Déduction Naturelle au premier ordre : Tactiques, Cohérence

Benjamin Wack

Université Grenoble Alpes

Avril 2022

Plan

Plan

Rappel : Règles « propositionnelles »

Table 3.1

Introduction	Élimination
$\dfrac{\begin{array}{c}[A] \\ \vdots \\ B\end{array}}{A \Rightarrow B} \Rightarrow I$	$\dfrac{A \quad A \Rightarrow B}{B} \Rightarrow E$
$\dfrac{A \quad B}{A \wedge B} \wedge I$	$\dfrac{A \wedge B}{A} \wedge E1$ $\dfrac{A \wedge B}{B} \wedge E2$
$\dfrac{A}{A \vee B} \vee I1$ $\dfrac{A}{B \vee A} \vee I2$	$\dfrac{A \vee B \quad A \Rightarrow C \quad B \Rightarrow C}{C} \vee E$
Règle du faux	
$\dfrac{\bot}{A}\ Efq$	
Réduction à l'absurde	
$\dfrac{\neg\neg A}{A}\ RAA$	

Récapitulatif des règles des quantificateurs : Tableau 6.1

$\dfrac{A}{\forall x A}$	$\forall I$	x ne doit être libre ni dans l'environnement, ni dans le contexte
$\dfrac{\forall x A}{A{<}x{:=}t{>}}$	$\forall E$	t est libre pour x dans A
$\dfrac{A{<}x{:=}t{>}}{\exists x A}$	$\exists I$	t est libre pour x dans A
$\dfrac{\exists x A \qquad (A \Rightarrow B)}{B}$	$\exists E$	x ne doit être libre ni dans l'environnement, ni dans le contexte, ni dans B.

Règle de la copie

$\dfrac{A'}{A}$	copie	si A est égale à A' au changement près des variables liées.

+ Réflexivité et congruence pour l'égalité

Plan

Tactiques

1. Deux tactiques de preuves :
   - pour la règle $\forall I$
   - pour la règle $\exists E$

2. Pas de tactique pour les règles $\forall E$ et $\exists I$ (ce sont celles qui rendent le système indécidable !)

Cohérence et Complétude

- **Nous montrons la cohérence des règles de ce système.**
- **Nous admettrons sans preuve que ce système est complet.**

  Preuves de complétude pour des systèmes proches :
  - Peter B.Andrews. *An introduction to mathematical logic : to truth through proof*. Academic Press, 1986.
  - Herbert B.Enderton. *A mathematical Introduction to Logic*. Academic Press, 2001.

Plan

Introduction

1. Deux tactiques de preuves pour les règles $\forall I$ et $\exists E$ qui correspondent à des formes de raisonnement mathématique :
   1.1 Raisonner en avant avec une hypothèse d'existence,
   1.2 Raisonner en arrière pour généraliser.

2. Application à un exemple.

Raisonner en avant avec une hypothèse d'existence

Soit Γ un ensemble de formules, x une variable, A et C des formules.

On cherche une preuve de C dans l'environnement $\Gamma, \exists x A$.

Deux cas possibles :

- x n'est libre ni dans Γ, ni dans C.
- x est libre dans Γ ou C.

1[er] cas : x n'est libre ni dans Γ, ni dans C

Dans ce cas, la preuve peut toujours s'écrire :

supposons A	
$\boxed{\text{preuve de } C \text{ dans l'environnement } \Gamma, A}$	
donc $A \Rightarrow C$	$\Rightarrow$I 1,...
C	$\exists$E

$2^{\text{ème}}$ cas : x est libre dans Γ ou C

On choisit une variable y :

- « nouvelle », c'est-à-dire non libre dans Γ, C
- absente de A

puis on se ramène au cas précédent, via la règle de copie.

La preuve s'écrit alors :

$\exists y A < x := y >$	copie de $\exists x A$
supposons $A < x := y >$	
$\boxed{\text{preuve de } C \text{ dans l'environnement } \Gamma, A < x := y >}$	
donc $A < x := y > \Rightarrow C$	$\Rightarrow$I 1,_
C	$\exists$E

Un exemple simple

Prouvons $\exists x P(x) \land \forall x \neg P(x) \Rightarrow \bot$.

