Chapter 8

Normalization

We discuss here an alternative proof method for proving normalization. We will focus here on a *semantic* proof method using *saturated sets*. This proof method goes back to Girard (1972) building on some previous ideas by Tait.

The key question is how to prove that give a lambda-term, its evaluation terminates, i.e. normalizes. Recall the lambda-calculus together with its reduction rules.

$$\text{Terms} \quad M, N \quad ::= \quad x \mid \lambda x.M \mid M\ N$$

We consider as the main rule for reduction (or evaluation) applying a term to an abstraction, called β-*reduction*.

$$(\lambda x.M)\ N \quad \longrightarrow \quad [N/x]M \qquad\qquad \beta\text{-reduction}$$

The β-reduction rule only applies once we have found a redex. However, we also need congruence rules to allow evaluation of arbitrary subterms.

$$\frac{M \longrightarrow M'}{M\,N \longrightarrow M'\,N} \qquad \frac{N \longrightarrow N'}{M\,N \longrightarrow M\,N'} \qquad \frac{M \longrightarrow M'}{\lambda x.M \longrightarrow \lambda x.M'}$$

The question then is, how do we know that reducing a well-typed lambda-term will halt? - This is equivalent to asking does a well-typed lambda-term normalize, i.e. after some reduction steps we will end up in a normal form where there are no further reductions possible. Since a normal lambda-term characterizes normal proofs, normalizing a lambda-term corresponds to normalizing proofs and demonstrates that every proof in the natural deduction system indeed has a normal proof.

Proving that reduction must terminate is not a simple syntactic argument based on terms, since the β-reduction rule may yield a term which is bigger than the term we started with. We hence need to find a different inductive argument. For the simply-typed lambda-calculus, we can prove that while the expression itself does not

get smaller, the type of an expression is. This is a syntactic argument; it however does not scale to polymorphic lambda-calculus. We will here instead discuss a *semantic* proof method where we define the meaning of well-typed terms using the abstract notion of *reducibility candidates*.

8.1 General idea

We can define the meaning of a well-typed term M in the context Γ of type A as follows: for all grounding instantiations σ providing values for the variables declared in Γ, $[\sigma]M$ is in the denotation of A. We write for the denotation of A as $[\![A]\!] = \mathcal{A}$. Similarly, the denotation of Γ is written as $[\![\Gamma]\!] = \mathcal{G}$.

$[\![A]\!]$ is interpreted as the sets of strongly normalizing terms of type A, i.e. $[\![A]\!] \in \mathsf{SN}$. We prove that if a term is well-typed, then it is strongly normalizing in two steps:

Step 1 If $M \in [\![A]\!]$ then $M \in \mathsf{SN}$.

Step 2 If $\Gamma \vdash M : A$ and $\sigma \in [\![\Gamma]\!]$ then $[\sigma]M \in [\![A]\!]$.

Therefore, we can conclude that if a term M has type A then $M \in \mathsf{SN}$, i.e. M is strongly normalizing and its reduction is finite, choosing σ to be the identity substitution.

We remark first, that all variables are in the denotations of a type A, i.e. $\mathsf{Var} \subseteq [\![A]\!]$, and variables are strongly normalizing, i.e. they are already in normal form.

Next, we define the denotations of the base type o and the function type $A \to B$.

- A term $M \in [\![o]\!]$ iff M is strongly normalizing, i.e. $M \in \mathsf{SN}$.
- A term $M \in [\![A \to B]\!]$ iff $M \in [\![A]\!] \Longrightarrow [\![B]\!]$, i.e. for all $N \in [\![A]\!].M\ N \in [\![B]\!]$.

We often write these definitions more compactly as follows

Semantic base type	$[\![o]\!]$	:=	SN
Semantic function type	$[\![A \to B]\!]$	:=	$\{M \mid \forall N \in [\![A]\!].M\ N \in [\![B]\!]\}$

8.2 Defining strongly normalizing terms

Intuitively, a term M is strongly normalizing, if there exists no infinite reduction sequence. Constructively, we can define strong normalization as follows:

Definition 8.2.1. *A term* M *is strongly normalizing, if all its reducts are strongly normalizing.*

$$\frac{\forall M'.\ M \longrightarrow M' \Longrightarrow \mathsf{sn}\ M'}{\mathsf{sn}\ M}$$

Moreover, we have that if a given term M is strongly normalizing, then any subterm must be strongly normalizing as well. We omit the proof here and leave it to an exercise.

