Deduction modulo rewriting I

An exercise

Take the axiom

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

Can you prove (for example, in Natural deduction)

$$(a+b)+((c+(d+e))+(f+g)) = (a+(b+c))+((d+(e+f))+g)$$

?

An exercise

$$
\begin{aligned}
(a+b)+((c+(d+e))+(f+g)) &= (a+(b+c))+((d+(e+f))+g) \\
a+(b+((c+(d+e))+(f+g))) &= (a+(b+c))+((d+(e+f))+g) \\
a+(b+(c+((d+e)+(f+g)))) &= (a+(b+c))+((d+(e+f))+g) \\
a+(b+(c+(d+(e+(f+g))))) &= (a+(b+c))+((d+(e+f))+g) \\
a+(b+(c+(d+(e+(f+g))))) &= a+((b+c)+((d+(e+f))+g)) \\
a+(b+(c+(d+(e+(f+g))))) &= a+(b+(c+((d+(e+f))+g))) \\
a+(b+(c+(d+(e+(f+g))))) &= a+(b+(c+(d+((e+f)+g)))) \\
a+(b+(c+(d+(e+(f+g))))) &= a+(b+(c+(d+(e+(f+g)))))
\end{aligned}
$$

8 steps: at each step $\sim$ 9 possibilities

A search space of $\sim 9^8 \sim 50,000,000$ possibilities

One per microsecond: $\sim$ 1mn to solve this problem

No need to explore such a large search space

Knuth-Bendix: orient the axiom

$$(x + y) + z = x + (y + z)$$

into a rewrite rule

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

Reduces (by a factor of 2) branching, but does not eliminate it

Confluence: completely eliminates branching

Another example

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

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

$$\forall y\ (0 \times y = 0)$$

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

Prove

$$S^{10}(0) + S^{10}(0) = S^{20}(0)$$

$$S^{10}(0) + S^{10}(0) = S^{20}(0 \times 0)$$

$$S^{10}(0) + S^{10}(0) = S^{19}(0 \times 0 + 0)$$

$$\dots$$

Don't use deduction rules for that

Natural deduction (Sequent calculus, Frege-Hilbert systems, Resolution...) permit to build proofs with deduction rules

Not enough: proof is made of deduction and computation

But a proof is not just made of computation: 221

Another 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

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

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

Replace 1 by $S(0)$

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

I. Deduction modulo theory
(a.k.a. Deduction modulo rewriting)

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

a constant 1
a congruence $\equiv$ 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 theory

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

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

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 (for example, $A = B \wedge C$, $A' = B' \wedge C'$, $B \equiv B'$, and $C \equiv C'$)

Congruences defined with rewrite rules

$\equiv$: same normal form for confluent and terminating rewrite system

$\equiv$: smallest congruence containing one step reduction

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

$$
\dfrac{\dfrac{}{\Gamma \vdash \forall x\ (x = x)}\ \text{axiom}}{\Gamma \vdash S^{10}(0) + S^{10}(0) = S^{20}(0)}\ \forall\text{-elim}
$$

Another example

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

$$\dfrac{\dfrac{}{\Gamma \vdash \forall x\ (x = x)}\ \text{axiom}}{\Gamma \vdash (a + b) + ((c + (d + e)) + (f + g)) = (a + (b + c)) + ((d + (e + f)) + g)}\ \forall\text{-elim}$$

The oldest arithmetic algorithm

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

Rewrites ~~terms to terms~~ (atomic) propositions to propositions

An example

$$(2 \times 2 = 4) \longrightarrow^* \top$$

In $\varnothing, \equiv$, the number 4 can be proved even

$$\dfrac{\dfrac{}{\vdash 2 \times 2 = 4}\ \top\text{-intro}}{\vdash \exists x\ (2 \times x = 4)}\ \exists\text{-intro}$$

