Natural deduction
0. What we have seen so far
Fundamental notions: inductive definitions and language in general

A particular case: the languages of predicate logic
I. Deduction rules
The set of provable proposition

An inductive definition

\[
\begin{align*}
A \Rightarrow B & \\
\hline
A & \\
B & \\
\hline
P \Rightarrow Q & \Rightarrow R \\
\hline
\neg P & \\
\hline
\neg Q & \\
\hline
\end{align*}
\]

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, $\Gamma \vdash A$

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

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

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

Prove $P \vdash Q \Rightarrow P$
\[\begin{align*}
\Gamma & \vdash A \quad \Gamma & \vdash B \\
\hline
\Gamma & \vdash A \land B & \text{\land-intro}
\end{align*}\]

\[\begin{align*}
\Gamma & \vdash A \land B \\
\hline
\Gamma & \vdash A & \text{\land-elim}
\end{align*}\]

\[\begin{align*}
\Gamma & \vdash A \land B \\
\hline
\Gamma & \vdash B & \text{\land-elim}
\end{align*}\]
The classification of the rules

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

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

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

introduction / elimination
\[
\Gamma \vdash A \\
\frac{}{\Gamma \vdash A \lor B} \lor\text{-intro} \\
\frac{}{\Gamma \vdash A \lor B} \lor\text{-intro} \\
\frac{\Gamma \vdash A \lor B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \lor\text{-elim}
\]
\[
\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \quad \Rightarrow\text{-intro}
\]

\[
\frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \quad \Rightarrow\text{-elim}
\]
\[ \frac{\Gamma \vdash A}{\Gamma \vdash \forall x \ A} \quad \forall\text{-intro if } x \notin FV(\Gamma) \]

\[ \frac{\Gamma \vdash \forall x \ A}{\Gamma \vdash (t/x)A} \quad \forall\text{-elim} \]
\[
\frac{\Gamma \vdash (t/x)A}{\Gamma \vdash \exists x A} \quad \exists\text{-intro}
\]

\[
\frac{\Gamma \vdash \exists x A \quad \Gamma, A \vdash B}{\Gamma \vdash B} \quad \exists\text{-elim if } x \not\in FV(\Gamma, B)
\]
\[ \Gamma \vdash \top \quad \text{T-intro} \]

\[ \Gamma \vdash \bot \quad \Gamma \vdash A \quad \bot\text{-elim} \]
\[ \Gamma \vdash A \text{ axiom if } A \in \Gamma \]

\[ \Gamma \vdash A \lor \neg A \text{ excluded-middle} \]
No rules for $\neg$ and $\iff$

$\neg A$ abbreviation for $A \Rightarrow \bot$

$A \iff B$ abbreviation for $(A \Rightarrow B) \land (B \Rightarrow A)$
**Substitution**

In ∀-elim and ∃-intro: a auxiliary operation: substitution \((t/x)u\)

\[
\frac{Γ ⊢ ∀x\ A}{Γ ⊢ (t/x)A} \quad ∀\text{-elim}
\]

\[
\frac{Γ ⊢ (t/x)A}{Γ ⊢ ∃x\ A} \quad ∃\text{-intro}
\]

From ∀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

\[ (t/x)(f(u_1, \ldots, u_n)) = f((t/x)u_1, \ldots, (t/x)u_n) \]

\[ (t/x)x = t \]

\[ (t/x)y = y \text{ if } x \neq y \]
For languages with binders

\[(4/x)(\forall x \ P(x)) = \forall x \ P(4) \text{ or } \forall x \ P(x) \] ?

**Rule 1: substitute free variables only**

First attempt:

- \[\langle t/x \rangle (\forall y \ A) = \forall y (\langle t/x \rangle A) \text{ if } x \neq y\]
- \[\langle t/x \rangle (\forall x \ A) = \forall x \ A\]
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 (\( \alpha \)-equivalence)
Alphabetic equivalence

\[ \forall x \ A \sim \forall y \ B \text{ If for all variables } z \text{ that occur neither in } \forall x \ A \text{ not in } \forall y \ B \text{ on a } \langle z/x \rangle A \sim \langle z/y \rangle B \]

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

From now on: classes of expressions modulo alphabetic equivalence
Substitution (finally...)

\[(t/x)(\forall y \ A) = \forall z (t/x)(z/y)A\] 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, programming 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 \( \Gamma \) 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 $n + 1 \notin P$?
\[ P(0), \neg P(S(S(0))) \vdash \exists x \ (P(x) \land \neg P(S(x))) \]

\[ \pi_1 \]

\[
\begin{array}{c}
\Gamma, P(S(0)) \vdash P(S(0)) \\
\hline
\Gamma, P(S(0)) \vdash \neg P(S(S(0)))
\end{array}
\]

\[
\begin{array}{c}
\Gamma, P(S(0)) \vdash P(S(0)) \land \neg P(S(S(0)))
\end{array}
\]

\[
\begin{array}{c}
\Gamma, P(S(0)) \vdash \exists x \ (P(x) \land \neg P(S(x)))
\end{array}
\]

where \( \Gamma = \{ P(0), \neg P(S(S(0))) \} \)
\[ \pi_2 \]

\[
\begin{align*}
\Gamma, \neg P(S(0)) & \vdash P(0) & \Gamma, \neg P(S(0)) & \vdash \neg P(S(0)) \\
\Gamma, \neg P(S(0)) & \vdash P(0) \land \neg P(S(0)) \\
\Gamma, \neg P(S(0)) & \vdash \exists x \ (P(x) \land \neg P(S(x)))
\end{align*}
\]

Finally

\[
\begin{align*}
\Gamma & \vdash P(S(0)) \lor \neg P(S(0)) & \pi_1 \\
\Gamma, P(S(0)) & \vdash A & \Gamma, \neg P(S(0)) & \vdash A \\
\Gamma & \vdash A & \pi_2
\end{align*}
\]

where \( A = \exists x \ (P(x) \land \neg P(S(x))) \)
We can prove

\[ \exists x \ (P(x) \land \neg P(S(x))) \]

Can we prove

\[ P(n) \land \neg P(S(n)) \]

for some natural number \( n \)?