Theorem 8.2.1 (Subterm property of strong normalization)**.** *Any subterm of a strongly normalizing term is strongly normalizing itself.*

Here, we define inductively the set of normal terms, SN, and the set of neutral terms, SNe, using the following judgements:

$$\begin{array}{ll} M \in \mathsf{SN} & M \text{ is in the set of normal terms} \\ M \in \mathsf{SNe} & M \text{ is in the set of neutral terms} \end{array}$$

The inductive definition given in Fig. 8.1 is often more amendable for proofs than its informal definition, since it allows us to prove properties by structural induction.

We will sketch here that these inductive definition is sound and complete with respect to our informal understanding of strongly normalizing reductions (Def. 8.2.1).

We will write $M \in \mathsf{sn}$ for M is strongly normalizing in our "informal definition", i.e. all reduction sequences starting in M are finite, to distinguish it from our inductive definition in Figure 8.1.

Lemma 8.2.2 (Properties of strongly normalizing terms)**.**

1. *If* $M \in \mathsf{sn}$ *and* $[N/x]M \in \mathsf{sn}$ *and* $N \in \mathsf{sn}$ *then* $(\lambda x.M)\ N \in \mathsf{sn}$.
2. *If* $M \in \mathsf{sn}$ *and* $N \in \mathsf{sn}$ *where* M *is not a* λ *then* $M\ N \in \mathsf{sn}$. *(we also have* $M\ N \longrightarrow M'\ N$ *and* $M'\ N \in \mathsf{sn}$ *as i.h.)*

Proof. By induction on $M \in \mathsf{sn}$ and $N \in \mathsf{sn}$. □

Lemma 8.2.3 (Closure properties of strongly normalizing terms)**.**

1. *If* $[N/x]M \in \mathsf{sn}$ *then* $M \in \mathsf{sn}$.
2. *For all variables* x*,* $x \in \mathsf{sn}$.

Neutral terms

$$\frac{}{x \in \mathsf{SNe}} \qquad \frac{R \in \mathsf{SNe} \qquad s \in \mathsf{SN}}{R\,M \in \mathsf{SNe}}$$

Normal terms

$$\frac{R \in \mathsf{SNe}}{R \in \mathsf{SN}} \qquad \frac{M \in \mathsf{SN}}{\lambda x.M \in \mathsf{SN}} \qquad \frac{M \longrightarrow_{\mathsf{SN}} M' \qquad M' \in \mathsf{SN}}{M \in \mathsf{SN}}$$

Strong head reduction

$$\frac{N \in \mathsf{SN}}{(\lambda x.M)\ N \longrightarrow_{\mathsf{SN}} [N/x]M} \qquad \frac{R \longrightarrow_{\mathsf{SN}} R' \qquad R \text{ is not a } \lambda}{R\,M \longrightarrow_{\mathsf{SN}} R'\,M}$$

Figure 8.1: Inductive definition of strongly normalizing terms

3. *If* $M \in \mathsf{sn}$ *and* $N \in \mathsf{sn}$ *where* $M = x\ \overrightarrow{N}$ *then* $M\,N \in \mathsf{sn}$.
4. *If* $M \in \mathsf{sn}$ *then* $\lambda x.M \in \mathsf{sn}$.
5. ***Expansion.*** *If* $M \longrightarrow_{\mathsf{sn}} M'$ *and* $M' \in \mathsf{sn}$ *then* $M \in \mathsf{sn}$ *where*

$$\frac{N \in \mathsf{sn}}{(\lambda x.M)\ N \longrightarrow_{\mathsf{sn}} [N/x]t} \qquad \frac{M \longrightarrow_{\mathsf{sn}} M' \quad M \textit{ is not a } \lambda}{M\ N \longrightarrow_{\mathsf{sn}} M'\ N}$$

Proof. By case analysis and induction. □

We can now prove our inductive definition to be sound and complete.

Theorem 8.2.4 (Soundness of SN)**.** 1. *If* $M \in \mathsf{SN}$ *then* $M \in \mathsf{sn}$.

2. *If* $M \in \mathsf{SNe}$ *then* $M \in \mathsf{sn}$ *and* $M = x\ \overrightarrow{N}$.
3. *If* $M \longrightarrow_{\mathsf{SN}} M'$ *then* $M \longrightarrow_{\mathsf{sn}} M'$.

Proof. By mutual structural induction on the given derivation using the closure properties. □

Theorem 8.2.5 (Completeness of SN)**.** 1. *If* $R = x\ \overrightarrow{N} \in \mathsf{sn}$ *then* $x\ \overrightarrow{N} \in \mathsf{SNe}$.

2. *If* $R = (\lambda x.M)\ N\ \overrightarrow{N} \in \mathsf{sn}$ *then* $R \longrightarrow_{\mathsf{SN}} [N/x]M\ \overrightarrow{N}$.

