Déduction Naturelle

Propriétés et tactiques

Benjamin Wack

Université Grenoble Alpes

Février 2022

Au dernier cours

Déduction naturelle

- Règles
- Contexte
- Preuves

Rappel des règles

	Introduction	Élimination
Implication	$\dfrac{\begin{matrix}[A]\\ \dots \\ B\end{matrix}}{A\Rightarrow B}\ \Rightarrow I$	$\dfrac{A \quad A\Rightarrow B}{B}\ \Rightarrow E$
Conjonction	$\dfrac{A \quad B}{A\wedge B}\ \wedge I$	$\dfrac{A\wedge B}{A}\ \wedge E1$ $\dfrac{A\wedge B}{B}\ \wedge E2$
Disjonction	$\dfrac{A}{A\vee B}\ \vee I1$ $\dfrac{B}{A\vee B}\ \vee I2$	$\dfrac{A\vee B \quad A\Rightarrow C \quad B\Rightarrow C}{C}\ \vee E$
	Règle du faux	
$\bot$	$\dfrac{\bot}{A}\ Efq$	
	Règle de réduction à l'absurde	
	$\dfrac{\neg\neg A}{A}\ RAA$	

Un exemple avec environnement

Prouvez que $\neg A$ dans l'environnement $\neg(A \vee B)$

environnement			
référence		formule	
(i)		$\neg(A \vee B)$	
contexte	numero	preuve	justification

environnement			
référence		formule	
(i)		$\neg(A \vee B)$	
contexte	numero	preuve	justification
1	1	`Supposons` A	

environnement			
référence		formule	
(i)		$\neg(A \vee B)$	
contexte	numero	preuve	justification
1	1	`Supposons` A	
1	2	$A \vee B$	$\vee I1$ 1

Encore un exemple... (exemple 3.1.12)

Prouver que $\neg A \vee B$ dans l'environnement $A \Rightarrow B$.

environnement			
référence		formule	
(i)		$A \Rightarrow B$	
contexte	numero	preuve	justification

environnement			
référence		formule	
(i)		$A \Rightarrow B$	
contexte	numero	preuve	justification
1	1	`Supposons` $\neg(\neg A \vee B)$	

environnement			
référence		formule	
(i)		$A \Rightarrow B$	
contexte	numero	preuve	justification
1	1	`Supposons` $\neg(\neg A \vee B)$	

Arbre (exemple 3.1.12)

Donnez la représentation en arbre de la preuve précédente :

$$
\dfrac{\dfrac{(1)\cancel{\neg(\neg A \vee B)} \qquad \dfrac{\dfrac{\dfrac{(1)\cancel{\neg(\neg A \vee B)} \qquad \dfrac{\dfrac{(i) A \Rightarrow B \quad (2)\cancel{A}}{(3) B} \Rightarrow E}{(4) \neg A \vee B} \vee 2}{(5) \bot} \Rightarrow E}{(6) \neg A} \Rightarrow I[2]}{(7) \neg A \vee B} \vee 1}{(8) \bot} \Rightarrow E}{(9) \neg\neg(\neg A \vee B)} \Rightarrow I[1]
$$

$$
\dfrac{(9) \neg\neg(\neg A \vee B)}{(10) \neg A \vee B} \; RAA
$$

L'environnement est constitué des formules portées par les feuilles non-enlevées.

Intuitionnisme et constructivisme (Brouwer, 1881-1966)

Dans la suite de Poincaré, fondateur (en 1918) de la philosophie **intuitionniste** : les mathématiques doivent manipuler des objets accessibles à l'intuition.

- refus des objets infinis comme dans la théorie des ensembles
- en particulier notion de **réel constructible** = algorithme qui produit ses décimales

Exemple de preuve non constructive : supposons $P(0)$ et $\neg P(2)$.
Alors $\exists x(P(x) \wedge \neg P(x+1))$ ... mais on ne sait pas dire si $x = 0$ ou $x = 1$ est le « bon » témoin pour cette propriété.
Les règles d'introduction du $\vee$ explicitent lequel des cas est vrai : suivre le raisonnement pas à pas constitue un *algorithme* !

