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

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.
```

Tactique `assumption`

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

Règle d'inférence (ax)

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
```

`intros HA`

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

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.

```
...
H : A -> B
____________(1/1)
B
```

```
...
H : A -> B
____________(1/1)
A
```

apply H

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

Règle d'inférence associée

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

$$\dfrac{\dfrac{}{\Gamma, A \Rightarrow B \vdash A \Rightarrow B}\ (ax) \qquad \Gamma, A \Rightarrow B \vdash A}{\Gamma, A \Rightarrow B \vdash B}\ (\Rightarrow_e)$$

□

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) $A \Rightarrow \bot$. 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 ($\neg_i$)

```
...
____________(1/1)
~A
```

```
...
____________(1/1)
A -> False
```

unfold not

```
...
____________(1/1)
~A
```

```
...
HA : A
____________(1/1)
False
```

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 \/ 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 \/ 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 \/ B
____________(1/1)
C
```

```
...
H : A \/ B
HA : A
____________(1/2)
C
____________(2/2)
C
```

```
...
H : A \/ B
HB : B
____________(2/2)
C
```

`destruct H as [HA | HB]`

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

Règle d'inférence associée

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

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

□

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 $(\Gamma\wedge_i)$.

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

□

6 Règles `Coq` pour le quantificateur universel

6.1 Introduction du quantificateur universel

La tactique `intros x` correspond directement à la règle $(\forall_i)$.

```
...
____________(1/1)
forall x: nat, A

...
x: nat
____________(1/1)
A
```

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x\ A}\ (\forall_i) \text{ si } x \notin FV(\Gamma)$$

Règle d'inférence $(\forall_i)$

7 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.

7.1 La preuve en `Coq`

```
Hypothesis P Q R: Prop.

Theorem not_or_implies_and_not : ~(P \/ Q) -> (~P /\ ~Q).
Proof.
intros H.
split. (* on prouve " (~P /\ ~Q)" en prouvant chaque sous-but *)
- (* le sous-but "~P" *)
  intros Hp.
  apply H.
  left.
  assumption.
- (* le sous-but "~Q" *)
  intros Hp.
  apply H.
  right.
  assumption.
Qed.
```

7.2 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 $\neg(P \vee Q), P, (P \vee Q)$.

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{(ax)}
\UnaryInfC{$\ldots \vdash P \vee Q$}
\AxiomC{}
\RightLabel{(ax)}
\UnaryInfC{$\ldots \vdash \neg(P \vee Q)$}
\RightLabel{$(\bot_i)$}
\BinaryInfC{$\neg(P \vee Q), P, (P \vee Q) \vdash \bot$}
\RightLabel{$(\Rightarrow_i)$}
\UnaryInfC{$\neg(P \vee Q), P \vdash (P \vee Q) \Rightarrow \bot$}
\AxiomC{}
\RightLabel{(ax)}
\UnaryInfC{$\neg(P \vee Q), P \vdash P$}
\RightLabel{$(\vee_i^g)$}
\UnaryInfC{$\neg(P \vee Q), P \vdash P \vee Q$}
\RightLabel{$(\Rightarrow_e)$}
\BinaryInfC{$\neg(P \vee Q), P \vdash \bot$}
\RightLabel{$(\neg_i)$}
\UnaryInfC{$\neg(P \vee Q) \vdash \neg P$}
\AxiomC{cf. branche gauche}
\RightLabel{$(\neg_i)$}
\UnaryInfC{$\neg(P \vee Q) \vdash \neg Q$}
\RightLabel{$(\wedge_i)$}
\BinaryInfC{$\neg(P \vee Q) \vdash (\neg P \wedge \neg Q)$}
\RightLabel{$(\Rightarrow_i)$}
\UnaryInfC{$\vdash \neg(P \vee Q) \Rightarrow (\neg P \wedge \neg Q)$}
\end{prooftree}
$$

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.

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

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg(P \vee Q), P \vdash P}\ (ax)}{\neg(P \vee Q), P \vdash P \vee Q}\ (\vee_i^g)}{\neg(P \vee Q), P \vdash \bot}\ (\Gamma\neg)}{\neg(P \vee Q) \vdash \neg P}\ (\neg_i) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\neg(P \vee Q), Q \vdash Q}\ (ax)}{\neg(P \vee Q), Q \vdash P \vee Q}\ (\vee_i^d)}{\neg(P \vee Q), Q \vdash \bot}\ (\Gamma\neg)}{\neg(P \vee Q) \vdash \neg Q}\ (\neg_i)}{\dfrac{\neg(P \vee Q) \vdash (\neg P \wedge \neg Q)}{\vdash \neg(P \vee Q) \Rightarrow (\neg P \wedge \neg Q)}\ (\Rightarrow_i)}\ (\wedge_i)$$

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

Axiome

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

Affaiblissement

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

Règles pour $\Rightarrow$

$$\frac{\Gamma \vdash A \Rightarrow \bot}{\Gamma \vdash \neg A}\ (\neg_i) \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash \neg A}{\Gamma \vdash \bot}\ (\neg_e) \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ (\neg_c)$$

Règles pour $\neg$ et $\bot$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ (\wedge_i) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ (\wedge_e^g) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ (\wedge_e^d)$$

Règles pour $\wedge$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ (\vee_i^g) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ (\vee_i^d) \qquad \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\ (\vee_e)$$

Règles pour $\vee$

FIGURE 1 – Règles de la déduction naturelle