First Order Natural Deduction : Tactics and Consistency

Benjamin Wack

Université Grenoble Alpes

April 2022

Overview

Reminder: Rules

Contents

Proof tactics

Properties

Consistency of the system

Conclusion

Overview

Reminder: Rules

Contents

Proof tactics

Properties

Consistency of the system

Conclusion

Reminder: "Propositional" rules

Table 3.1

Introduction	Elimination
$\dfrac{\begin{matrix}[A] \\ \dots \\ B\end{matrix}}{A \Rightarrow B} \Rightarrow I$	$\dfrac{A \quad A \Rightarrow B}{B} \Rightarrow E$
$\dfrac{A \quad B}{A \wedge B} \wedge I$	$\dfrac{A \wedge B}{A} \wedge E1$ $\dfrac{A \wedge B}{B} \wedge E2$
$\dfrac{A}{A \vee B} \vee I1$ $\dfrac{A}{B \vee A} \vee I2$	$\dfrac{A \vee B \quad A \Rightarrow C \quad B \Rightarrow C}{C} \vee E$
Ex falso quodlibet	
$\dfrac{\bot}{A}$ *Efq*	
Reductio ad absurdum	
$\dfrac{\neg\neg A}{A}$ *RAA*	

Summary of the quantification rules: Figure 6.1

$\dfrac{A}{\forall x A}$	$\forall I$	x must be free neither in the proof environment, nor in the context
$\dfrac{\forall x A}{A{<}x{:=}t{>}}$	$\forall E$	t is free for x in A
$\dfrac{A{<}x{:=}t{>}}{\exists x A}$	$\exists I$	t is free for x in A
$\dfrac{\exists x A \qquad (A \Rightarrow B)}{B}$	$\exists E$	x must be free neither in the proof environment, nor in the context, nor in B.

Copy rule

$\dfrac{A'}{A}$	copy	if A is equal to A' up to renaming of bound variables.

+ Reflexivity and congruence for equality

Overview

Reminder: Rules

Contents

Proof tactics

Properties

Consistency of the system

Conclusion

Tactics

1. Two proof tactics:
   - for the rule $\forall I$
   - for the rule $\exists E$

2. No tactic for the rules $\forall E$ and $\exists I$ (the ones that make the system undecidable !)

Consistency and Completeness

- **We will prove the consistency of the rules in our system.**
- **We will assume without proof that the system is complete.**
  You'll find similar proofs of completeness in the following books:
  - 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.

Overview

Reminder: Rules

Contents

Proof tactics

Properties

Consistency of the system

Conclusion

Introduction

1. Two proof tactics for the rules $\forall I$ and $\exists E$ which correspond to forms of mathematical reasoning:
   1.1 Reason forwards with an existence hypothesis,
   1.2 Reason backwards to generalize.
2. Application to an example.

Reason forwards with an existence hypothesis

Let Γ be a set of formulae, x a variable, A and C formulae.

We're looking for a proof of C under environment $\Gamma, \exists x A$.

Two distinct cases:

- x is free neither in Γ nor in C.
- x is free either in Γ or C.

1^{st} case: x is free neither in Γ nor in C

In this case, the proof can be written:

Assume A	
proof of C under environment Γ, A	
Therefore $A \Rightarrow C$	$\Rightarrow$I 1,...
C	$\exists$E

2^{nd} case: x is free either in Γ or in C

We choose a variable y :

- "fresh", *i.e.* not free in Γ, C
- not occurring in A

then we reduce this case to the previous one, via the copy rule.

The proof is then written:

$\exists y A < x := y >$	copy of $\exists x A$
Assume $A < x := y >$	
proof of C under environment $\Gamma, A < x := y >$	
Therefore $A < x := y > \Rightarrow C$	$\Rightarrow$I 1,_
C	$\exists$E

A simple example

Let's prove $\exists x P(x) \wedge \forall x \neg P(x) \Rightarrow \bot$.

1	1	Assume $\exists x P(x) \wedge \forall x \neg P(x)$	
1	2	$\exists x P(x)$	$\wedge$E1 1
1	3	$\forall x \neg P(x)$	$\wedge$E2 1
1,2	4	Assume $P(x)$	
1,2	5	$\neg P(x)$	$\forall$E 3 x
1,2	6	$\bot$	$\Rightarrow$E 4,5
1	7	Therefore $P(x) \Rightarrow \bot$	
1	8	$\bot$	$\exists$E 2,7
	9	Therefore $\exists x P(x) \wedge \forall x \neg P(x) \Rightarrow \bot$	$\Rightarrow$I 1, 8

Remarks

The search for the initial proof has been reduced to the search for a proof of the *same* formula in a simpler environment.