3. *If* $R \in \mathsf{sn}$ *then* $R \in \mathsf{SN}$.

Proof. By lexicographic induction on the height of the reduction tree of R and the height of R. □

8.3 Reducibility Candidates

One might ask, what is a good definition of a semantic type? - Rather than attempting the proof of the fundamental lemma directly and then trying to extract additional lemmas one might need about the semantic types, we follow Girard's technique and characterize some key properties our semantic types need to satisfy. If a semantic type satisfies these key properties, then our proof of the fundamental lemma will be straightforward. To put it differently, defining these key properties, will allow for a a modular proof of the fundamental lemma.

Definition 8.3.1 (Reducibility Candidate)**.** *A set* $[\![A]\!]$ *is a reducibility candidate,* $[\![A]\!] \in \mathsf{CR}$ *if the following conditions hold*

- CR1 : *If* $M \in [\![A]\!]$ *then* $M \in \mathsf{SN}$*, i.e.* $[\![A]\!] \subseteq \mathsf{SN}$.
- CR2 : *If* $M \in \mathsf{SNe}$ *then* $M \in [\![A]\!]$*, i.e.* $\mathsf{SNe} \subseteq [\![A]\!]$.
- CR3 : $\dfrac{M \longrightarrow_{\mathsf{SN}} M' \qquad M' \in [\![A]\!]}{M \in [\![A]\!]}$*, i.e.* $[\![A]\!]$ *is closed under reduction.*

The last property is often also referred to as *backward closed*. We show that that all semantic types $[\![A]\!]$ satisfy the conditions above.

Theorem 8.3.1. *For all types* C*,* $[\![C]\!] \in \mathsf{CR}$.

Proof. By induction on the structure of A. We highlight the cases below.

Case: $C = o$.

1. *Show* CR1: By definition, for all $M \in [\![o]\!]$, we have that $M \in \mathsf{SN}$.
2. *Show* CR2: By assumption $M \in \mathsf{SNe}$. By the definition of SN, we therefore know $M \in \mathsf{SN}$; by definition of $[\![o]\!]$, $M \in [\![o]\!]$.
3. *Show* CR3: Trivially true, since there is no step we can take with $\longrightarrow_{\mathsf{SN}}$.

Case: $C = A \to B$

1. *Show* CR1 : if $M \in [\![A \to B]\!]$, then $M \in \mathsf{SN}$, i.e. $[\![A \to B]\!] \subseteq \mathsf{SN}$.

   Assume that $M \in [\![A \to B]\!]$, i.e. for all $N \in [\![A]\!]$, $M\ N \in [\![B]\!]$
   $x \in [\![A]\!]$ by assumption $\mathsf{Var} \subseteq [\![A]\!]$
   $M\ x \in [\![B]\!]$ by previous lines
   $M\ x \in \mathsf{SN}$ by i.h. (CR1)
   $M \in \mathsf{SN}$ by subterm property

2. *Show* CR2 :if $M \in \mathsf{SNe}$, then $M \in [\![A \to B]\!]$, i.e. $\mathsf{SNe} \subseteq [\![A \to B]\!]$.

   $M \in \mathsf{SNe}$ by assumption
   Assume $N \in [\![A]\!]$.
   $N \in \mathsf{SN}$ by i.h. (CR1)
   $M\ N \in \mathsf{SNe}$ by def. of SNe
   $M\ N \in [\![B]\!]$ by i.h. (CR2)
   $M \in [\![A \to B]\!]$ by definition of $[\![A \to B]\!]$.

3. *Show* CR3 : if $M \longrightarrow_{\mathsf{SN}} M'$ and $M' \in [\![A \to B]\!]$, then $M \in [\![A \to B]\!]$.

   $M \longrightarrow_{\mathsf{SN}} M'$ by assumption
   $M' \in [\![A \to B]\!]$ by assumption
   for all $N' \in [\![A]\!]$, $M'\ N' \in [\![B]\!]$ by definition of $[\![A \to B]\!]$
   Assume $N \in [\![A]\!]$
   $M'\ N \in [\![B]\!]$ by previous lines
   $M\ N \longrightarrow_{\mathsf{SN}} M'\ N$ by $\longrightarrow_{\mathsf{SN}}$
   $M\ N \in [\![B]\!]$ by i.h. (CR3)
   $M \in [\![A \to B]\!]$ by definition of $[\![A \to B]\!]$

□

8.4 Proving strong normalization

As mentioned before, we prove that if a term is well-typed, then it is strongly normalizing in two steps:

Step 1 If $M \in [\![A]\!]$ then $M \in \mathsf{SN}$.

Step 2 If $\Gamma \vdash M : A$ and $\sigma \in [\![\Gamma]\!]$ then $[\sigma]M \in [\![A]\!]$.