En revanche la règle $\dfrac{\neg\neg A}{A}$ permet de contourner cette contrainte.

L'exemple du cours

contexte	numero	preuve	justification
1	1	Supposons $(p \Rightarrow \neg j) \wedge (\neg p \Rightarrow j) \wedge (j \Rightarrow m)$	
1	2	$\neg p \Rightarrow j$	$\wedge E$ 1
1	3	$j \Rightarrow m$	$\wedge E$ 1
1,4	4	Supposons $\neg(m \vee p)$	
1,4,5	5	Supposons p	
1,4,5	6	$m \vee p$	$\vee I$ 5
1,4,5	7	$\perp$	$\Rightarrow E$ 4,6
1,4	8	Donc $\neg p$	$\Rightarrow I$ 5,7
1,4	9	j	$\Rightarrow E$ 2, 8
1,4	10	m	$\Rightarrow E$ 3, 9
1,4	11	$m \vee p$	$\vee I$ 10
1,4	12	$\perp$	$\Rightarrow E$ 4, 11
1	13	Donc $\neg\neg(m \vee p)$	$\Rightarrow I$ 4, 13
1	14	$m \vee p$	RAA 13

Théorème

Théorème 3.3.1

Si une formule A est déduite d'un environnement de formules Γ ($\Gamma \vdash A$) alors A est une conséquence de Γ ($\Gamma \models A$).

Toute preuve écrite dans un environnement Γ est correcte !

Preuve par récurrence sur le nombre de lignes d'une preuve P :

- On note H_i le contexte et C_i la conclusion de la $i^{\text{ème}}$ ligne de P.
- On montre que pour tout k on a $\Gamma, H_k \models C_k$.

D'où pour la dernière ligne n de la preuve $\Gamma \models A$.
(H_n est vide et $C_n = A$.)

Cas de base

Supposons que A est déduite de Γ par la preuve vide.

Alors A est élément de Γ.

Donc $\Gamma \models A$.

Hypothèse de récurrence

Supposons que pour toute ligne $i < k$ nous avons $\Gamma,\ H_i \models C_i$.

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

Trois cas sont possibles :

- La ligne k est « `Supposons` C_k ».
- La ligne k est « `Donc` C_k ».
- La ligne k est « C_k ».

La ligne k est « `Supposons` C_k »

Alors la formule C_k est la dernière formule de H_k.

Donc $\Gamma, H_k \models C_k$.

La ligne k est « `Donc` C_k »

C_k est alors de la forme $B \Rightarrow D$ où :

- B est la dernière formule de H_{k-1} et $H_{k-1} = H_k, B$
- D est utilisable sur la ligne précédente.

Il existe une ligne $i < k$ telle que $D = C_i$ et H_i est préfixe de H_{k-1}.
Par hypothèse de récurrence $\Gamma,\ H_i \models D$.

Puisque H_i est préfixe de H_{k-1} on a $\Gamma,\ H_{k-1} \models D$
ce qui s'écrit également $\Gamma,\ H_k,\ B \models D$.
On en déduit que $\Gamma,\ H_k \models B \Rightarrow D$.

La ligne k est « C_k »

C_k est alors la conclusion d'une règle dont les prémisses sont :

- utilisables à la ligne précédente
- ou éléments de Γ.

On considère le seul cas de la règle $\wedge$I (autres cas analogues).
$C_k = D \wedge E$ et les prémisses de la règle sont D et E.

Par hypothèse de récurrence, nous avons :
$\Gamma,\ H_{k-1} \models D$ et $\Gamma,\ H_{k-1} \models E$.
Puisque la règle appliquée n'est pas $\Rightarrow I$, on a $H_{k-1} = H_k$.

