The Notion of theory
1. What we have seen before the break
Natural deduction rules

Introductions, eliminations, axiom, excluded-middle
Define a notion of provable sequent $\Gamma \vdash A$ (and of proof)

$A$ is provable (without any axioms), if $\vdash A$ provable
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
Classical and constructive proofs

Set of provable propositions: no witness property. Proof of

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

but no term t such that a proof of

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

Origin: excluded-middle rule

Proofs without the excluded-middle: constructive

Set of constructively provable propositions: witness property
How to prove it?

Cut: proof ending with an elimination rule whose main premise is proved by an introduction rule on the same symbol

\[
\begin{align*}
\pi &\quad \pi' \\
\Gamma \vdash A &\quad \Gamma \vdash B \\
\Gamma \vdash A \land B &\quad \land\text{-intro} \\
\Gamma \vdash A &\quad \land\text{-elim}
\end{align*}
\]

and a cut-elimination algorithm
Prove the termination of this algorithm
A proof $\pi$ that is (1.) constructive, (2.) cut-free, and (3.) without any axioms ends with an introduction rule:

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

witness $t$
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

$$x = 2 \times y \lor x = 2 \times y + 1$$
II. Deduction modulo theory
Final rule

An introduction (hence witness property)

(1) constructive (2) cut-free (3) without any axioms

(2) is not a restriction once we have proved cut-elimination
(1) many proofs do not use the excluded-middle
(3) is a real limitation: to prove

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

need to know something about =, +, ×...
In general: failure

\[ \exists x \ P(x) \vdash \exists x \ P(x) \text{ axiom} \]

Final rule: axiom rule
Also: failure of the witness property

But in some cases...
An example: definitions

1: abbreviation for the term $S(0)$

What does this mean?
(a) add a constant 1 an axiom $1 = S(0)$
(b) pretend you have read $S(0)$ each time you read 1
Constant + axiom

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

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

Cut-free, but ends but with an elimination rule
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

ends with an introduction rule
Deduction modulo theory

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

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

\[
\Gamma \vdash A \equiv B \quad \text{axiom if } A \in \Gamma \text{ and } A \equiv B
\]

and the same for the other Natural deduction rule
The rules of Natural Deduction modulo theory

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

\[\begin{array}{c}
\hline
\vdash A \\
\end{array}\]
\(\top\)-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 \( C \equiv C' \))
Why is non confusion important?

If $\exists A \equiv \top$ then a proof of $\exists A$ that ends with an introduction rule, may end with a $\top$-intro rule. The final rule property may fail to imply the witness property.

If $(A \lor B) \equiv (C \land D)$

$\vdash C \land D \land$-elim

$\vdash C \land$-intro

$\vdash A \lor$-intro

$\vdash A$

$\vdash C \land D \land$-elim

$\vdash C$

How can we reduce this cut?
Theories in Deduction modulo theory

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 $\equiv$
An example

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

In \(\emptyset, \equiv\), the number 4 can be proved even

\[
\begin{align*}
\vdash 2 \times 2 &= 4 & \top\text{-intro} \\
\vdash \exists x \ (2 \times x &= 4) & \exists\text{-intro}
\end{align*}
\]

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

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

\[
\begin{align*}
&\frac{z \in A}{\vdash z \in A} \quad \text{axiom} \\
&\vdash z \in A \Rightarrow z \in A \quad \Rightarrow\text{-intro} \\
&\vdash A \subseteq A \quad \forall\text{-intro}
\end{align*}
\]
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

\[(A \Rightarrow B) \land (A \Rightarrow C) \equiv (A \Rightarrow (B \land C))\]
III. Congruences defined with reduction rules
Congruences often defined with reduction (rewrite) rules, e.g.

\[
\begin{align*}
0 + y & \rightarrow y \\
S(x) + y & \rightarrow S(x + y) \\
0 \times y & \rightarrow 0 \\
S(x) \times y & \rightarrow x \times y + y \\
0 = 0 & \rightarrow \top \\
S(x) = 0 & \rightarrow \bot \\
0 = S(y) & \rightarrow \bot \\
S(x) = S(y) & \rightarrow x = y
\end{align*}
\]
An exercise

Reduce $S(S(0)) \times S(S(0)) = S(S(S(S(0))))$
Reduction rules

Reduction rule: ordered pair \( l \rightarrow r \) of terms or propositions

Reduction system: set of reduction rules

\( t \) reduces in one step at the root to \( u \): \( t = \sigma l, \ u = \sigma r \)

\( t \) reduces in one step to \( u \) (\( t \rightarrow^1 u \)): \( t = C[\sigma l], \ u = C[\sigma r] \)

reducible: reduces in one step to some \( u \), irreducible otherwise
reduction sequence: (finite or infinite) sequence $t_0, t_1...$ s.t. $t_i \rightarrow^1 t_{i+1}$

$t$ reduces to $u$ ($t \rightarrow^* u$): a finite reduction sequence from $t$ to $u$

$t$ reduces in at least one step to $u$ ($t \rightarrow^+ u$): $t \rightarrow^1 v \rightarrow^* u$

$u$ is a irreducible form of $t$: $t \rightarrow^* u$ and $u$ irreducible

congruence sequence: finite or infinite sequence $t_0, t_1...$ s.t. $t_i \rightarrow^1 t_{i+1}$ or $t_{i+1} \rightarrow^1 t_i$

$t$ and $u$ are congruent ($t \equiv u$): a finite congruence sequence from $t$ to $u$
Decidability

≡: a congruence by construction

\( t \) \textbf{terminates}: it has a irreducible form, i.e. a finite reduction sequence from \( t \) to a irreducible expression

\( t \) \textbf{strongly terminates}: all reduction sequences starting from \( t \) finite

\( R \) \textbf{terminates} (resp. \textbf{strongly terminates}) if all \( t \) do

\( R \) \textbf{confluent}: whenever \( t \) reduces to \( u_1 \) and \( u_2 \), there exists \( v \) s.t. \( u_1 \) reduces to \( v \) and \( u_2 \) reduces to \( v \)
Decidability

\[ R \text{ strongly terminating and confluent} \]
- each \( t \) has exactly one irreducible form
- this irreducible form can be computed from \( t \)
- \( t \equiv u \) if \( t \) and \( u \) same irreducible form

Thus \( \equiv \) decidable
Non confusion

$R$ confluent and reduces terms to terms and atomic propositions to propositions, the congruence is non confusing

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

$A \land \neg A \rightarrow \bot$
IV. Cuts in Deduction modulo theory
What is a cuts in Deduction modulo theory?

Same as in Predicate logic:

A proof ending with an elimination rule whose main premise is proved by an introduction rule on the same symbol
Failure of termination of proof reduction

For some theories: e.g. $P \rightarrow (P \Rightarrow Q)$

\[
\begin{align*}
 P \vdash P \Rightarrow Q \quad \text{axiom} & \quad P \vdash P \quad \text{axiom} \\
 \quad & \Rightarrow\text{-elim} \\
 \quad & \Rightarrow\text{-intro} \\
 \vdash P \Rightarrow Q & \Rightarrow\text{-elim} \\
 \end{align*}
\]
An exercise

Prove that the sequent $\vdash Q$ has no cut-free proof
But when proof-reduction terminates

Cut-free proofs have the same properties than in Predicate logic. A proof that is (1) constructive (2) cut-free and (3) in a purely computational theory ends with an introduction rule.

All (1) purely computational theories where (2) proof-reduction terminates have the witness property.
Next time

The notion of model