This kind of reasoning is used in maths when we look for a proof of a formula C under hypothesis $\exists x P(x)$.

It amounts to introducing a “new” constant a such that $P(a)$ holds, and proving C under hypothesis $P(a)$.

Reasoning backwards to generalize

We're looking for a proof of $\forall x A$ under environment Γ.

Two distinct cases:

- x is not free in Γ.
- x is free in Γ.

1^{st} case: x is not free in Γ

proof of A under environment Γ

$\forall xA$ $\quad \forall I$

2^{nd} case: x is free in Γ

We choose a variable y :

- “fresh”, *i.e.* not free in Γ
- not occurring in A

then we reduce this case to the previous one, via the copy rule.

The proof can then be written:

proof of $A < x := y >$ under environment Γ	
$\forall y A < x := y >$	$\forall$I
$\forall x A$	copy of the previous formula

A simple example

Let us prove $\forall x P(x) \Rightarrow \forall y P(y)$ without copy.

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

Remark

The search for the initial proof has been reduced to the search for a proof of a simpler formula in the same environment.

This kind of reasoning is used in maths when we're looking for a proof of $\forall x P(x)$.

It amounts to introducing a “fresh” variable y and proving the formula $P(y)$.
Then we conclude: since the choice of y was arbitrary, we have $\forall x P(x)$.

An example of tactics application

We define "there exists one x and only one" (briefly noted $\exists! x$) as:

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

Expressing separately the existence of x and its uniqueness, we can define the same notion as:

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

These two definitions are equivalent of course: here we prove formally that **the former implies the latter**.

Since the proof is large, we're going to decompose it.

6.2.3 Proof overview

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

We apply the two following tactics:

- To prove $A \Rightarrow B$, assume A and deduce B.
- To prove $B_1 \land B_2$, prove B_1 and prove B_2.

1	Assume $\exists x(P(x) \land \forall y(P(y) \Rightarrow x = y))$	
1	proof of $\exists x P(x)$ under environment 1	
1	proof of $\forall x \forall y(P(x) \land P(y) \Rightarrow x = y)$ under environment 1	
1	$\exists x P(x) \land \forall x \forall y(P(x) \land P(y) \Rightarrow x = y)$	$\land$I
	Therefore $\exists x(P(x) \land \forall y(P(y) \Rightarrow x = y)) \Rightarrow \exists x P(x) \land \forall x \forall y(P(x) \land P(y) \Rightarrow x = y)$	$\Rightarrow$I

6.2.3 Application of the tactic for using an existence hypothesis

Proof of $\exists x P(x)$ under environment $\exists x(P(x) \wedge \forall y(P(y) \Rightarrow x = y))$

context	N^o	formula	rule
	i	$\exists x(P(x) \wedge \forall y(P(y) \Rightarrow x = y))$	
1	1	Assume $P(x) \wedge \forall y(P(y) \Rightarrow x = y)$	
1	2	$P(x)$	$\wedge$E1 1
1	3	$\exists x P(x)$	$\exists$I 2, x
	4	Therefore $P(x) \wedge \forall y(P(y) \Rightarrow x = y) \Rightarrow \exists x P(x)$	$\Rightarrow$I 1,2
	5	$\exists x P(x)$	$\exists$E i, 4

6.2.3 Application of the tactic for obtaining a general conclusion: proof overview

Proof of $\forall x \forall y (P(x) \wedge P(y) \Rightarrow x = y)$
under environment $\exists x (P(x) \wedge \forall y (P(y) \Rightarrow x = y))$

We apply the following tactics:

1. "Reason forwards with an existence hypothesis"
2. "Reason backwards to generalize"
   (twice)
3. To prove $A \Rightarrow B$, assume A and deduce B