1	1	supposons $\exists x P(x) \land \forall x \neg P(x)$	
1	2	$\exists x P(x)$	$\land$E1 1
1	3	$\forall x \neg P(x)$	$\land$E1 1
1,2	4	supposons $P(x)$	
1,2	5	$\neg P(x)$	$\forall$E 3 x
1,2	6	$\bot$	$\Rightarrow$E 4,5
1	7	donc $P(x) \Rightarrow \bot$	
1	8	$\bot$	$\exists$E 2,7
	9	donc $\exists x P(x) \land \forall x \neg P(x) \Rightarrow \bot$	$\Rightarrow$I 1, 8

Remarques

La recherche de la preuve initiale a été réduite à la recherche d'une preuve de la même formule dans un environnement plus simple.

Mode de raisonnement appliqué en mathématiques quand on cherche une preuve d'une formule C avec l'hypothèse $\exists x P(x)$.

Cela revient à introduire une constante « nouvelle » a vérifiant $P(a)$ et à prouver C sous l'hypothèse $P(a)$.

Raisonner en arrière pour généraliser

On cherche une preuve de $\forall x A$ dans l'environnement Γ.

Deux cas possibles :

- x n'est pas libre dans Γ.
- x est libre dans Γ.

1^er cas : x n'est pas libre dans Γ

$$\dfrac{\boxed{\text{preuve de } A \text{ dans l'environnement } \Gamma}}{\forall x A}\ \forall\mathrm{I}$$

2ème cas : x est libre dans Γ

On choisit une variable y :

- « nouvelle », c'est-à-dire non libre dans Γ
- absente de A

puis on se ramène au cas précédent, via la règle de copie.

La preuve s'écrit alors :

preuve de $A < x := y >$ dans l'environnement Γ	
$\forall y A < x := y >$	$\forall$I
$\forall x A$	copie de la formule précédente

Un exemple simple

Prouvons $\forall x P(x) \Rightarrow \forall y P(y)$ sans copie.

1	1	supposons $\forall x P(x)$	
1	2	$P(y)$	$\forall$E 1 y
1	3	$\forall y P(y)$	$\forall$I 2
	4	donc $\forall x P(x) \Rightarrow \forall y P(y)$	$\Rightarrow$I 1, 4

Remarque

La recherche de la preuve initiale a été réduite à la recherche d'une preuve d'une formule plus simple dans le même environnement.

Mode de raisonnement appliqué en mathématiques quand on cherche une preuve de $\forall x P(x)$.

Cela revient à introduire une variable « nouvelle » y et à prouver la formule $P(y)$.
Puis on conclut : puisque le choix de y est arbitraire, on a $\forall x P(x)$.

Un exemple d'application des tactiques

On définit « il existe un et un seul x » (noté en bref $\exists ! x$) par :

- $\exists ! x P(x) \doteq \exists x (P(x) \wedge \forall y (P(y) \Rightarrow x = y))$

En séparant l'existence de x et son unicité, on peut aussi la définir par :

- $\exists ! x P(x) \doteq \exists x P(x) \wedge \forall x \forall y (P(x) \wedge P(y) \Rightarrow x = y)$.

Ces deux définitions sont bien sûr équivalentes : on montre ici formellement que **la première implique la deuxième**.

Comme la preuve est longue, nous allons la décomposer.

6.2.3 Plan de la preuve

$$\exists x(P(x) \land \forall y(P(y) \Rightarrow x = y)) \Rightarrow \exists x P(x) \land \forall x \forall y(P(x) \land P(y) \Rightarrow x = y)$$

On applique les deux tactiques suivantes :

- Pour prouver $A \Rightarrow B$, supposer A et déduire B
- Pour prouver $B_1 \land B_2$, prouver B_1 et prouver B_2.

