The termination of proof reduction in Deduction modulo theory
I. What we have seen so far
Proof, theory, model

Examples of theories

Termination of proof-reduction in Predicate logic
Connecting the notions

Termination of proof-reduction in some theories

Main tool: the notion of model
II. Counter-examples and examples
Counter-examples

As we have seen

\[ P \rightarrow P \Rightarrow Q \]
\[ P \rightarrow Q \land \neg P \]

consistent but no termination of proof-reduction
Example

\[ P \rightarrow Q \Rightarrow Q \]

\( P \) abbreviation for \( Q \Rightarrow Q \)
Replace \( P \) by \( Q \Rightarrow Q \) everywhere

Or direct proof: \( R_Q \) set of all strongly terminating proof-terms
\( R_P = R_Q \Rightarrow Q \)
Instead of: \( R_P \) set of all strongly terminating proof-terms
Same proof as for predicat logic: associate a set $R_A$ of proof-terms to each proposition $A$.

Such that $R_A \Rightarrow_B$ the set of proof-terms $\pi$ such that $\pi$ strongly terminates and when $\pi$ reduces to $\lambda \alpha : A \; \pi_1$, then for every $\pi'$ in $R_A$, $(\pi' / \alpha) \pi_1$ in $R_B$, etc.

Extra condition: if $A \equiv B$ then $R_A = R_B$
III. Sets candidates to be associated to propositions
Naming operations

\[ R_{A \land B} = \text{set of proof-terms } \pi, \text{ such that } \pi \text{ strongly terminates and if } \pi \text{ reduces to } \langle \pi_1, \pi_2 \rangle \text{ then } \pi_1 \text{ in } R_A \text{ and } \pi_2 \text{ in } R_B \]

\[ E \tilde{\land} F = \text{set of proof-terms } \pi, \text{ such that } \pi \text{ strongly terminates and if } \pi \text{ reduces to } \langle \pi_1, \pi_2 \rangle \text{ then } \pi_1 \text{ in } E \text{ and } \pi_2 \text{ in } F \]

Then define \( R_{A \land B} \) as \( R_A \tilde{\land} R_B \)
Operations on sets of proof-terms

\[ \tilde{\wedge} \text{ maps } E \text{ and } F \text{ to the set of proof-terms } \pi, \text{ such that } \pi \text{ strongly terminates and if } \pi \text{ reduces to } \langle \pi_1, \pi_2 \rangle \text{ then } \pi_1 \in E \text{ and } \pi_2 \in F \]

\[ \Rightarrow \text{ maps } E \text{ and } F \text{ to the set of proof-terms } \pi, \text{ such that } \pi \text{ strongly terminates and if } \pi \text{ reduces to } \lambda \alpha : A \pi_1 \text{ then for every } \pi' \text{ in } E, \]
\[ (\pi' / \alpha) \pi_1 \in F \]

\[ \tilde{T}, \tilde{I}, \tilde{\lor}, \tilde{\land}, \tilde{\exists} \]
The set $\mathcal{C}$ of candidates (reducibility candidates) inductively defined as the smallest set of set of proof terms closed by these operations and intersection

- $\tilde{T}$ and $\tilde{\bot}$ are candidates
- if $E$ and $F$ are candidates, then $E \tilde{\land} F$, $E \tilde{\lor} F$, and $E \tilde{\Rightarrow} F$ are candidates
- if $S$ is a set of candidates, then $\tilde{\forall} S$ and $\tilde{\exists} S$ are candidates
- if $S$ is a set of candidates, then $\bigcap S$ is a candidate
IV. The algebra of candidates
To prove that proof-reduction terminate in $\equiv$

- Define a function $R$ mapping every proposition $A$ to a candidate $R_A$ s.t.
  1. $R_{A \land B} = R_A \wedge R_B$, $R_{A \Rightarrow B} = R_A \Rightarrow R_B$, etc.
  2. if $A \equiv B$, then $R_A = R_B$

