The Notion of theory

I. 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 Γ 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

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

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

A proof π of $\exists x \ A$ that is (1.) constructive, (2.) cut-free, and (3.) without any axioms ends with a \exists -intro rule:

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

witness t

Why do we care? Programming with proofs

A constructive proof π 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 =, +, \times ...

In general: failure

$\exists x \ P(x) \vdash \exists x \ P(x)$ 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

$$\begin{array}{l} \overline{\Gamma \vdash \forall x \forall y \ (x = y \Rightarrow P(x) \Rightarrow P(y))} \stackrel{\text{axiom}}{\Gamma \vdash \forall y \ (1 = y \Rightarrow P(1) \Rightarrow P(y))} \stackrel{\forall \text{-elim}}{\forall \text{-elim}} \\ \overline{\Gamma \vdash 1 = S(0) \Rightarrow P(1) \Rightarrow P(S(0))} \stackrel{\forall \text{-elim}}{\forall \text{-elim}} \\ \overline{\Gamma \vdash 1 = S(0), \forall x \forall y \ (x = y \Rightarrow P(x) \Rightarrow P(y))} \stackrel{\text{axiom}}{\Rightarrow \text{-elim}} \\ \text{where } \Gamma = \{1 = S(0), \forall x \forall y \ (x = y \Rightarrow P(x) \Rightarrow P(y))\} \\ \text{Cut-free, but ends but with an elimination rule} \end{array}$$

Replace 1 by S(0)

$$\frac{\overline{P(1) \vdash P(S(0))}}{\vdash P(1) \Rightarrow P(S(0))} \stackrel{\text{axiom}}{\Rightarrow \text{-intro}}$$

uses no axioms ends with an introduction rule

Deduction modulo theory

$$\overline{P(1) \vdash P(S(0))}^{\mathsf{axiom}}$$

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

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

and the same for the other Natural deduction rule

The rules of Natural Deduction modulo theory

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

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

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

 $\overline{\vdash A}$ \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 $C \equiv C'$)

Why is non confusion important?

If $\exists x \ A \equiv \top$ then a proof of $\exists x \ A$ 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
$$(A \lor B) \equiv (C \land D)$$

$$\frac{\overbrace{\vdash A}}{\vdash C \land D} \lor -\text{intro} \\ \xrightarrow{\vdash C} \land -\text{elim}$$

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 Γ 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

$$\frac{\overline{\vdash 2 \times 2 = 4}}{\vdash \exists x \ (2 \times x = 4)} \overline{\langle x, 2 \times x = 4, 2 \rangle} \exists \text{-intro}$$

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

Another example

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

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

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

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

III. Congruences defined with reduction rules

$$(2 \times 2 = 4) \equiv \top$$
?
Congruences often defined with reduction (rewrite) rules, e.g.

$$0 + y \longrightarrow y$$

$$S(x) + y \longrightarrow S(x + y)$$

$$0 \times y \longrightarrow 0$$

$$S(x) \times y \longrightarrow x \times y + y$$

$$0 = 0 \longrightarrow \top$$

$$S(x) = 0 \longrightarrow \bot$$

$$0 = S(y) \longrightarrow \bot$$

$$S(x) = S(y) \longrightarrow x = y$$



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

Reduction rules

Reduction rule: ordered pair $I \longrightarrow r$ of terms or propositions

Reduction system: set of reduction rules

t reduces in one step at the root to u: $t = \sigma I$, $u = \sigma r$

t reduces in one step to u $(t \longrightarrow^{1} u)$: $t = C[\sigma I] u = C[\sigma r]$

reducible: reduces in one step to some *u*, irreducible otherwise

reduction sequence: (finite or infinite) sequence $t_0, t_1...$ s.t. $t_i \longrightarrow^1 t_{i+1}$

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

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

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. $t_i \longrightarrow^1 t_{i+1}$ or $t_{i+1} \longrightarrow^1 t_i$

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

Decidability

 \equiv : a congruence by construction

t terminates: it has a irreducible form, i.e. a finite reduction sequence from t to a irreducible expression

t strongly terminates: all reduction sequences starting from t finite

R terminates (resp. strongly terminates) if all t do

R 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 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

 $\mathsf{Thus} \equiv \mathsf{decidable}$

Non confusion

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

$$x \subseteq y \longrightarrow \forall z \ (z \in x \Rightarrow z \in y)$$
$$A \land \neg A \longrightarrow \bot$$

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. $P \longrightarrow (P \Rightarrow Q)$





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