Natural deduction

0. What we have seen so far

Fundamental notions: inductive definitions and language in general

A particular case: the langages of predicate logic

I. Deduction rules

The set of provable proposition

An inductive definition

$$\frac{A \Rightarrow B \quad A}{B}$$

$$\frac{}{P \Rightarrow Q \Rightarrow R}$$

$$\frac{}{P}$$

$$\frac{}{Q}$$

Exercise: give a derivation (proof) of R

But not so comfortable

To prove $A \Rightarrow B$, assume A and prove B

Do not deduce propositions but pairs formed with hypotheses and a conclusion, sequents, $\Gamma \vdash A$

$$\frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}$$

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

$$\frac{}{\Gamma, A \vdash A}$$

An exercise

Prove $P \vdash Q \Rightarrow P$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-intro}$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-elim}$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-elim}$$

The classification of the rules

These three rules mention only the connective $\wedge$
Most rules mention only one connective: the rules of $\wedge$, the rules of $\vee$, etc.
Either in the conclusion or in the premises

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-intro}$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-elim}$$

introduction / elimination

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee\text{-intro}$$

$$\frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee\text{-intro}$$

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\ \vee\text{-elim}$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \Rightarrow\text{-intro}$$

$$\frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \Rightarrow\text{-elim}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x\ A}\ \forall\text{-intro if } x \notin FV(\Gamma)$$

$$\frac{\Gamma \vdash \forall x\ A}{\Gamma \vdash (t/x)A}\ \forall\text{-elim}$$

$$\frac{\Gamma \vdash (t/x)A}{\Gamma \vdash \exists x\ A}\ \exists\text{-intro}$$

$$\frac{\Gamma \vdash \exists x\ A \quad \Gamma, A \vdash B}{\Gamma \vdash B}\ \exists\text{-elim if } x \notin FV(\Gamma, B)$$

$$\frac{}{\Gamma \vdash \top}\ \top\text{-intro}$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}\ \bot\text{-elim}$$

$$\frac{}{\Gamma \vdash A}\ \text{axiom if } A \in \Gamma$$

$$\frac{}{\Gamma \vdash A \vee \neg A}\ \text{excluded-middle}$$

$\neg$, $\Leftrightarrow$

No rules for $\neg$ and $\Leftrightarrow$

$\neg A$ abbreviation for $A \Rightarrow \bot$
$A \Leftrightarrow B$ abbreviation for $(A \Rightarrow B) \land (B \Rightarrow A)$

Substitution

In $\forall$-elim and $\exists$-intro: a auxillary operation: substitution $(t/x)u$

$$\frac{\Gamma \vdash \forall x\ A}{\Gamma \vdash (t/x)A}\ \forall\text{-elim}$$

$$\frac{\Gamma \vdash (t/x)A}{\Gamma \vdash \exists x\ A}\ \exists\text{-intro}$$

From $\forall x\ (x + x = 2 \times x)$ deduce $7 + 7 = 2 \times 7$
(substituting 7 for x)
The operation that gives its meaning to the word variable
In the language of predicate logic and in all languages (in particular in programming languages)

A simple definition

for languages with no binders

- $(t/x)(f(u_1, ..., u_n)) = f((t/x)u_1, ..., (t/x)u_n)$
- $(t/x)x = t$
- $(t/x)y = y$ if $x \neq y$

For languages with binders

$(4/x)(\forall x\ P(x)) = \forall x\ P(4)$ or $\forall x\ P(x)$?

Rule 1: substitute free variables only

First attempt:

- $\langle t/x\rangle(\forall y\ A) = \forall y\ (\langle t/x\rangle A)$ if $x \neq y$
- $\langle t/x\rangle(\forall x\ A) = \forall x\ A$

But not enough

$\langle 4/y\rangle(\forall x\ P(x+y)) = \forall x\ P(x+4)$
$\langle z/y\rangle(\forall x\ P(x+y)) = \forall x\ P(x+z)$
$\langle x/y\rangle(\forall x\ P(x+y)) = \forall x\ P(x+x)$
The free occurrence of x has been captured

Rule 2: avoid variable capture
Rename the bound variable x in w
$(x/y)(\forall x\ P(x+y)) = \forall w\ P(w+x)$
Why w rather than v?
Equivalent
Alphabetic equivalence (α-equivalence)

Alphabetic equialence

- $\forall x\ A \sim \forall y\ B$ If for all variables z that occur neither in $\forall x\ A$ not in $\forall y\ B$ on a $\langle z/x \rangle A \sim \langle z/y \rangle B$

Example: $\forall x\ P(x + w)$ and $\forall y\ P(y + w)$ equivalent

From now on: classes of expressions modulo alphabetic equivalence

Substitution (finally...)

- $(t/x)(\forall y\ A) = \forall z\ (t/x)\langle z/y\rangle A$ where z is any variable different from x and y and that occurs in neither in t nor in A

Piling notions: substitution with captures $\rightarrow$ alphabetic equivalence $\rightarrow$ classes of expressions $\rightarrow$ substitution

Many mistakes in books and... computer algebra systems, prorgamming languages, proof processing systems...