Enfin $D,\ E \models D \wedge E$. Par transitivité $\Gamma,\ H_k \models C_k$.

Pour toutes les autres règles, la conclusion est également conséquence des prémisses.

Théorème

Uniquement pour les formules avec les symboles $\bot$, $\land$, $\lor$, $\Rightarrow$.

La complétude avec les symboles $\top$, $\neg$, $\Leftrightarrow$ est obtenue par le biais d'une formule équivalente (en développant les abréviations).

Théorème 3.4.1

Soient Γ un ensemble fini de formules et A une formule.
Si $\Gamma \models A$ alors $\Gamma \vdash A$.

Définitions

Un littéral est une variable x ou une implication $x \Rightarrow \perp$.
Des littéraux complémentaires sont x et $x \Rightarrow \perp$ (abrégé en $\neg x$).

On définit une mesure m des formules et des listes de formules :

- $m(\perp) = 0$
- $m(x) = 1$
- $m(A \Rightarrow B) = 1 + m(A) + m(B)$ (d'où $m(\neg A) = m(A) + 1$)
- $m(A \wedge B) = 1 + m(A) + m(B)$
- $m(A \vee B) = 2 + m(A) + m(B)$
- $m(\Gamma) = \sum_{A \in \Gamma} m(A)$

Par exemple soit $A = (a \vee \neg a)$.
$m(\neg a) = 2,\qquad m(A) = 5\qquad$ et $m(A,\ (b \wedge b),\ A) = 13$.

Récurrence

Soit $P(n)$ la propriété suivante :
Si $m(\Gamma,\ A) = n$, si $\Gamma \models A$ alors $\Gamma \vdash A$.

Pour montrer que $P(n)$ est vraie pour tout entier n, nous utilisons la récurrence « forte » :

Supposons que pour tout $i < k$, la propriété $P(i)$ est vérifiée.
Supposons que $m(\Gamma,\ A) = k$ et que $\Gamma \models A$.
Montrons que : $\Gamma \vdash A$.

Décomposition

On décompose Γ ou A pour pouvoir appliquer l'hypothèse de récurrence.

A est indécomposable si A est $\perp$ ou une variable.
Γ est indécomposable si Γ est une liste de littéraux ou comprend la formule $\perp$.

Nous étudions trois cas :

Cas 1 : Ni A, ni Γ ne sont décomposables.

Cas 2 : A est décomposable.
Alors $A = B \circ C$ pour un certain connecteur binaire $\circ$.
On voit facilement que $m(\Gamma, B) < m(\Gamma, A)$ et $m(\Gamma, C) < m(\Gamma, A)$.

Cas 3 : Γ est décomposable.
On choisit une formule décomposable (autre que $x \Rightarrow \perp$) dans Γ.

Cas 1 : ni A, ni Γ ne sont décomposables

Alors :

- Γ comprend la formule $\perp$ ou est une liste de littéraux.
- A est $\perp$ ou une variable.

(a) Si $\perp \in \Gamma$ alors A peut se déduire de $\perp$ par la règle *Efq*.

(b) Si Γ est une liste de littéraux on distingue les deux cas pour A :

- $A = \perp$.
  Puisque $\Gamma \models A$, il y a deux littéraux complémentaires dans Γ.
  On peut alors déduire $\perp$ par la règle $\Rightarrow$E.
- A est une variable.
  Puisque $\Gamma \models A$:
  - soit Γ comporte deux littéraux complémentaires et de même $\Gamma \vdash A$.
  - soit $A \in \Gamma$ et alors immédiatement $\Gamma \vdash A$.

Cas 2 : A est décomposable

A se décompose en $B \wedge C$ ou $B \vee C$, ou $B \Rightarrow C$.

On étudie uniquement le cas $A = B \wedge C$, les autres cas sont similaires.