The first part described in Step 1, is satisfied by the fact that $[\![A]\!]$ must be a reducibility candidate. Hence by CR1 all terms in $[\![A]\!]$ are strongly normalizing. We now prove the second step, which is often referred to as the *Fundamental Lemma*. It states that if M has type A and we can provide "good" instantiation σ, which provides terms which are themselves normalizing for all the free variables in M, then $[\sigma]M$ is in $[\![A]\!]$.

Lemma 8.4.1 (Fundamental lemma)**.** *If* $\Gamma \vdash M : A$ *and* $\sigma \in [\![\Gamma]\!]$ *then* $[\sigma]M \in [\![A]\!]$.

Proof. By induction on $\Gamma \vdash M : A$.

Case $\mathcal{D} = \dfrac{\Gamma(x) = A}{\Gamma \vdash x : A}$

$\sigma \in [\![\Gamma]\!]$	by assumption
$[\sigma]x \in [\![\Gamma(x)]\!] = [\![A]\!]$	by definition

Case $\mathcal{D} = \dfrac{\Gamma \vdash M : A \to B \qquad \Gamma \vdash N : A}{\Gamma \vdash M\ N : B}$

$\sigma \in [\![\Gamma]\!]$	by assumption
$[\sigma]M \in [\![A \to B]\!]$	by i.h.
for all $N' \in [\![A]\!]$. $([\sigma]M)\ N' \in [\![B]\!]$	by definition of $[\![A \to B]\!]$
$[\sigma]N \in [\![A]\!]$	by i.h.
$[\sigma]M\ [\sigma]N \in [\![B]\!]$	by previous lines
$[\sigma](M\ N) \in [\![B]\!]$	by subst. definition

Case $\mathcal{D} = \dfrac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x.M : A \to B}$

$\sigma \in [\![\Gamma]\!]$	by assumption
Assume $N \in [\![A]\!]$	
$(\sigma, N/x) \in [\![\Gamma, x : A]\!]$	by definition
$[\sigma, N/x]M \in [\![B]\!]$	by i.h.
$(\lambda x.[\sigma, x/x]M)\ N \longrightarrow_{SN} [\sigma, N/x]M$	by reduction $\longrightarrow_{SN}$
$(\lambda x.[\sigma, x/x]M) = [\sigma](\lambda x.M)$	by subst. def
$([\sigma]\lambda x.M)\ N \in [\![B]\!]$	by CR3
for all $N \in [\![A]\!]$. $([\sigma]\lambda x.M)\ N \in [\![B]\!]$	by previous lines
$[\sigma](\lambda x.M) \in [\![A \to B]\!]$	by definition of $[\![A \to B]\!]$

Neutral terms

$$\frac{M \in \mathsf{SNe} \quad N_1 \in \mathsf{SN} \quad N_2 \in \mathsf{SN}}{\mathsf{case}\, M\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow N_1 \mid \mathsf{inr}\, y \Rightarrow N_2 \in \mathsf{SNe}}$$

Normal terms

$$\frac{M \in \mathsf{SN}}{\mathsf{inl}\, M \in \mathsf{SN}} \qquad \frac{M \in \mathsf{SN}}{\mathsf{inr}\, M \in \mathsf{SN}}$$

Strong head reduction

$$\frac{M \in \mathsf{SN} \quad N_2 \in \mathsf{SN}}{\mathsf{case}\, (\mathsf{inl}\, M)\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow N_1 \mid \mathsf{inr}\, y \Rightarrow N_2 \longrightarrow_{\mathsf{SN}} [M/x]N_1}$$

$$\frac{M \in \mathsf{SN} \quad N_1 \in \mathsf{SN}}{\mathsf{case}\, (\mathsf{inr}\, M)\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow N_1 \mid \mathsf{inr}\, y \Rightarrow N_2 \longrightarrow_{\mathsf{SN}} [M/x]N_2}$$

$$\frac{M \longrightarrow_{\mathsf{SN}} M'}{\mathsf{case}\, M\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow N_1 \mid \mathsf{inr}\, y \Rightarrow N_2 \longrightarrow_{\mathsf{SN}} \mathsf{case}\, M'\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow N_1 \mid \mathsf{inr}\, y \Rightarrow N_2}$$

Figure 8.2: Inductive definition of strongly normalizing terms - extended for case-expressions and injections

□

Corollary 8.4.2. *If* $\Gamma \vdash M : A$ *then* $M \in \mathsf{SN}$.

