Foundations of proof systems

You have taken a course in logic

Deduction rule
Classical and constructive proof
Last rule property, programming with proofs
Proofs in axiomatic theories: arithmetic, set theory...
...

How do you prove that $S(S(0)) + S(S(0)) = S(S(S(S(0))))$?

You have taken a course on rewriting

Rewrite rule
Termination, confluence
...

How do you prove that $S(S(0)) + S(S(0)) = S(S(S(S(0))))$?

Last rule property

An introduction rule (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

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

need to know something about $=$, $+$, $\times$...

In general: failure

$$\frac{}{\exists x\ P(x) \vdash \exists x\ P(x)}\ \text{axiom}$$

Final rule: axiom rule

Also: failure of the witness property

But in some cases...

An example: definitions

1: abbreviation for the 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

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

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

Cut-free, but ends but with an elimination rule

Replace 1 by $S(0)$

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

uses no axioms

ends with an introduction rule

Deduction modulo theory

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

a constant 1

a rewrite rule $1 \longrightarrow S(0)$

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

and the same for the other Natural deduction rule

The rules of Natural Deduction modulo theory

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

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

Theories in Deduction modulo theory

A set of axioms + a set of rewrite rule

Besides definitions

Instead of the axioms

$$\forall x \forall y \ (0 + y = y)$$

$$\forall x \forall y \ (S(x) + y = S(x + y))$$

the rules

$$0 + y \longrightarrow y$$

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

Multiplication

$$0 \times y \longrightarrow 0$$

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

An exercise

How do you prove

$$S(S(0)) + S(S(0)) = S(S(S(S(0))))$$

?

But not too much

All provable propositions $A \longrightarrow \top$

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

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

Dedidability of $\equiv$

Another example

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

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

How far can we go?

Arithmetic?

(1) Axioms of equality
(2) The axioms of successor

$$\forall x \forall y \ (S(x) = S(y) \Rightarrow x = y)$$

$$\forall x \ \neg 0 = S(x)$$

(3) Induction
(4) The axioms of addition and multiplication

The axioms of successor

A function symbol *Pred*
A predicate symbol *Null*

$$Pred(0) \longrightarrow 0$$

$$Pred(S(x)) \longrightarrow x$$

$$Null(0) \longrightarrow \top$$

$$Null(S(x)) \longrightarrow \bot$$

An exercise

Prove

$$\forall x \forall y \ (S(x) = S(y) \Rightarrow x = y)$$

$$\forall x \ \neg 0 = S(x)$$

The big question: induction

No other numbers than those constructed with 0 and S
Every class containing 0 and closed by S contains everything
Besides ι, a sort κ for classes, a predicate symbol ϵ

Induction axiom

$$\forall c\ (0\ \epsilon\ c \Rightarrow \forall x\ (x\ \epsilon\ c \Rightarrow S(x)\ \epsilon\ c) \Rightarrow \forall y\ y\ \epsilon\ c)$$

Comprehension axiom scheme: existence of some classes

$$\forall x_1 ... \forall x_n \exists c \forall y\ (y\ \epsilon\ c \Leftrightarrow A)$$

if A does not contain ϵ (predicative arithmetic)

Now two problems instead of one

The comprehension scheme

$$\forall x_1 ... \forall x_n \exists c \forall y \ (y \ \epsilon \ c \Leftrightarrow A)$$

Introduce a notation for this class: $f_{x_1,...,x_n,y,A}(x_1, ..., x_n)$

$$\forall x_1 ... \forall x_n \forall y \ (y \ \epsilon \ f_{x_1,...,x_n,y,A}(x_1, ..., x_n) \Leftrightarrow A)$$

$$y \ \epsilon \ f_{x_1,...,x_n,y,A}(x_1, ..., x_n) \longrightarrow A$$

The induction axiom

All objects of sort ι are natural numbers
Alternative: not all objects are natural numbers, a predicate symbol N for the natural numbers

$$\forall c\ (0\ \epsilon\ c \Rightarrow \forall x\ (x\ \epsilon\ c \Rightarrow S(x)\ \epsilon\ c) \Rightarrow \forall y\ (N(y) \Rightarrow y\ \epsilon\ c))$$

More axioms

$$N(0)$$

$$\forall x\ (N(x) \Rightarrow N(S(x)))$$

$$\forall y\ (N(y) \Rightarrow \forall c\ (0\ \epsilon\ c \Rightarrow \forall x\ (N(x) \Rightarrow x\ \epsilon\ c \Rightarrow S(x)\ \epsilon\ c) \Rightarrow y\ \epsilon\ c))$$

Converse provable (with $N(0)$ and $\forall x\ (N(x) \Rightarrow N(S(x)))$)
Alternative:

$$\forall y\ (N(y) \Leftrightarrow \forall c\ (0\ \epsilon\ c \Rightarrow \forall x\ (x\ \epsilon\ c \Rightarrow S(x)\ \epsilon\ c) \Rightarrow y\ \epsilon\ c))$$

($N(0)$ and $\forall x\ (N(x) \Rightarrow N(S(x)))$ dropped)

$$N(y) \longrightarrow \forall c\ (0\ \epsilon\ c \Rightarrow \forall x\ (N(x) \Rightarrow x\ \epsilon\ c \Rightarrow S(x)\ \epsilon\ c) \Rightarrow y\ \epsilon\ c)$$

The definition of natural numbers

Equality

Classes also used to define equality

$$x = y \longrightarrow \forall c \ (x \ \epsilon \ c \Rightarrow y \ \epsilon \ c)$$

Arithmetic as a purely computational theory

$$0 + y \longrightarrow y$$

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

$$0 \times y \longrightarrow 0$$

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

$$\mathit{Pred}(0) \longrightarrow 0$$

$$\mathit{Pred}(S(x)) \longrightarrow x$$

$$\mathit{Null}(0) \longrightarrow \top$$

$$\mathit{Null}(S(x)) \longrightarrow \bot$$

$$x = y \longrightarrow \forall c\ (x\ \epsilon\ c \Rightarrow y\ \epsilon\ c)$$

$$N(y) \longrightarrow \forall c\ (0\ \epsilon\ c \Rightarrow \forall x\ (x\ \epsilon\ c \Rightarrow S(x)\ \epsilon\ c) \Rightarrow y\ \epsilon\ c)$$

$$y\ \epsilon\ f_{x_1,\ldots,x_n,y,A}(x_1, \ldots, x_n) \longrightarrow A$$

Deduction rules + computation rules

Everywhere in (contemporary) logic: Martin-Löf's type theory, the Calculus of Constructions...

But also Automated theorem proving

A resurection of the notion of theory

Interoperability

Libraries (encyclopedia)

The course *Foundations of proof systems*

The algorithmic interpretation of proofs (Curry-de Bruijn-Howard interpretation)

Deduction rules + computation rules

Theories

Along the way: Proof-checking systems

Simple type theory: HOL, HOL-light, Isabelle/HOL, PVS

$\lambda\Pi$: Twelf

$\lambda\Pi$-modulo: Dedukti

Martin-Löf's type theory: Agda

The Calculus of constructions: Coq