Proofs

A sequent $\Gamma \vdash A$ is provable iff it has a derivation (proof)

A tree where nodes are labelled with sequents

Root labelled by $\Gamma \vdash A$

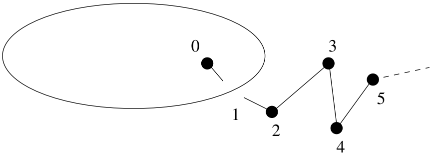
If node labelled by $\Delta \vdash B$ and children labelled by $\Sigma_1 \vdash C_1$, ..., $\Sigma_n \vdash C_n$ then a Natural deduction rule deduces $\Delta \vdash B$ from $\Sigma_1 \vdash C_1, \ldots, \Sigma_n \vdash C_n$

Proof of a proposition, proof in an axiomatic theory

A proposition A is provable (without any axioms), if $\vdash A$ is

Axiomatic theory $\mathcal{T}$: set of closed propositions (axioms)
A provable in $\mathcal{T}$ if finite subset Γ of $\mathcal{T}$, $\Gamma \vdash A$ provable

II. What is a constructive proof?



$0 \in P$ and $2 \notin P$
Does there exists n such that $n \in P$ and $n + 1 \notin P$?

$$P(0), \neg P(S(S(0))) \vdash \exists x\ (P(x) \land \neg P(S(x)))$$

π_1

$$\cfrac{\cfrac{}{\Gamma, P(S(0)) \vdash P(S(0))} \quad \cfrac{}{\Gamma, P(S(0)) \vdash \neg P(S(S(0)))}}{\cfrac{\Gamma, P(S(0)) \vdash P(S(0)) \land \neg P(S(S(0)))}{\Gamma, P(S(0)) \vdash \exists x\ (P(x) \land \neg P(S(x)))}}$$

where $\Gamma = \{P(0), \neg P(S(S(0)))\}$

π_2

$$\dfrac{\dfrac{}{\Gamma, \neg P(S(0)) \vdash P(0)} \quad \dfrac{}{\Gamma, \neg P(S(0)) \vdash \neg P(S(0))}}{\dfrac{\Gamma, \neg P(S(0)) \vdash P(0) \wedge \neg P(S(0))}{\Gamma, \neg P(S(0)) \vdash \exists x\ (P(x) \wedge \neg P(S(x)))}}$$

Finally

$$\dfrac{\dfrac{}{\Gamma \vdash P(S(0)) \vee \neg P(S(0))} \quad \dfrac{\pi_1}{\Gamma, P(S(0)) \vdash A} \quad \dfrac{\pi_2}{\Gamma, \neg P(S(0)) \vdash A}}{\Gamma \vdash A}$$

where $A = \exists x\ (P(x) \wedge \neg P(S(x)))$

We can prove

$$\exists x \; (P(x) \wedge \neg P(S(x)))$$

Can we prove

$$P(n) \wedge \neg P(S(n))$$

for some natural number n?

No: easy to prove that for each number n

$$P(0), \neg P(S(S(0))) \vdash P(n) \wedge \neg P(S(n))$$

not provable

Without any axioms

We can prove

$$\exists x \; (P(0) \Rightarrow \neg P(S(S(0))) \Rightarrow (P(x) \wedge \neg P(S(x))))$$

We can prove

$$P(0) \Rightarrow \neg P(S(S(0))) \Rightarrow (P(n) \wedge \neg P(S(n)))$$

for no natural number n

The notion of witness

E has the witness property if
when $\exists x\ A$ is in E, there exists t such that $(t/x)A$ is in E

The set of provable propositions: no witness property

How is this possible?

Only one possibility to prove $\exists x\ A$: prove $(t/x)A$ and then use the $\exists$-intro rule

Example π_1 and π_2

Then a proof by case

$$\frac{\dots \quad \dfrac{\pi_1}{\Gamma, P(S(0)) \vdash A} \quad \dfrac{\pi_2}{\Gamma, \neg P(S(0)) \vdash A}}{\Gamma \vdash A}$$

0 or $S(0)$?

But still needs to prove $P(S(0)) \vee \neg P(S(0))$

The excluded-middle rule

$(A \vee \neg A)$ without knowing which of A or $\neg A$ holds

The notion of constructive proof

A proof that does not use the excluded-middle rule

As we shall see: if a proposition $\exists x\ A$ has a constructive proof, without any axioms, then there exists a term t such that $(t/x)A$ has a proof

Algorithm to extract witness from proof: proof reduction

Extends to many theories

Programming with proofs

A constructive proof π of

$$\forall x \exists y \ (x = 2 \times y \vee x = 2 \times y + 1)$$

A proof of the proposition

$$\exists y \ (25 = 2 \times y \vee 25 = 2 \times y + 1)$$

Extract a witness from this proof
By construction, correct with respect to specification

$$x = 2 \times y \vee x = 2 \times y + 1$$

III. Theories

How can we prove

$$\forall x \exists y\ (x = 2 \times y \vee x = 2 \times y + 1)$$

?
Need to know something about $=$, $+$, $\times$...
Axioms

Too many axioms

What is a definition?
Define 1 as $S(0)$

(a) add a constant 1 an axiom $1 = S(0)$
(b) pretend you have read $S(0)$ each time you read 1