- prove all proofs of $A$ are in $R_A$, hence strongly terminate
Because $R_{A \land B} = R_A \tilde{\land} R_B$, $R_{A \Rightarrow B} = R_A \tilde{\Rightarrow} R_B$, etc.
Once $R$ defined on atomic propositions, it extends in a unique way

A function mapping atomic propositions to candidates

For each predicate symbol $P$, a function $\overline{P}$ mapping tuples of terms to candidates: $R_P(t_1, \ldots, t_n) = \overline{P}(t_1, \ldots, t_n)$

In a first step associate, to each term $t$, an element of an arbitrary set $\mathcal{M}$ and then define a function $\hat{P}$ from $\mathcal{M}^n$ to $\mathcal{C}$

Just a model valued in the algebra $\mathcal{C}$, $R_A = [A]$
Condition (2.) rephrases:
if $A \equiv B$ then $[A] = [B]$
The algebra $\mathcal{C}$

Trivial pre-order relation $\leq$ defined by $\mathcal{C} \leq \mathcal{C}'$ always
operations $\tilde{\top}, \tilde{\bot}, \tilde{\land}, \tilde{\lor}, \tilde{\Rightarrow}, \tilde{\forall}$ and $\tilde{\exists}$ pre-Heyting algebra
(any set is)

Ordered $\subseteq$, complete $(\cap)$

Not a Heyting algebra
$\tilde{\top} \neq \tilde{\top} \Rightarrow \tilde{\top}$
\[ \lambda \alpha : A (\alpha \alpha) \text{ in } \tilde{\top} \text{ but not in } \tilde{\top} \Rightarrow \tilde{\top} \]
V. The termination of proof-term reduction
If $\mathcal{T}, \equiv$ has a model valued in the algebra $C$
Then every proof-term this theory strongly terminates
Four easy lemmas

If $C$ is a candidate, then all the elements of $C$ strongly terminate.

Let $C$ be a candidate and $\alpha$ a variable, then $\alpha \in C$.

If $C$ is a candidate, $\pi$ is an element of $C$ and $\pi \xrightarrow{*} \pi'$, then $\pi'$ is an element of $C$.

Let $C$ be a candidate and $\pi$ a proof-term that is an elimination and such that all one-step reducts of $\pi$ are in $C$, then $\pi$ is in $C$. 
Main theorem

≡ a congruence
\( \mathcal{M} \) a model valued in the algebra \( C \) of \( \equiv \)
\( \pi \) a proof-term of type \( A \) in a context \( \Gamma \)
\( \theta \) a substitution mapping variables to terms
\( \phi \) a valuation mapping variables to elements of \( \mathcal{M} \)
\( \sigma \) a substitution mapping any proof-term variable bound to proposition \( B \) in \( \Gamma \) to an element of \( \llbracket B \rrbracket_\phi \)

Then \( \sigma \theta \pi \) is an element of \( \llbracket A \rrbracket_\phi \)
Corollaries

If $\mathcal{T}, \equiv$ has a model valued in the algebra $\mathcal{C}$
Then every proof-term this theory strongly terminates

If $\mathcal{T}, \equiv$ is super-consistent
Then, every proof-term this theory strongly terminates
More corollaries

$\emptyset, \equiv$ purely computational and super-consistent

If there exists a proof of $A$, then there exists one that ends with an introduction rule.

If there exists a proof of $\exists x \, A$, then there exists a term $t$ and a proof of $(t/x)A$.
And corollaries of corollaries

Every proof-term in \textit{Arithmetic} strongly terminates
\textit{Arithmetic} has the witness property

Every proof-term in \textit{Simple type theory (with Peano numbers)} strongly terminates
\textit{Simple type theory (with Peano numbers)} has the witness property
VI. Proof-terms reduction in Arithmetic
A class that contains zero that is closed by successor

