrow_e)$$

□

3 Règles Coq de la négation

En Coq, la négation n'est pas un constructeur primitif, $\neg A$ est en fait simplement un alias pour la formule (classiquement équivalente) $A \Rightarrow \perp$. On peut donc réécrire les deux formules avec les tactiques `fold` et `unfold` et ensuite utiliser les tactiques de l'implication. Ce comportement correspond à la règle (\neg_i)

$$\begin{array}{c} \dots \\ \hline \sim A \end{array} (1/1)$$

$$\begin{array}{c} \dots \\ \hline \sim A \end{array} (1/1)$$

$$\begin{array}{c} \dots \\ \hline A \rightarrow \text{False} \end{array} (1/1)$$

$$\begin{array}{c} \dots \\ HA : A \\ \hline \text{False} \end{array} (1/1)$$

unfold not

intro HA

4 Règles Coq de la disjonction

4.1 Introduction de la disjonction

Dans Coq, pour prouver que $A \vee B$, il faut être soit capable de prouver A , soit être capable de prouver B . On a donc une tactique pour choisir quel membre on veut prouver, ces tactiques sont `left` et `right`. Elles correspondent directement aux règles (\vee_e^g) et (\vee_e^d) lue à l'envers.

...
 ----- (1/1)
 A \wedge B

...
 ----- (1/1)
 A

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} (\vee_e^g)$$

Règle d'inférence (\vee_e^g)

left

...
 ----- (1/1)
 A \wedge B

...
 ----- (1/1)
 B

$$\frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} (\vee_e^d)$$

Règle d'inférence (\vee_e^d)

right

4.2 Destruction de disjonction en hypothèse

On utilise la tactique `destruct H` où `H` est une hypothèse de la forme $A \vee B$ qui va générer deux sous buts avec la même conclusion :

1. le premier est à prouver à partir d'un contexte où on a une preuve de A
2. le second est à prouver à partir d'un contexte où on a une preuve de B

On peut utiliser `destruct H as [HA | HB]` si on veut nommer les nouvelles hypothèses.

La règle d'inférence utilisée par Coq réécrit le contexte courant Γ . Ce n'est pas une règle de la déduction naturelle, mais elle est assez directe à prouver.

...
 H : A \wedge B
 ----- (1/1)
 C

...
 H : A \wedge B
 HA : A
 ----- (1/2)
 C
 ----- (2/2)
 C

...
 H : A \wedge B
 HB : B
 ----- (2/2)
 C

$$\frac{\Gamma, A \vee B, A \vdash C \quad \Gamma, A \vee B, B \vdash C}{\Gamma, A \vee B \vdash C} (\Gamma \vee)$$

Règle d'inférence associée

`destruct H as [HA | HB]`

Correction de la règle ($\Gamma \vee$).

$$\frac{\overline{\Gamma, A \vee B \vdash A \vee B}^{(ax)} \quad \Gamma, A \vee B, A \vdash C \quad \Gamma, A \vee B, B \vdash C}{\Gamma, A \vee B \vdash C} (\vee_e)$$

□

5 Règles Coq de la conjonction

5.1 Introduction de la conjonction

On utilise la tactique `split` sur le but $A \wedge B$ qui va générer deux sous buts avec les mêmes hypothèses que celles de départ :

1. dans le premier il faut prouver que A
2. dans le second il faut prouver que B
- ...

----- (1/1)
A /\ B

...
----- (1/2)
A

----- (2/2)
B

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} (\wedge_i)$$

Règle d'inférence (\wedge_i)

`split`

5.2 Destruction de conjonction en hypothèse

On utilise la tactique `destruct H` où H est une hypothèse de la forme $A \wedge B$ qui va générer un seul sous but, mais où le contexte contient désormais une preuve de A et une preuve de B . La tactique `destruct` a le même effet que `elim`; `intros`.

On peut utiliser `destruct H as [HA HB]` si on veut nommer les nouvelles hypothèses. Similairement, on montre que la règle d'inférence de Coq, nommons-la ($\Gamma \wedge$), peut être obtenue par la déduction naturelle. Ici la preuve de la règle ($\Gamma \wedge$) est un peu moins directe.

...
H : A /\ B
----- (1/1)
C

...
H : A /\ B
HA : A
HB : B
----- (1/1)
C

$$\frac{\Gamma, A \wedge B, A, B \vdash C}{\Gamma, A \wedge B \vdash C} (\Gamma \wedge)$$

Règle d'inférence associée

`destruct H as [HA HB]`

Correction de la règle ($\Gamma \wedge_i$).

$$\frac{\frac{\frac{\Gamma, A \wedge B, A, B \vdash C}{\Gamma, A \wedge B, A \vdash B \Rightarrow C} (\Rightarrow_i) \quad \frac{\Gamma, A \wedge B \vdash A \wedge B}{\Gamma, A \wedge B \vdash A} (\wedge_e^g) \quad \frac{\Gamma, A \wedge B, A, B \vdash C}{\Gamma, A \wedge B \vdash A \wedge B} (ax)}{\Gamma, A \wedge B \vdash B \Rightarrow C} (\Rightarrow_e) \quad \frac{\Gamma, A \wedge B \vdash A \wedge B}{\Gamma, A \wedge B \vdash B} (\wedge_e^d)}{\Gamma, A \wedge B \vdash C} (\Rightarrow_e)$$

□

6 Un exemple de preuve en Coq et en déduction naturelle

On va prouver la tautologie $\neg(P \vee Q) \Rightarrow (\neg P \wedge \neg Q)$ qui fait intervenir tous les connecteurs.