6.2.3 Application of the tactic for obtaining a general conclusion: proof

context	N^o	formula	rule
	i	$\exists x(P(x) \wedge \forall y(P(y) \Rightarrow x = y))$	
1	1	Assume $P(x) \wedge \forall y(P(y) \Rightarrow x = y)$	
1,2	2	Assume $P(u) \wedge P(y)$	
1,2	3	$\forall y(P(y) \Rightarrow x = y)$	$\wedge$E2 1
1,2	4	$P(u)$	$\wedge$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	$P(y)$	$\wedge$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	Therefore $P(u) \wedge P(y) \Rightarrow u = y$	$\Rightarrow$I 2, 10
1	12	$\forall y(P(u) \wedge P(y) \Rightarrow u = y)$	$\forall$I 11
1	13	$\forall u \forall y(P(u) \wedge P(y) \Rightarrow u = y)$	$\forall$I 12
1	14	$\forall x \forall y(P(x) \wedge P(y) \Rightarrow x = y)$	copy of 13
	15	Therefore $(P(x) \wedge \forall y(P(y) \Rightarrow x = y)) \Rightarrow \forall x \forall y(P(x) \wedge P(y) \Rightarrow x = y)$	$\Rightarrow$I 1, 14
	16	$\forall x \forall y(P(x) \wedge P(y) \Rightarrow x = y)$	$\exists$E i, 15

Conclusion

The hard points in looking for proofs are the rules $\forall$E and $\exists$I :

- in forward reasoning, for formulae beginning with $\forall$, we need to find suitable instances of the bound variables
- in backward reasoning, we need to find suitable instances for proving formulae beginning with $\exists$

Overview

Reminder: Rules

Contents

Proof tactics

Properties

Consistency of the system

Conclusion

Reminder

We are going to use (again) two results about substitution:

Theorem 4.3.36

If t is a free term for the variable x in A, then

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

Corollary 4.3.38

If t is a free term for x in A, then

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

Properties of consequence

Property 6.3.1

If x is not free in Γ, then

$$\Gamma \models A \quad \text{if and only if} \quad \Gamma \models \forall x A$$

Proof of the property 6.3.1

$\Rightarrow$ Assume that $\Gamma \models A$.

Let (I, e) be a model of Γ.

Since x is not free in Γ, for every $d \in D$:
$(I, e[x = d])$ and (I, e) give the same value to the formulae in Γ
hence $(I, e[x = d])$ is model of Γ.

Therefore, $(I, e[x = d])$ is a model of A for any $d \in D$,
so (I, e) is a model of $\forall x A$.

$\Leftarrow$ Assume that $\Gamma \models \forall x A$.
Since the formula $\forall x A \Rightarrow A$ is valid (corollary with $t = x$),
we have $\Gamma \models A$.

Properties of consequence

Property 6.3.2

If x is free neither in Γ, nor in B, then we have:

$$\Gamma \models A \Rightarrow B \text{ if and only if } \Gamma \models (\exists x A) \Rightarrow B$$

Proof of property 6.3.2

- $\Rightarrow$ Assume that $\Gamma \models A \Rightarrow B$. Actually we prove that $\Gamma, \exists x A \models B$

  Let (I, e) be a model of Γ.

  Assume also that (I, e) is a model of $\exists x A$.

  This means that $(I, e[x = d])$ is a model of A for some $d \in D$.

  Because x is not free in Γ, the assignments $(I, e[x = d])$ and (I, e) give the same value to the formulae in Γ.

  Hence $(I, e[x = d])$ is a model of $A \Rightarrow B$.

  Since $(I, e[x = d])$ is a model of A too, it must be a model of B.

  Finally, since x is not free in B, (I, e) and $(I, e[x = d])$ give the same value to B.

- $\Leftarrow$ Assume that $\Gamma \models (\exists x A) \Rightarrow B$, *i.e.* $\Gamma, \exists A \models B$.

  Since the formula $A \Rightarrow (\exists x A)$ is valid (corollary with $x = t$),

  we have $\Gamma, A \models \Gamma, \exists x A \models B$, thus $\Gamma \models A \Rightarrow B$.

Overview

Reminder: Rules

Contents

Proof tactics

Properties

Consistency of the system

Conclusion

Consistency of deduction

Theorem 6.3.3

If $\Gamma \vdash A$ (by a proof in natural deduction) then $\Gamma \models A$.

Consistency proof overview

Let Γ be a set of formulae. Let P be a proof of A under Γ.
Let C_i be the conclusion and H_i the context of the i-th line in proof P.

Induction Hypothesis:
Assume that for every i where $0 < i < k$, we have $\Gamma, H_i \models C_i$.

Let us prove that $\Gamma, H_k \models C_k$.

The cases where C_k has been obtained by a propositional rule has already been checked.
We only deal with the new rules.

The rule $\forall$E

Assume that $C_k = A < x := t >$ was deduced by rule $\forall$E.

By induction hypothesis, there is an $i < k$ such that $\Gamma, H_i \models \forall x A$.