Puisque $\Gamma \models A$ et $A = B \wedge C$, on a $\Gamma \models B$ et $\Gamma \models C$.

Les mesures de B et C sont strictement inférieures à celles de A, d'où $m(\Gamma, B) < k$ et aussi $m(\Gamma, C) < k$.
Par hypothèse de récurrence, il existe deux preuves P et Q telles que $\Gamma \vdash P : B$ et $\Gamma \vdash Q : C$.

Donc la preuve « P, Q, A » où la dernière ligne est obtenue par la règle $\wedge$I est une preuve de A dans l'environnement Γ.

Cas 3 : Γ est décomposable

Il existe alors une formule décomposable dans Γ qui est de l'une des six formes suivantes :

- $B \wedge C$
- $B \vee C$
- $B \Rightarrow C$ où $C \neq \bot$
- $(B \wedge C) \Rightarrow \bot$
- $(B \vee C) \Rightarrow \bot$
- $(B \Rightarrow C) \Rightarrow \bot$

Nous étudions seulement le premier cas.

Γ est une permutation de la liste $B \wedge C,\ \Delta$

Γ et $B \wedge C,\ \Delta$ ont la même mesure.

Puisque $\Gamma \models A$, on a $B, C, \Delta \models A$.

$m(B) + m(C) < m(B \wedge C)$.

Donc $m(B, C, \Delta, A) < m(B \wedge C,\ \Delta, A) = m(\Gamma, A)$.
Par hypothèse de récurrence, il existe une preuve P telle que $B, C, \Delta \vdash P : A$.

La preuve « $B,\ C,\ P$ » où les deux premières lignes sont obtenues par les règles $\wedge$E1 et $\wedge$E2 est une preuve de A dans l'environnement Γ.

Remarque 3.4.2

La preuve de complétude est constructive, c'est-à-dire qu'elle donne un algorithme pour construire une preuve de A dans Γ.

Cependant les preuves ainsi construites peuvent être longues.

L'outil
`http://teachinglogic.univ-grenoble-alpes.fr/DN/`
construit des preuves plus efficaces.
Il utilise les tactiques « optimisées » présentées section 3.2, page 71.

Par exemple, pour prouver $B \vee C$:

- Essayez d'abord de prouver B.
- Si vous échouez, essayez de prouver C.
- Sinon, utilisez la tactique 10 (prouver C sous l'hypothèse $\neg B$).

Tactiques

Liste de 13 tactiques à utiliser dans l'ordre !

- Tactiques 1 à 3 : la preuve est terminée
- Tactiques 4 à 6 : preuve guidée par la formule à prouver (règles I)
- Tactiques 7 à 9 : preuve guidée par l'environnement (règles E)
- Tactiques 10 à 13 : raisonnement par l'absurde

Tactique 1 (trivial)

Si $A \in \Gamma$ alors la preuve obtenue est vide.

Tactique 2 (trivial + intro)

Si A est la conséquence d'une règle dont les prémisses sont dans Γ, alors la preuve obtenue est « A ».

Tactique 3 (Efq)

Si Γ comporte une contradiction, c'est-à-dire une formule B et une formule $\neg B$,
alors la preuve obtenue est « $\perp, A$ ».

Tactique 4

Si $A = B \wedge C$ alors :

contexte	preuve	justification
Γ	B	$\cdots P \cdots$
Γ	C	$\cdots Q \cdots$
Γ	$B \wedge C$	$\wedge I$

Les preuves peuvent échouer (si $\Gamma \not\models A$).
Ici, si la preuve de B ou C échoue, celle de A aussi.

Par la suite on ne signale plus les cas d'échecs,
sauf s'il faut essayer une autre preuve.