Two proofs that 100 is in this class

Express these proofs in HA or in Simple type theory with Peano numbers

Eliminating cuts in one yields the other
Proofs by induction

\[\pi\] proof of \(0 \in c\)
\[\pi'\] proof of \(\forall x (N(x) \Rightarrow x \in c \Rightarrow S(x) \in c)\)

\[\lambda y \lambda \alpha (\alpha \ c \ \pi \ \pi')\] proof of \(\forall y (N(y) \Rightarrow y \in c)\)
$$(((\lambda y \lambda \alpha (\alpha \ c \ \pi \ \pi')) \ S^{100}(0) \ \rho_{100})$$

where $\rho_{100} : N(S^{100}(0))$

Second

$$(\pi' \ S^{99}(0) \ \rho_{99} \ (\pi' \ S^{98}(0) \ \rho_{98} \ (... \ (\pi' \ 0 \ \rho_0 \ \pi))))$$

where $\rho_0 : N(0), \ \rho_1 : N(S(0)), \ \rho_2 : N(S^2(0))$, etc.
Parigot numbers

\( N(S^{100}(0)) \) is

\[
\forall c \ (0 \in c \Rightarrow \forall x \ (N(x) \Rightarrow x \in c \Rightarrow S(x) \in c) \Rightarrow S^{100}(0) \in c)
\]

Only one irreducible proof of this proposition

\[
\rho_{100} = \lambda c \lambda x \lambda f \ (f \ S^{99}(0) \ \rho_{99} \ (f \ S^{98}(0) \ \rho_{98} \ (\ldots (f \ 0 \ \rho_0 \ x))))
\]
\[
((\lambda y \ \lambda \alpha (\alpha \ c \ \pi \ \pi')) \ S^{100}(0) \ \rho_{100})
\]
reduces to
\[
(\rho_{100} \ c \ \pi \ \pi')
\]
and then to
\[
(\pi' \ S^{99}(0) \ \rho_{99} \ (\pi' \ S^{98}(0) \ \rho_{98} \ (\ldots \ (\pi' \ 0 \ \rho_{0} \ \pi))))
\]

Iterator: \(\rho_{100}, \text{ not } S^{100}(0)\)
VII. Proofs as programs
\( \pi \) proof of
\[
\forall x \ (N(x) \Rightarrow \exists y \ (N(y) \land (x = 0 \Rightarrow y = 0) \land (\neg x = 0 \Rightarrow y = S(0))))
\]

\((\pi \ S^n(0) \ \rho_n)\) proof of
\[
\exists y \ (N(y) \land (S^n(0) = 0 \Rightarrow y = 0) \land (\neg S^n(0) = 0 \Rightarrow y = S(0)))
\]
Irreducible form of this proof $\langle t, \langle \pi_1, \pi_2 \rangle \rangle$
where $t$ is a irreducible term expressing a natural number ($S^p(0)$)
$\pi_1$ proof of $N(t)$
$\pi_2$ proof of

$$(S^n(0) = 0 \Rightarrow t = 0) \land (\neg S^n(0) = 0 \Rightarrow t = S(0))$$

Thus if $n = 0$, then $p = 0$ and if $n \neq 0$, then $p = 1$
Computing the function $\chi$: proofs are programs and proof-reduction an interpreter
Provably total computable function

Specification of $\chi$:

$$(x = 0 \Rightarrow y = 0) \land (\neg x = 0 \Rightarrow y = S(0))$$

Any computable function $f$ can be specified by a proposition $A$, s.t. $(n/x, p/y)A$ provable if and only if $p = f(n)$

When

$$\forall x \ (N(x) \Rightarrow \exists y \ (N(y) \land A))$$

provable, $f$ provably total in arithmetic
Irreducible form of $(\pi S^n(0) \rho_n)$: $\langle t, \langle \pi_1, \pi_2 \rangle \rangle$

t = S^p(0) \text{ for } p = f(n)$

All functions that are provably total in arithmetic, can be expressed in this programming language

Much more expressive than Simply typed lambda-calculus

\[ N(y) \rightarrow \forall c \ (0 \in c \Rightarrow \forall x \ (N(x) \Rightarrow x \in c \Rightarrow S(x) \in c) \Rightarrow y \in c) \]

permits to type iterators
Next time

Dependent types