Proof. Using the fundamental lemma with the identity substitution $\mathsf{id} \in [\![\Gamma]\!]$, we obtain $M \in [\![A]\!]$. By CR1, we know $M \in \mathsf{SN}$. □

8.5 Extension: Disjoint sums

We will now extend our simply-typed lambda-calculus to disjoint sums.

$$\begin{array}{llll} \text{Types} & A & ::= & \ldots \mid A + B \\ \text{Terms} & M & ::= & \ldots \mid \mathsf{inl}\, M \mid \mathsf{inr}\, M \mid \mathsf{case}\, M\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow N_1 \mid \mathsf{inr}\, y \Rightarrow N_2 \end{array}$$

Let us first extend our definition of SN and SNe (see Fig. 8.2).

Next, we extend our definition of semantic type to disjoint sums. A first attempt might be to define $[\![A + B]\!]$ as follows

Attempt 1

$$[\![A + B]\!] := \{\mathsf{inl}\ M \mid M \in [\![A]\!]\} \cup \{\mathsf{inr}\ M \mid M \in [\![B]\!]\}$$

However, this definition would not satisfy the key property CR3 and hence would fail to be a reducibility candidate. For example, while $\mathsf{inl}\ y$ is in $[\![A + B]\!]$, $(\lambda x.\mathsf{inl}\ x)\ y$ would not be in $[\![A + B]\!]$ despite the fact that $(\lambda x.\mathsf{inl}\ x)\ y \longrightarrow_{\mathsf{SN}} \mathsf{inl}\ y$.

Our definition of $[\![A + B]\!]$ is not closed under the reduction relation $\longrightarrow_{\mathsf{SN}}$. Let $\mathcal{A}$ denote the denotation of $[\![A]\!]$. We then define the closure of $[\![A]\!] = \mathcal{A}$, written as $\overline{\mathcal{A}}$, inductively as follows:

$$\frac{M \in \mathcal{A}}{M \in \overline{\mathcal{A}}} \qquad \frac{M \in \mathsf{SNe}}{M \in \overline{\mathcal{A}}} \qquad \frac{M \in \overline{\mathcal{A}} \qquad N \longrightarrow_{\mathsf{SN}} M}{N \in \overline{\mathcal{A}}}$$

and we define

$$[\![A + B]\!] \quad = \quad \overline{\{\mathsf{inl}\ M \mid M \in [\![A]\!]\} \cup \{\mathsf{inr}\ M \mid M \in [\![B]\!]\}}$$

8.5.1 Semantic type $[\![A + B]\!]$ is a reducibility candidate

We first extend our previous theorem which states that all denotations of types must be in CR.

Theorem 8.5.1. *For all types* C, $[\![C]\!] \in \mathsf{CR}$.

Proof. By induction on the structure of A. We highlight the case for disjoint sums.

Case $C = A + B$**.**

1. *Show* CR1. Assume that $M \in [\![A+B]\!]$. We consider different subcases and prove by an induction on the closure defining $[\![A + B]\!]$ that $M \in \mathsf{SN}$.

   Subcase: $M \in \{\mathsf{inl}\ N \mid N \in [\![A]\!]\}$. Therefore $M = \mathsf{inl}\ N$. Since $N \in [\![A]\!]$ and by i.h. (CR1), $N \in \mathsf{SN}$. By definition of SN, we have that $\mathsf{inl}\ N \in \mathsf{SN}$.

   Subcase: $M \in \{\mathsf{inr}\ N \mid N \in [\![B]\!]\}$. Therefore $M = \mathsf{inr}\ N$. Since $N \in [\![B]\!]$ and by i.h. (CR1), $N \in \mathsf{SN}$. By definition of SN, we have that $\mathsf{inr}\ N \in \mathsf{SN}$.

   Subcase: $M \in \mathsf{SNe}$. By definition of SN, we conclude that $M \in \mathsf{SN}$.

Subcase: $M \in [\![A + B]\!]$**, if** $M \longrightarrow_{SN} M'$ **and** $M' \in [\![A + B]\!]$.

$M \longrightarrow_{SN} M'$ and $M' \in [\![A + B]\!]$	by assumption
$M' \in SN$	by inner i.h.
$M \in SN$	by reduction $\longrightarrow_{SN}$

2. *Show* CR2.if $M \in SNe$, then $M \in [\![A + B]\!]$
   By definition of the closure, if $M \in SNe$, we have $M \in [\![A + B]\!]$.

3. *Show* CR3. if $M \longrightarrow_{SN} M'$ and $M' \in [\![A + B]\!]$ then $M \in [\![A + B]\!]$.
   By definition of the closure, if $M \longrightarrow_{SN} M'$ and $M' \in [\![A + B]\!]$, we have $M \in [\![A + B]\!]$.

□

8.5.2 Revisiting the fundamental lemma

We can now revisit the fundamental lemma.