Tactique 5

Si $A = B \Rightarrow C$, alors prouver C sous l'hypothèse B :

contexte	preuve	justification
Γ, B	$\texttt{Supposons } B$	
Γ, B	C	$\cdots P \cdots$
Γ	$\texttt{Donc } B \Rightarrow C$	$\Rightarrow I$

Tactique 6

Si $A = B \vee C$, alors prouver B :

contexte	preuve	justification
Γ	B	$\cdots P \cdots$
Γ	$B \vee C$	$\vee I1$

Si la preuve de B échoue alors prouver C :

contexte	preuve	justification
Γ	C	$\cdots P \cdots$
Γ	$B \vee C$	$\vee I2$

Si la preuve de C échoue aussi, essayer les tactiques suivantes.

Tactique 7

Si $B \wedge C$ est dans l'environnement, alors prouver A à partir des formules B, C, qui remplacent $B \wedge C$ dans l'environnement :

contexte	preuve	justification
$\Gamma, B \wedge C$	B	$\wedge E1$
$\Gamma, B \wedge C$	C	$\wedge E2$
$\Gamma, B \wedge C$	A	$\cdots P \cdots$

Tactique 8

Si $B \vee C$ est dans l'environnement, alors :

- prouver A dans l'environnement où B remplace $B \vee C$
- puis prouver A dans l'environnement où C remplace $B \vee C$:

contexte	preuve	justification
$\Gamma, B \vee C, B$	Supposons B	
$\Gamma, B \vee C, B$	A	$\cdots P \cdots$
$\Gamma, B \vee C$	Donc $B \Rightarrow A$	$\Rightarrow I$
$\Gamma, B \vee C, C$	Supposons C	
$\Gamma, B \vee C, C$	A	$\cdots Q \cdots$
$\Gamma, B \vee C$	Donc $C \Rightarrow A$	$\Rightarrow I$
$\Gamma, B \vee C$	A	$\vee E$

Tactique 9 ($\neg\vee$ dans Γ)

Si $\neg(B \vee C)$ est dans l'environnement, alors

- nous déduisons $\neg B$ par la preuve $P4$ et
- $\neg C$ par la preuve $P5$ (preuves demandées à l'exercice 59).
- Soit P la preuve de A dans l'environnement où $\neg B$, $\neg C$ remplacent la formule $\neg(B \vee C)$.

La preuve de A est « $P4$, $P5$, P ».

Tactique 10 (tiers exclus)

Si $A = B \vee C$, alors prouver C sous l'hypothèse $\neg B$: soit P la preuve obtenue.
« `Supposons` $\neg B$, P, `Donc` $\neg B \Rightarrow C$ » est une preuve de la formule $\neg B \Rightarrow C$ qui est équivalente à A.

Pour obtenir la preuve de A, il suffit d'ajouter la preuve $P1$, demandé à l'exercice 59 de A dans l'environnement $\neg B \Rightarrow C$.
La preuve obtenue de A est donc « `Supposons` $\neg B$, P, `Donc` $\neg B \Rightarrow C$, $P1$ ».

Tactique 11 ($\neg\wedge$ dans Γ)

Si $\neg(B \wedge C)$ est dans l'environnement, alors nous en déduisons $\neg B \vee \neg C$ par la preuve $P3$ demandée à l'exercice 59 puis nous raisonnons par cas comme ci-dessus :

- prouver A dans l'environnement où $\neg B$ remplace $\neg(B \wedge C)$: Soit P la preuve obtenue,
- prouver A dans l'environnement où $\neg C$ remplace $\neg(B \wedge C)$: Soit Q la preuve obtenue.

La preuve de A est « $P3$, `Supposons` $\neg B$, P, `Donc` $\neg B \Rightarrow A$, `Supposons` $\neg C$, Q, `Donc` $\neg C \Rightarrow A$, A ».

Tactique 12 ($\neg \Rightarrow$ dans Γ)

Si $\neg(B \Rightarrow C)$ est dans l'environnement, alors

- nous déduisons B par la preuve $P6$,
- $\neg C$ par la preuve $P7$ (preuves demandées à l'exercice 59).
- Soit P la preuve de A dans l'environnement où B, $\neg C$ remplacent la formule $\neg(B \Rightarrow C)$.