1	supposons $\exists x(P(x) \land \forall y(P(y) \Rightarrow x = y))$	
1	preuve de $\exists x P(x)$ dans l'environnement 1	
1	preuve de $\forall x \forall y(P(x) \land P(y) \Rightarrow x = y)$ dans l'environnement 1	
1	$\exists x P(x) \land \forall x \forall y(P(x) \land P(y) \Rightarrow x = y)$	$\land$I
	donc $\exists x(P(x) \land \forall y(P(y) \Rightarrow x = y)) \Rightarrow \exists x P(x) \land \forall x \forall y(P(x) \land P(y) \Rightarrow x = y)$	$\Rightarrow$I

6.2.3 Application de la tactique utilisant une hypothèse d'existence

Preuve de $\exists x P(x)$ dans l'environnement
$\exists x (P(x) \wedge \forall y (P(y) \Rightarrow x = y))$

contexte	N°	formule	règle
	i	$\exists x (P(x) \wedge \forall y (P(y) \Rightarrow x = y))$	
1	1	supposons $P(x) \wedge \forall y (P(y) \Rightarrow x = y)$	
1	2	$P(x)$	$\wedge$E1 1
1	3	$\exists x P(x)$	$\exists$I 2, x
	4	donc $P(x) \wedge \forall y (P(y) \Rightarrow x = y) \Rightarrow \exists x P(x)$	$\Rightarrow$I 1,3
	5	$\exists x P(x)$	$\exists$E i, 4

6.2.3 Application de la tactique pour obtenir une conclusion générale : plan de preuve

Preuve de $\forall x \forall y (P(x) \land P(y) \Rightarrow x = y)$
dans l'environnement $\exists x (P(x) \land \forall y (P(y) \Rightarrow x = y))$

On applique les tactiques suivantes :

1. « raisonner en avant en utilisant une hypothèse existentielle »
2. « raisonner en arrière pour obtenir une conclusion générale » (2 fois)
3. Pour prouver $A \Rightarrow B$, supposer A et déduire B

6.2.3 Application de la tactique pour obtenir une conclusion générale : preuve

contexte	N°	formule	règle
	i	$\exists x(P(x) \land \forall y(P(y) \Rightarrow x = y))$	
1	1	supposons $P(x) \land \forall y(P(y) \Rightarrow x = y)$	
1,2	2	supposons $P(u) \land P(y)$	
1,2	3	$\forall y(P(y) \Rightarrow x = y)$	$\land$E2 1
1,2	4	$P(u)$	$\land$E1 2
1,2	5	$P(u) \Rightarrow x = u$	$\forall$E 3, u
1,2	6	$x = u$	$\Rightarrow$E 4, 5
1,2	7	$P(y)$	$\land$E2 2
1,2	8	$P(y) \Rightarrow x = y$	$\forall$E 3, y
1,2	9	$\underline{x} = y$	$\Rightarrow$E 7, 8
1,2	10	$\underline{u} = y$	congruence 6, 9
1	11	donc $P(u) \land P(y) \Rightarrow u = y$	$\Rightarrow$I 2, 10
1	12	$\forall y(P(u) \land P(y) \Rightarrow u = y)$	$\forall$I 11
1	13	$\forall u \forall y(P(u) \land P(y) \Rightarrow u = y)$	$\forall$I 12
1	14	$\forall x \forall y(P(x) \land P(y) \Rightarrow x = y)$	copie de 13
	15	donc $(P(x) \land \forall y(P(y) \Rightarrow x = y)) \Rightarrow \forall x \forall y(P(x) \land P(y) \Rightarrow x = y)$	$\Rightarrow$I 1, 14
	16	$\forall x \forall y(P(x) \land P(y) \Rightarrow x = y)$	$\exists$E i, 15

Conclusion

Toute la difficulté des preuves est donc concentrée dans les règles $\forall$E et $\exists$I :

- dans le raisonnement en avant, il faut trouver les bonnes instanciations des formules commençant par $\forall$
- dans le raisonnement en arrière, il faut trouver la bonne instance permettant de déduire une formule commençant par $\exists$

Plan

Rappel

Nous allons utiliser (encore) deux résultats sur la substitution :

Théorème 4.3.36

Si t est libre pour la variable x dans A, alors

$$[A < x := t >]_{(I,e)} = [A]_{(I,e[x=d])} \quad \text{où } d = [\![t]\!]_{(I,e)}$$

Corollaire 4.3.38

Si t est libre pour la variable x dans A, alors

- $\models \ \forall xA \Rightarrow A < x := t >$
- $\models \ A < x := t > \Rightarrow \exists xA$

Propriétés de la conséquence

Propriété 6.3.1

Si x n'est pas libre dans Γ, alors

$$\Gamma \models A \text{ si et seulement si } \Gamma \models \forall x A$$

Preuve de la propriété 6.3.1

$\Rightarrow$ Supposons que $\Gamma \models A$.