Lemma 8.5.2 (Fundamental lemma)**.** *If* $\Gamma \vdash M : A$ *and* $\sigma \in [\![\Gamma]\!]$ *then* $[\sigma]M \in [\![A]\!]$.

Proof. By induction on $\Gamma \vdash M : A$.

Case $\mathcal{D} = \dfrac{\Gamma \vdash M : A + B \qquad \Gamma, x{:}A \vdash N_1 : C \qquad \Gamma, y{:}B \vdash N_2 : C}{\Gamma \vdash \mathsf{case}\, M\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow N_1 \mid \mathsf{inr}\, y \Rightarrow N_2 : C}$

$\sigma \in [\![\Gamma]\!]$	by assumption
$[\sigma]M \in [\![A + B]\!]$	by i.h.

We consider different subcases and prove by induction on the closure defining $[\![A + B]\!]$, that $[\sigma](\mathsf{case}\, M\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow M_1 \mid \mathsf{inr}\, y \Rightarrow M_2) \in [\![C]\!]$.

Subcase $[\sigma]M \in \{\mathsf{inl}\ N \mid N \in [\![A]\!]\}$

$[\sigma]M = \mathsf{inl}\ N$ for some $N \in [\![A]\!]$	by assumption
$N \in SN$	by CR1
$\sigma \in [\![\Gamma]\!]$	by assumption
$[\sigma, N/x] \in [\![\Gamma, x : A]\!]$	by definition
$[\sigma, N/x]M_1 \in [\![C]\!]$	by outer i.h.
$y \in [\![B]\!]$	by definition
$[\sigma, y/y] \in [\![\Gamma, y : B]\!]$	by definition

$[\sigma, y/y]M_2 \in [\![C]\!]$ by outer i.h.
$[\sigma, y/y]M_2 \in \mathsf{SN}$ by CR1
$\mathsf{case}\,(\mathsf{inl}\,N)\,\mathsf{of}\,\mathsf{inl}\,x \Rightarrow [\sigma, x/x]M_1 \mid \mathsf{inr}\,y \Rightarrow [\sigma, y/y]M_2 \longrightarrow_{\mathsf{SN}} [\sigma, N/x]M_1$ by $\longrightarrow_{\mathsf{SN}}$
$\mathsf{case}\,(\mathsf{inl}\,N)\,\mathsf{of}\,\mathsf{inl}\,x \Rightarrow [\sigma, x/x]M_1 \mid \mathsf{inr}\,y \Rightarrow [\sigma, y/y]M_2$
$\quad = [\sigma](\mathsf{case}\,M\,\mathsf{of}\,\mathsf{inl}\,x \Rightarrow M_1 \mid \mathsf{inr}\,y \Rightarrow M_2)$ by subst. definition and $[\sigma]M = \mathsf{inl}\,N$
$[\sigma](\mathsf{case}\,M\,\mathsf{of}\,\mathsf{inl}\,x \Rightarrow M_1 \mid \mathsf{inr}\,y \Rightarrow M_2) \in [\![C]\!]$ by CR3

Subcase $[\sigma]M \in \{\mathsf{inr}\,N \mid N \in [\![B]\!]\}$

similar to the case above.

Subcase: $[\sigma]M \in \mathsf{SNe}$.
$\sigma \in \Gamma$ by assumption
$x \in [\![A]\!]$, $y \in [\![B]\!]$ by definition
$[\sigma, y/y] \in [\![\Gamma, y : B]\!]$ by definition
$[\sigma, x/x] \in [\![\Gamma, x : A]\!]$ by definition
$[\sigma, x/x]M_1 \in [\![C]\!]$ by outer i.h.
$[\sigma, y/y]M_2 \in [\![C]\!]$ by outer i.h.
$[\sigma, y/y]M_2 \in \mathsf{SN}$ by CR1
$[\sigma, x/x]M_1 \in \mathsf{SN}$ by CR1
$\mathsf{case}\,[\sigma]M\,\mathsf{of}\,\mathsf{inl}\,x \Rightarrow [\sigma, x/x]M_1 \mid \mathsf{inr}\,y \Rightarrow [\sigma, y/y]M_2 \in \mathsf{SNe}$ by SNe
$[\sigma](\mathsf{case}\,M\,\mathsf{of}\,\mathsf{inl}\,x \Rightarrow M_1 \mid \mathsf{inr}\,y \Rightarrow M_2) \in \mathsf{SNe}$ by substitution def.
$[\sigma](\mathsf{case}\,M\,\mathsf{of}\,\mathsf{inl}\,x \Rightarrow M_1 \mid \mathsf{inr}\,y \Rightarrow M_2) \in [\![C]\!]$ by CR2