No: easy to prove that for each number \( n \)

\[ P(0), \neg P(S(S(0))) \vdash P(n) \land \neg P(S(n)) \]

not provable
Without any axioms

We can prove

$$\exists x \ (P(0) \Rightarrow \neg P(S(S(0)))) \Rightarrow (P(x) \land \neg P(S(x))))$$

We can prove

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

for no natural number $n$
The notion of witness

\[ E \text{ has the witness property if} \]
\[ \text{when } \exists x \ A \text{ is in } E, \text{ there exists } t \text{ such that } (t/x)A \text{ is in } E \]

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 \( \pi_1 \) and \( \pi_2 \).

Then a proof by case:

\[
\begin{align*}
\pi_1 & \quad \Gamma, P(S(0)) \vdash A \\
\pi_2 & \quad \Gamma, \neg P(S(0)) \vdash A
\end{align*}
\]

\[
\frac{
\pi_1 \\
\pi_2
}{\Gamma \vdash A}
\]

0 or \( S(0) \)?
But still needs to prove $P(S(0)) \lor \neg P(S(0))$

The excluded-middle rule
$(A \lor \neg A)$ 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 \( \pi \) of

\[ \forall x \exists y \ (x = 2 \times y \lor x = 2 \times y + 1) \]

A proof of the proposition

\[ \exists y \ (25 = 2 \times y \lor 25 = 2 \times y + 1) \]

Extract a witness from this proof

By construction, correct with respect to specification

\[ x = 2 \times y \lor x = 2 \times y + 1 \]
III. Theories
How can we prove

\[ \forall x \exists y \ (x = 2 \times y \lor x = 2 \times y + 1) \]

Need to know something about \(=, +, \times\)...
Axioms
Too many axioms

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

(a) add a constant 1 as an axiom $1 = S(0)$
(b) pretend you have read $S(0)$ each time you read 1
\[\Gamma \vdash \forall x \forall y \ (x = y \Rightarrow P(x) \Rightarrow P(y)) \quad \text{axiom}\]

\[\Gamma \vdash \forall y \ (1 = y \Rightarrow P(1) \Rightarrow P(y)) \quad \text{\forall-elim}\]

\[\Gamma \vdash 1 = S(0) \Rightarrow P(1) \Rightarrow P(S(0)) \quad \text{\forall-elim}\]

\[\Gamma \vdash 1 = S(0) \quad \text{axiom}\]

\[\Gamma \vdash P(1) \Rightarrow P(S(0)) \quad \Rightarrow\text{-elim}\]

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

\[
\frac{P(1) \vdash P(S(0))}{\vdash P(1) \Rightarrow P(S(0))} \quad \text{axiom}
\]

\[
\Rightarrow\text{-into}
\]

uses no axioms
Deduction modulo a congruence

\[ P(1) \vdash P(S(0)) \]  \text{axiom}

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

\[ \Gamma \vdash B \]  \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

\[
\begin{aligned}
\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \land B} & \quad \land\text{-intro} \\
\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash C} & \quad \land\text{-intro if } C \equiv A \land B
\end{aligned}
\]
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

$\vdash A$ $\top$-intro
The conditions on the equivalence relation

1. **Congruence**: if \( A \equiv A' \) and \( B \equiv B' \) then \( (A \land B) \equiv (A' \land B') \), 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 (\( \land \), \( \lor \), etc.) and sub-trees are equivalent (e.g. \( A = B \land C \), \( A' = B' \land C' \), \( B \equiv B' \), 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 $\Gamma$ of $\mathcal{T}$ s.t. $\Gamma \vdash A$ has a proof modulo $\equiv$
Congruences defined with reduction (rewrite) rules

\[
\begin{align*}
0 + y & \longrightarrow y \\
S(x) + y & \longrightarrow S(x + y) \\
0 \times y & \longrightarrow 0 \\
S(x) \times y & \longrightarrow x \times y + y
\end{align*}
\]

\((2 \times 2 = 4) \equiv (4 = 4)\,?\)
An example

\[(2 \times 2 = 4) \equiv (4 = 4)\]

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

\[
\begin{align*}
\Gamma \vdash \forall x \ (x = x) & \quad \text{axiom} \\
\Gamma \vdash 2 \times 2 = 4 & \quad \forall\text{-elim} \\
\Gamma \vdash \exists x \ (2 \times x = 4) & \quad \exists\text{-intro}
\end{align*}
\]

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

\[ x \subseteq y \equiv (\forall z \ (z \in x \Rightarrow z \in y)) \]

\[
\begin{array}{c}
\dfrac{
\frac{z \in A}{\vdash z \in A}
\hline
\vdash z \in A \Rightarrow z \in A
}{\vdash A \subseteq A}
\end{array}
\]

\text{axiom}\quad \Rightarrow\text{-intro}\quad \forall\text{-intro}
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

\[ ((A \Rightarrow B) \land (A \Rightarrow C)) \equiv (A \Rightarrow (B \land C)) \]
Message to take home

Provable sequents: inductively defined
Proofs: derivations

Constructive proof

Theory can be defined with axioms or with rewrite rules
An example of theory: Arithmetic

A completely new topic: Simply typed lambda-calculus