Soit (I, e) une assignation modèle de Γ.

Puisque x n'est pas libre dans Γ, pour <u>tout $d \in D$</u> :
(I, e) et $(I, e[x = d])$ donnent la même valeur aux formules de Γ
donc $(I, e[x = d])$ est modèle de Γ.

Par conséquent $(I, e[x = d])$ est modèle de A pour tout $d \in D$,
donc (I, e) est modèle de $\forall x A$.

$\Leftarrow$ Supposons que $\Gamma \models \forall x A$.
Puisque la formule $\forall x A \Rightarrow A$ est valide (corollaire avec $t = x$),
on a $\Gamma \models A$.

Propriétés de la conséquence

Propriété 6.3.2

Si x n'est libre ni dans Γ, ni dans B, alors :

$$\Gamma \models A \Rightarrow B \text{ si et seulement si } \Gamma \models (\exists x A) \Rightarrow B$$

Preuve de la propriété 6.3.2

$\Rightarrow$ Supposons que $\Gamma \models A \Rightarrow B$. On montre en fait que $\Gamma, \exists xA \models B$.

Soit (I, e) une assignation modèle de Γ.

Supposons que (I, e) est aussi modèle de $\exists xA$.

Ceci signifie que $(I, e[x = d])$ est modèle de A pour un certain $d \in D$.

(I, e) et $(I, e[x = d])$ donnent la même valeur aux formules de Γ (car x non libre dans Γ).

D'où $(I, e[x = d])$ est modèle de $A \Rightarrow B$.

Comme $(I, e[x = d])$ est aussi modèle de A, par conséquent c'est un modèle de B.

Enfin puisque x non libre dans B, $(I, e[x = d])$ et (I, e) donnent la même valeur à B.

$\Leftarrow$ Supposons que $\Gamma \models (\exists xA) \Rightarrow B$, autrement dit $\Gamma, \exists xA \models B$.

Puisque la formule $A \Rightarrow (\exists xA)$ est valide (corollaire avec $t = x$), nous avons $\Gamma, A \models \Gamma, \exists xA \models B$ et donc $\Gamma \models A \Rightarrow B$.

Plan

Cohérence de la déduction

Théorème 6.3.3

Si $\Gamma \vdash A$ (par une preuve en déduction naturelle) alors $\Gamma \models A$.

Plan de la preuve de cohérence

Soit Γ un ensemble de formules. Soit P une preuve de A dans Γ.
Soient C_i la conclusion et H_i le contexte de la i-ème ligne de la preuve P.

Hypothèse de récurrence :
Supposons que pour tout i où $0 < i < k$, on a $\Gamma, H_i \models C_i$.

Montrons que $\Gamma, H_k \models C_k$.

Les cas où $C_k \in \Gamma, H_k$ ou bien est obtenue par une règle propositionnelle ont déjà été traités.
On examine donc uniquement le cas des nouvelles règles.

La règle $\forall$E

Supposons que $C_k = A < x := t >$ a été déduite par la règle $\forall$E.

Par hypothèse de récurrence, il existe $i < k$ tel que $\Gamma, H_i \models \forall x A$.

D'après les conditions de la règle $\forall$E, t est libre pour x dans A.
Donc (**corollaire 4.3.38**), la formule $\forall x A \Rightarrow A < x := t >$ est valide et $\Gamma, H_i \models A < x := t >$.

Puisque la ligne i est utilisable, H_i est préfixe de H_k, donc $\Gamma, H_k \models C_k$.
$\square$

La règle $\exists$I

Supposons que $C_k = \exists x A$ a été déduite par la règle $\exists$I.

Par hypothèse de récurrence, il existe $i < k$ tel que
$\Gamma, H_i \models A < x := t >$

D'après les conditions de la règle $\exists$I, t est libre pour x dans A.
Donc, (**corollaire 4.3.38**), la formule $A < x := t > \Rightarrow \exists x A$ est valide et
$\Gamma, H_i \models \exists x A$.

Puisque la ligne i est utilisable, H_i est préfixe de H_k, donc $\Gamma, H_k \models C_k$.
$\square$

La règle $\forall$I

Supposons que $C_k = \forall x A$ a été déduite par la règle $\forall$I.