Subcase: $[\sigma]M \in [\![A + B]\!]$**, if** $[\sigma]M \longrightarrow_{\mathsf{SN}} M'$ **and** $M' \in [\![A + B]\!]$
$[\sigma]M \longrightarrow_{\mathsf{SN}} M'$ and $M' \in [\![A + B]\!]$ by assumption
$\mathsf{case}\,M'\,\mathsf{of}\,\mathsf{inl}\,x \Rightarrow [\sigma, x/x]M_1 \mid \mathsf{inr}\,y \Rightarrow [\sigma, y/y]M_2 \in [\![C]\!]$ by inner i.h.
$\mathsf{case}\,[\sigma]M\,\mathsf{of}\,\mathsf{inl}\,x \Rightarrow [\sigma, x/x]M_1 \mid \mathsf{inr}\,y \Rightarrow [\sigma, y/y]M_2$
$\quad \longrightarrow_{\mathsf{SN}} \mathsf{case}\,M'\,\mathsf{of}\,\mathsf{inl}\,x \Rightarrow [\sigma, x/x]M_1 \mid \mathsf{inr}\,y \Rightarrow [\sigma, y/y]M_2$ by $\longrightarrow_{\mathsf{SN}}$
$[\sigma](\mathsf{case}\,M\,\mathsf{of}\,\mathsf{inl}\,x \Rightarrow M_1 \mid \mathsf{inr}\,y \Rightarrow M_2) \in [\![C]\!]$ by CR3 □

8.6 Extension: Recursion

We now extend our simply-typed lambda-calculus to include natural numbers defined by z and $\mathsf{suc}\,t$ as well as a primitive recursion operator written as $\mathsf{rec}\ M\ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to M_z \mid \mathsf{f}\ (\mathsf{suc}\,n) \to M_s$ where M is the argument we recurse over, M_z describes the branch taken if $M = \mathsf{z}$ and M_s describes the branch taken when $M = \mathsf{suc}\,N$ where n will be instantiated with N and $\mathsf{f}\ n$ describes the recursive call.

$$\begin{array}{llll} \text{Types} & A & ::= & \ldots \mid \mathsf{nat} \\ \text{Terms} & t & ::= & \ldots \mid \mathsf{z} \mid \mathsf{suc}\, t \mid \mathsf{rec}\ t\ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to t_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to t_s \end{array}$$

To clarify, we give the typing rules for the additional constructs.

$$\frac{}{\Gamma \vdash \mathsf{z} : \mathsf{nat}} \qquad \frac{\Gamma \vdash M : \mathsf{nat}}{\Gamma \vdash \mathsf{suc}\, M : \mathsf{nat}}$$

$$\frac{\Gamma \vdash M : \mathsf{nat} \quad \Gamma \vdash M_z : C \quad \Gamma, n : \mathsf{nat},\ \mathsf{f}\, n : C \vdash M_s : C}{\Gamma \vdash \mathsf{rec}\ M\ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to M_s : C}$$

We again extend our definition of SN and SNe.

Neutral terms

$$\frac{M \in \mathsf{SNe} \quad M_z \in \mathsf{SN} \quad M_s \in \mathsf{SN}}{\mathsf{rec}\ M\ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to M_s \in \mathsf{SNe}}$$

Normal terms

$$\frac{}{\mathsf{z} \in \mathsf{SN}} \qquad \frac{M \in \mathsf{SN}}{\mathsf{suc}\, M \in \mathsf{SN}}$$

Strong head reduction

$$\frac{M_s \in \mathsf{SN}}{\mathsf{rec}\ \mathsf{z}\ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to M_s \longrightarrow_{\mathsf{SN}} M_z}$$

$$\frac{N \in \mathsf{SN} \quad M_z \in \mathsf{SN} \quad M_s \in \mathsf{SN} \quad f_r = \mathsf{rec}\ N\ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to M_s}{\mathsf{rec}\ (\mathsf{suc}\, N)\ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to M_s \longrightarrow_{\mathsf{SN}} [N/n,\ f_r/\mathsf{f}\, n]M_s}$$

$$\frac{M \longrightarrow_{\mathsf{SN}} M'}{\mathsf{rec}\ M\ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to M_s \longrightarrow_{\mathsf{SN}} \mathsf{rec}\ M'\ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to M_s}$$

8.7 Extension: Natural numbers

Here we add natural numbers to our language and show how the language remains normalizing.

8.7.1 Semantic type $[\![\mathsf{nat}]\!]$

We define the denotation of nat as follows:

$$[\![\mathsf{nat}]\!] := \overline{\{\mathsf{z}\} \cup \{\mathsf{suc}\, M \mid M \in [\![\mathsf{nat}]\!]\}}$$

8.7.2 Semantic type $[\![\mathsf{nat}]\!]$ is a reducibility candidate

We again extend our previous theorem which states that all denotations of types must be in CR.