6.1 La preuve en Coq

Hypothesis P Q R: Prop.

Theorem not_or_implies_and_not : $\sim(P \vee Q) \rightarrow (\sim P \wedge \sim Q)$.

Proof.

intros H.

split. (* on prouve " $\sim P \wedge \sim Q$ " en prouvant chaque sous-but *)

- (* le sous-but " $\sim P$ " *)

intros Hp.

apply H.

left.

assumption.

- (* le sous-but " $\sim Q$ " *)

intros Hp.

apply H.

right.

assumption.

Qed.

6.2 La preuve en déduction naturelle

On montre ici une preuve en déduction naturelle qui mime le plus fidèlement possible la preuve Coq. La branche de droite qui prouve que $\neg(P \vee Q) \vdash \neg Q$ est similaire à celle de gauche. Les ... en fin de preuve sont là pour éviter de répéter le contexte $\neg(P \vee Q), P, (P \vee Q)$.

$$\frac{\frac{\frac{\overline{\dots \vdash P \vee Q} \text{ (ax)}}{\neg(P \vee Q), P, (P \vee Q) \vdash \perp} (\perp_i)}{\neg(P \vee Q), P \vdash (P \vee Q) \Rightarrow \perp} (\Rightarrow_i)}{\frac{\frac{\overline{\dots \vdash \neg(P \vee Q)} \text{ (ax)}}{\neg(P \vee Q), P \vdash P} \text{ (ax)}}{\neg(P \vee Q), P \vdash P \vee Q} (\vee_i^g)}{\neg(P \vee Q), P \vdash \perp} (\neg_i)} (\Rightarrow_e)}{\frac{\frac{\neg(P \vee Q), P \vdash \perp}{\neg(P \vee Q) \vdash \neg P} (\neg_i)}{\neg(P \vee Q) \vdash \neg P \wedge \neg Q} (\wedge_i)}{\vdash \neg(P \vee Q) \Rightarrow (\neg P \wedge \neg Q)} (\Rightarrow_i)} \text{ cf. branche gauche } (\neg_i)$$

On voit ici que la fin de la preuve est un peu laborieuse avec la gestion de la négation. Pour plus de parallélisme avec Coq, on pourrait prouver la règle suivante $(\Gamma \neg)$ qui correspond à `apply H` et `simplifier`.

$$\frac{\frac{\frac{\overline{\Gamma \vdash A}}{\Gamma, \neg A \vdash \perp} (\Gamma \neg)}{\frac{\overline{\neg(P \vee Q), P \vdash P} \text{ (ax)}}{\neg(P \vee Q), P \vdash P \vee Q} (\vee_i^g)}{\neg(P \vee Q), P \vdash \perp} (\neg_i)}{\neg(P \vee Q) \vdash \neg P} (\neg_i)}{\frac{\frac{\overline{\neg(P \vee Q), Q \vdash Q} \text{ (ax)}}{\neg(P \vee Q), Q \vdash P \vee Q} (\vee_i^d)}{\neg(P \vee Q), Q \vdash \perp} (\neg_i)}{\neg(P \vee Q) \vdash \neg Q} (\neg_i)} (\wedge_i)}{\frac{\neg(P \vee Q) \vdash (\neg P \wedge \neg Q)}{\vdash \neg(P \vee Q) \Rightarrow (\neg P \wedge \neg Q)} (\Rightarrow_i)}$$

$$\frac{}{\Gamma, A \vdash A} \text{ (ax)}$$

Axiome

$$\frac{\Gamma \vdash A}{\Gamma, B \vdash A} \text{ (aff)}$$

Affaiblissement

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \text{ (\Rightarrow}_i\text{)}$$

$$\frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \text{ (\Rightarrow}_e\text{)}$$

Règles pour \Rightarrow

$$\frac{\Gamma \vdash A \Rightarrow \perp}{\Gamma \vdash \neg A} \text{ (\neg}_i\text{)}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash \neg A}{\Gamma \vdash \perp} \text{ (\neg}_e\text{)}$$

$$\frac{\Gamma, \neg A \vdash \perp}{\Gamma \vdash A} \text{ (\neg}_c\text{)}$$

Règles pour \neg et \perp

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \text{ (\wedge}_i\text{)}$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \text{ (\wedge}_e^g\text{)}$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \text{ (\wedge}_e^d\text{)}$$

Règles pour \wedge

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \text{ (\vee}_i^g\text{)}$$

$$\frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \text{ (\vee}_i^d\text{)}$$

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \text{ (\vee}_e\text{)}$$

Règles pour \vee

FIGURE 1 – Règles de la déduction naturelle