

LIFLC – Logique classique

Tactiques Coq et déduction naturelle

Licence informatique UCBL – Automne 2017–2018

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 d'introduction *lue de bas en haut*, c'est-à-dire qu'on réécrit le but de Coq en un ou plusieurs autres.

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, mais on peut montrer que les règles de Coq sont correctes.

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
```

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

No more subgoals.

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
```

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

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

Règle d'inférence (\Rightarrow_i)

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 $(\Gamma \Rightarrow)$.

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

□

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.

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

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

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

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

`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 ($\Gamma \wedge_i$).

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

□