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

Another example

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

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

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 $\equiv$

Not more... better

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

Not more provable propositions... better proofs

II. Arithmetic in Deduction modulo theory

Comprehension

A two sorted-theory with a sort of natural numbers and one for classes of natural numbers

A 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)

Equality

Classes used to express the properties of equality

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

Exercise: prove reflexivity, symmetry, transitivity, and substitutivity

0 and S

$$Pred(0) = 0$$

$$\forall x\ (Pred(S(x)) = x)$$

$$Null(0)$$

$$\forall x\ \neg Null(S(x))$$

Exercise: prove

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

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

Being a natural number

Being a natural number: being in the smallest class containing 0 and closed by S

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

Exercise: prove

$$N(0)$$

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

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

Addition and multiplication

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

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

$$\forall y \ (0 \times y = 0)$$

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

How to use these axioms to prove $\forall y\ (y + 0 = y)$?

High school proof:
$0 + 0 = 0$
$\forall x\ (x + 0 = x \Rightarrow S(x) + 0 = S(x))$
hence $\forall y\ (y + 0 = y)$

Using the axioms

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

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

How do we know

$$0 + 0 = 0 \Rightarrow \forall x \ (x + 0 = x \Rightarrow S(x) + 0 = S(x)) \\ \Rightarrow \forall y \ (y + 0 = y) \ ?$$

How do we know

$$0+0=0 \Rightarrow \forall x\ (x+0=x \Rightarrow S(x)+0=S(x)) \\ \Rightarrow \forall y\ (y+0=y)\ ?$$

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

How do we know

$$0+0=0 \Rightarrow \forall x\ (x+0=x \Rightarrow S(x)+0=S(x)) \\ \Rightarrow \forall y\ (y+0=y)\ ?$$

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

$$\exists c \forall y\ (y \in c \Leftrightarrow y+0=y)$$

Differences with other formulations of arithmetic

- Classes and comprehension scheme (just like Peano did)
- A symbol N (just like Peano did)
- Slight variation in the axioms

Orienting the axioms as rewrite rules

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

Orienting the axioms as rewrite rules

$$Pred(0) \longrightarrow 0$$

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

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

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

Orienting the axioms as rewrite rules

$$0 + y \longrightarrow y$$

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

$$0 \times y \longrightarrow 0$$

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

Orienting the axioms as rewrite rules

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

The comprehension scheme

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

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

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

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

III. Cuts in Deduction modulo theory

Natural deduction rules

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

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

Without the excluded middle: constructivity

Constructively provable propositions: witness property

Each time $\exists x\ A$ provable

a term t and a proof of $(t/x)A$

How to prove it?

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

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A} \quad \dfrac{\pi'}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\ \wedge\text{-intro}}{\Gamma \vdash A}\ \wedge\text{-elim}$$

and a proof-reduction algorithm

Prove the termination of this algorithm

Final rule property

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:

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

witness t

Why do we care? 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

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

Final rule property

An introduction (hence witness property)

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

(2) is not a restriction once termination of proof-reduction proved
(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...

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: for example $P \longrightarrow (P \Rightarrow Q)$

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{P \vdash P \Rightarrow Q}\,\text{axiom}
\qquad
\dfrac{}{P \vdash P}\,\text{axiom}
}{P \vdash Q}\,\Rightarrow\text{-elim}
}{\vdash P \Rightarrow Q}\,\Rightarrow\text{-intro}
\qquad
\dfrac{
\dfrac{
\dfrac{}{P \vdash P \Rightarrow Q}\,\text{axiom}
\qquad
\dfrac{}{P \vdash P}\,\text{axiom}
}{P \vdash Q}\,\Rightarrow\text{-elim}
}{\vdash P}\,\Rightarrow\text{-intro}
}{\vdash Q}\,\Rightarrow\text{-elim}
$$

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

For example, arithmetic has the witness property

Thursday

How these ideas can be used to build a logical framework and an encyclopedia of formal proofs