La preuve de A est « $P6$, $P7$, P ».

Tactique 13 ($\Rightarrow$ dans Γ)

Si $B \Rightarrow C$ est dans l'environnement et si $C \neq \bot$, autrement dit si $B \Rightarrow C$ n'est pas égale à $\neg B$, alors,
nous déduisons $\neg B \vee C$ dans l'environnement $B \Rightarrow C$ par la preuve $P2$ demandée à l'exercice 59 puis nous raisonnons par cas :

- prouver A dans l'environnement où $\neg B$ remplace $B \Rightarrow C$: Soit P la preuve obtenue,
- prouver A dans l'environnement où C remplace $B \Rightarrow C$: Soit Q la preuve obtenue.

La preuve de A est « $P2$, `Supposons` $\neg B$, P, `Donc` $\neg B \Rightarrow A$, `Supposons` C, Q, `Donc` $C \Rightarrow A$, A ».

Exemple

Preuve de la formule de Pierce :

$$((p \Rightarrow q) \Rightarrow p) \Rightarrow p$$

Plan de preuve

Tactique 5 ($\Rightarrow$I) obligatoire !

Preuve Q :
`Supposons` $(p \Rightarrow q) \Rightarrow p$
$\boxed{Q_1 \text{ preuve de } p \text{ dans l'environnement } (p \Rightarrow q) \Rightarrow p}$
`Donc` $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$

La preuve Q_1 utilise nécessairement la tactique 13 (environnement formé de $B \Rightarrow C \ = \ (p \Rightarrow q) \Rightarrow p$).

Donc on doit prouver p :

- dans l'environnement $\neg B = \neg(p \Rightarrow q)$
- dans l'environnement $C = p$.

Plan de la preuve de Q_1

Preuve Q_1 :

$\boxed{Q_{11} \text{ est la preuve de } \neg B \vee C \text{ dans l'environnement } B \Rightarrow C \text{, voir exercice 59}}$

`Supposons` $\neg(p \Rightarrow q)$

$\boxed{Q_{12} \text{ preuve de } p \text{ dans l'environnement } \neg(p \Rightarrow q)}$

`Donc` $\neg(p \Rightarrow q) \Rightarrow p$

`Supposons` p

$\boxed{Q_{13} \text{ preuve de } p \text{ dans l'environnement } p}$

`Donc` $p \Rightarrow p$

p

Preuve de Q_1

Q_{13} est la preuve vide, car $A = C = p$.

Q_{12} est la preuve de $A = p$ dans l'environnement $\neg(p \Rightarrow q)$.
(c'est la preuve P_6 demandée à l'exercice 59)

En recollant les morceaux Q_1, Q_{11}, Q_{12}, Q_{13}, nous obtenons la preuve Q.

On peut aussi faire la preuve Q_{12} sans utiliser les tactiques.

Aujourd’hui

- La Déduction Naturelle propositionnelle est correcte et complète.
- Tactiques pour la construction d’une preuve

Preuves automatiques

Pour produire automatiquement des preuves sous forme de tableau, on recommande d'utiliser le logiciel (il implémente les treize tactiques précédentes) :

`http://teachinglogic.univ-grenoble-alpes.fr/DN/`

Pour construire des preuves sous forme d'arbres, on peut s'aider du logiciel :

`http://www-sop.inria.fr/marelle/Laurent.Thery/peanoware/Nd.html`

Plan du Semestre

RENTREE S4

- Logique propositionnelle
- Résolution propositionnelle
- Déduction naturelle propositionnelle *
- Logique du premier ordre

PARTIEL

- Base de la démonstration automatique (« résolution au premier ordre »)
- Déduction naturelle au premier ordre

EXAMEN