According to the application conditions of rule $\forall E$,
the term t is free for x in A.
Hence, **according to corollary 4.3.38**, the formula
$\forall x A \Rightarrow A < x := t >$ is valid and therefore $\Gamma, H_i \models A < x := t >$.

Since line i is usable, H_i is a prefix of H_k, hence $\Gamma, H_k \models C_k$.
$\square$

The rule ∃I

Assume that $C_k = \exists x A$ was deduced by rule ∃I.

By induction hypothesis, there is an $i < k$ such that
$\Gamma, H_i \models A < x := t >$

According to the application conditions of rule $\exists I$, t is free for the variable x in A.
Hence, **according to the corollary 4.3.38**, the formula
$A < x := t > \Rightarrow \exists x A$ is valid and so $\Gamma, H_i \models \exists x A$.

Since line i is usable, H_i is a prefix of H_k, hence $\Gamma, H_k \models C_k$.
□

The rule $\forall$I

Assume that $C_k = \forall x A$ was deduced by the rule $\forall$I.

Either $A = C_i$ with $i < k$, **by induction hypothesis** we have $\Gamma, H_i \models A$.
Or $A \in \Gamma$ and then $\Gamma \models A$.

According to the application conditions of rule $\forall I$,
x is not free in Γ, H_i.
Hence, **according to property 6.3.1**, we also have $\Gamma, H_i \models \forall x A$.

Since line i is usable, H_i is a prefix of H_k, hence $\Gamma, H_k \models C_k$.
□

The rule $\exists$E

Assume that $C_k = B$ was deduced by rule $\exists$E, from formulae $\exists x A$ and $A \Rightarrow B$.

By induction hypothesis, there are some $i < k$ and $j < k$ such that $\Gamma, H_i \models \exists x A$ and $\Gamma, H_j \models A \Rightarrow B$.

According to the application conditions of rule $\exists E$, x is free neither in Γ, H_j, nor in B.
Hence (**property 6.3.2**), we also have $\Gamma, H_j \models (\exists x A) \Rightarrow B$.

Since lines i and j are usable, H_i and H_j are prefixes of H_k, hence
$\Gamma, H_k \models \exists x A$ and $\Gamma, H_k \models (\exists x A) \Rightarrow B$.
Consequently $\Gamma, H_k \models C_k$.
$\square$

The copy rule

Assume that $C_k = A'$ was deduced by copy from formula A.

By induction hypothesis, there exists an $i < k$ such that $\Gamma, H_i \models A$.

We know that if $A =_\alpha A'$, then $A \equiv A'$, hence $\Gamma, H_i \models A'$.

Since line i is usable, H_i is a prefix of H_k, hence $\Gamma, H_k \models C_k$.
$\square$

Reflexivity

Assume that C_k is the formula $t = t$.

Let us recall that equality is always interpreted as $\{(d, d) \mid d \in D\}$, so in particular $=_I$ always contains $(\llbracket t \rrbracket_I, \llbracket t \rrbracket_I)$.

Thus, the formula C_k is valid, and $\Gamma, H_k \models C_k$.
$\square$

Congruence

Assume that $C_k = A < x := t >$ was deduced by the congruence rule.

By induction hypothesis, there exist some $i < k$ and $j < k$ such that $\Gamma, H_i \models (s = t)$ and $\Gamma, H_j \models A < x := s >$.

Since lines i and j are usable, H_i and H_j are prefixes of H_k, hence $\Gamma, H_k \models (s = t)$ and $\Gamma, H_k \models A < x := s >$.

The use conditions of the rule ensure that s and t are free for x in A. Hence we can use:

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

Furthermore, equality ensures that if (I, e) is a model of $s = t$ then d and d' are the **same** member of D.
Hence $s = t, A < x := s > \models A < x := t >$, so $\Gamma, H_k \models C_k$. □

Kurt Gödel (1906-1978) and his incompleteness theorems

First incompleteness theorem (1931)

Every logical system in which we can formalize arithmetics also allows to state:

“This statement is unprovable”.

- either this statement is false; thus it is provable, and our system is inconsistent
- or this statement is true; thus it is unprovable, and our system is incomplete

Second incompleteness theorem

No logical system can prove its own consistency.

Overview

Reminder: Rules

Contents

Proof tactics

Properties

Consistency of the system

Conclusion

Today

- First-order Natural Deduction:
  - Tactics
  - Consistency

Overview of the Semester

- Propositional logic
- Propositional resolution
- Propositional natural deduction

MID-TERM EXAM

- First-order logic
- Basis for the automated deduction (“first-order resolution”)
- First-order natural deduction

EXAM