Soit $A = C_i$ avec $i < k$, **par hypothèse de récurrence** on a $\Gamma, H_i \models A$.
Soit $A \in \Gamma$ d'où $\Gamma \models A$.

D'après les conditions de la règle $\forall$I, x n'est pas libre dans Γ, H_i.
Donc, **d'après la propriété 6.3.1**, on a aussi $\Gamma, H_i \models \forall x A$.

Puisque la ligne i est utilisable, H_i est préfixe de H_k, donc $\Gamma, H_k \models C_k$.
$\square$

La règle $\exists$E

Supposons que $C_k = B$ a été déduite par la règle $\exists$E, des formules $\exists x A$ et $A \Rightarrow B$.

Par hypothèse de récurrence, il existe $i < k$ et $j < k$ tels que $\Gamma, H_i \models \exists x A$ et $\Gamma, H_j \models A \Rightarrow B$.

D'après les conditions de la règle $\exists$E, x n'est libre ni dans Γ, H_j ni dans B.
Donc, (**propriété 6.3.2**), on a aussi $\Gamma, H_j \models (\exists x A) \Rightarrow B$.

Puisque les lignes i et j sont utilisables, H_i et H_j sont préfixes de H_k, donc $\Gamma, H_k \models \exists x A$ et $\Gamma, H_k \models (\exists x A) \Rightarrow B$.
Par suite $\Gamma, H_k \models C_k$. $\square$

Règle de copie

Supposons que $C_k = A'$ a été déduite par copie de la formule A.

Par hypothèse de récurrence, il existe $i < k$ tel que $\Gamma, H_i \models A$.

On sait que si $A =_\alpha A'$ alors $A \equiv A'$, d'où $\Gamma, H_i \models A'$.

Puisque la ligne i est utilisable, H_i est préfixe de H_k, donc $\Gamma, H_k \models C_k$.
$\square$

Réflexivité

Supposons que C_k est la formule $t = t$ (pour un certain terme t).

On rappelle que l'égalité s'interprète toujours comme $\{(d, d) \mid d \in D\}$ donc en particulier $=_I$ contient toujours $([\![t]\!]_I, [\![t]\!]_I)$.

La formule C_k est donc valide, d'où $\Gamma, H_k \models C_k$. $\square$

Congruence

Supposons que $C_k = A < x := t >$ a été déduite par congruence.

Par hypothèse de récurrence, il existe $i < k$ et $j < k$ tels que $\Gamma, H_i \models s = t$ et $\Gamma, H_j \models A < x := s >$.

Puisque les lignes i et j sont utilisables, H_i et H_j sont préfixes de H_k, donc $\Gamma, H_k \models s = t$ et $\Gamma, H_k \models A < x := s >$.

Les conditions de la règle assurent que s et t libres pour x dans A. On peut donc utiliser :

- $[A < x := s >]_{(I,e)} = [A]_{(I,e[x=d])}$ où $d = [\![s]\!]_{(I,e)}$
- $[A < x := t >]_{(I,e)} = [A]_{(I,e[x=d'])}$ où $d' = [\![t]\!]_{(I,e)}$

De plus l'égalité assure que si (I, e) est modèle de $s = t$ alors d et d' sont le **même** élément de D.

D'où : $s = t, A < x := s > \models A < x := t >$

Par suite $\Gamma, H_k \models C_k$. $\square$

Les théorèmes d'incomplétude de Kurt Gödel (1906-1978)

Premier théorème d'incomplétude (1931)

Tout système logique qui permet de formaliser l'arithmétique permet également d'énoncer :

« *Cet énoncé est indémontrable* ».

- ou bien cet énoncé est faux ; il est donc aussi démontrable, et notre système est incohérent
- ou bien cet énoncé est vrai ; il est donc indémontrable, et notre système est incomplet

Second théorème d'incomplétude

Aucun système logique ne peut démontrer sa propre cohérence.

Plan

Aujourd'hui

- Déduction naturelle au premier ordre :
  - Tactiques
  - Cohérence

Plan du Semestre

- Logique propositionnelle
- Résolution propositionnelle
- Déduction naturelle propositionnelle

PARTIEL

- Logique du premier ordre
- Base de la démonstration automatique (“résolution au premier ordre”)
- Déduction naturelle au premier ordre

EXAMEN