Constant + axiom

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash \forall x \forall y\ (x = y \Rightarrow P(x) \Rightarrow P(y))}\ \text{axiom}}{\Gamma \vdash \forall y\ (1 = y \Rightarrow P(1) \Rightarrow P(y))}\ \forall\text{-elim}}{\Gamma \vdash 1 = S(0) \Rightarrow P(1) \Rightarrow P(S(0))}\ \forall\text{-elim} \qquad \dfrac{}{\Gamma \vdash 1 = S(0)}\ \text{axiom}}{\Gamma \vdash P(1) \Rightarrow P(S(0))}\ \Rightarrow\text{-elim}$$

where $\Gamma = \{1 = S(0), \forall x \forall y\ (x = y \Rightarrow P(x) \Rightarrow P(y))\}$

Replace 1 by $S(0)$

$$\dfrac{\overline{P(1) \vdash P(S(0))}\ \text{axiom}}{\vdash P(1) \Rightarrow P(S(0))}\ \Rightarrow\text{-into}$$

uses no axioms

Deduction modulo a congruence

$$\frac{}{P(1) \vdash P(S(0))} \text{ axiom}$$

a constant 1
an equivalence relation $\equiv$ such that $1 \equiv S(0)$

$$\frac{}{\Gamma \vdash B} \text{ axiom if } A \in \Gamma \text{ and } A \equiv B$$

and the same for the other Natural deduction rule

The rules of Natural Deduction modulo a congruence

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-intro}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash C} \wedge\text{-intro if } C \equiv A \wedge B$$

Besides definitions

Instead of the axiom

$$\forall x \forall y \forall z \; ((x + y) + z = x + (y + z))$$

$(t + u) + v \equiv t + (u + v)$
and even $t + u + v$

But not too much

All provable propositions $A \equiv \top$

All provable propositions (including existential ones): a trivial proof

$$\frac{}{\vdash A}\ \top\text{-intro}$$

The conditions on the equivalence relation

1. Congruence: if $A \equiv A'$ and $B \equiv B'$ then $(A \wedge B) \equiv (A' \wedge B')$, etc.

2. Decidable: proof-checking must be decidable

3. Non confusing: if $A \equiv A'$, then either one is atomic or they have the same head symbol ($\wedge$, $\vee$, etc.) and sub-trees are equivalent (e.g. $A = B \wedge C$, $A' = B' \wedge C'$, $B \equiv B'$, and $C \equiv C'$)

Theories in Deduction modulo

A set of *axioms* + a decidable and non confusing congruence
Purely axiomatic, purely computational

A provable in $\mathcal{T}, \equiv$, if there exists finite subset Γ of $\mathcal{T}$ s.t. $\Gamma \vdash A$ has a proof modulo $\equiv$

Congruences defined with reduction (rewrite) rules

$$
\begin{gathered}
0 + y \longrightarrow y \\
S(x) + y \longrightarrow S(x + y) \\
0 \times y \longrightarrow 0 \\
S(x) \times y \longrightarrow x \times y + y
\end{gathered}
$$

$(2 \times 2 = 4) \equiv (4 = 4)$?

An example

$$(2 \times 2 = 4) \equiv (4 = 4)$$

In $\forall x\ (x = x)$, $\equiv$, the number 4 can be proved even

$$\cfrac{\cfrac{\overline{\Gamma \vdash \forall x\ (x = x)}\ \text{axiom}}{\Gamma \vdash 2 \times 2 = 4}\ \forall\text{-elim}}{\Gamma \vdash \exists x\ (2 \times x = 4)}\ \exists\text{-intro}$$

Decidable congruence: congruence = computation part of proofs, deduction rules = deduction part

Another example

$x \subseteq y \equiv (\forall z\ (z \in x \Rightarrow z \in y))$

$$
\dfrac{\dfrac{\overline{z \in A \vdash z \in A}\ \text{axiom}}{\vdash z \in A \Rightarrow z \in A}\ \Rightarrow\text{-intro}}{\vdash A \subseteq A}\ \forall\text{-intro}
$$

Not more... better

For every theory $\mathcal{T}, \equiv$, a purely axiomatic theory $\mathcal{T}'$ s.t. A provable in $\mathcal{T}, \equiv$ iff A provable in $\mathcal{T}'$

Not more provable propositions... better proofs

On-going research

$$((A \Rightarrow B) \wedge (A \Rightarrow C)) \equiv (A \Rightarrow (B \wedge C))$$

Message to take home

Provable sequents: inductively defined
Proofs: derivations

Constructive proof

Theory can be defined with axioms or with rewrite rules

Tomorrow

An example of theory: Arithmetic

A completely new topic: Simply typed lambda-calculus