Theorem 8.7.1. *For all types* C, $[\![C]\!] \in \mathsf{CR}$.

Proof. By induction on the structure of A. We highlight the case for nat.

Case $C = \mathsf{nat}$

1. *Show* CR1: Assume $M \in \mathsf{nat}$. we consider different subcases and prove by induction on the closure defining nat that $M \in \mathsf{SN}$.

   Subcase $M = \mathsf{z}$. By definition of SN, $\mathsf{z} \in \mathsf{SN}$.

   Subcase $M = \mathsf{suc}\, N$ where $N \in [\![\mathsf{nat}]\!]$. By i.h. (CR1), $N \in \mathsf{SN}$. By definition of SN, $\mathsf{suc}\, N \in \mathsf{SN}$.

   Subcase $M \in \mathsf{SNe}$. By definition of SN, $M \in \mathsf{SN}$.

   Subcase $M \in [\![\mathsf{nat}]\!]$, if $M \longrightarrow_{\mathsf{SN}} M'$ and $M' \in [\![\mathsf{nat}]\!]$.

$M \longrightarrow_{\mathsf{SN}} M'$ and $M' \in [\![\mathsf{nat}]\!]$	by assumption
$M' \in \mathsf{SN}$	by inner i.h.
$M \in \mathsf{SN}$	by reduction $\longrightarrow_{\mathsf{SN}}$

Show CR2: By definition of the closure, $M \in \mathsf{SNe}$, then $M \in [\![\mathsf{nat}]\!]$.

Show CR3: $M \in \mathsf{nat}$, if $M \longrightarrow_{\mathsf{SN}} M'$ and $M' \in \mathsf{nat}$. By definition of the closure, we have that $M \in \mathsf{nat}$. □

8.7.3 Revisiting the fundamental lemma

We can now revisit the fundamental lemma.

Lemma 8.7.2 (Fundamental lemma)**.** *If* $\Gamma \vdash M : A$ *and* $\sigma \in [\![\Gamma]\!]$ *then* $[\sigma]M \in [\![A]\!]$.

Proof. By induction on $\Gamma \vdash M : A$.

Case $\mathcal{D} = \dfrac{}{\Gamma \vdash z : \mathsf{nat}}$

$z \in [\![\mathsf{nat}]\!]$ by definition.

Case $\mathcal{D} = \dfrac{\Gamma \vdash M : \mathsf{nat}}{\Gamma \vdash \mathsf{suc}\, M : \mathsf{nat}}$

$\sigma \in [\![\Gamma]\!]$ by assumption
$M \in [\![\mathsf{nat}]\!]$ by i.h.
$\mathsf{suc}\, M \in [\![\mathsf{nat}]\!]$ by definition

Case $\mathcal{D} = \dfrac{\Gamma \vdash M : \mathsf{nat} \qquad \Gamma \vdash M_z : C \qquad \Gamma, n : \mathsf{nat},\ f\ n : C \vdash M_s : C}{\Gamma \vdash \mathsf{rec}\ M\ \mathsf{with}\ f\ z \to M_z \mid f\ (\mathsf{suc}\, n) \to M_s : C}$

$\sigma \in [\![\Gamma]\!]$ by assumption
$[\sigma]M \in [\![\mathsf{nat}]\!]$ by i.h.

We distinguish cases based on $M \in [\![\mathsf{nat}]\!]$ and prove by induction on $M \in [\![\mathsf{nat}]\!]$ that $[\sigma](\mathsf{rec}\ M\ \mathsf{with}\ f\ z \to M_z \mid f\ (\mathsf{suc}\, n) \to M_s) \in [\![C]\!]$.

Subcase $[\sigma]M = z$.

$n \in [\![\mathsf{nat}]\!]$, $f\ n \in [\![C]\!]$ by definition
$[\sigma, n/n, f\ n/f\ n] \in [\![\Gamma, n : \mathsf{nat}, f\ n : C]\!]$ by definition
$[\sigma, n/n, f\ n/f\ n]M_s \in [\![C]\!]$ by outer i.h.
$[\sigma, n/n, f\ n/f\ n]M_s \in \mathsf{SN}$ by CR1
$[\sigma]M_z \in [\![C]\!]$ by outer i.h.
$\mathsf{rec}\ z\ \mathsf{with}\ f\ z \to [\sigma]M_z \mid f\ (\mathsf{suc}\, n) \to [\sigma, n/n, f\ n/f\ n]M_s \longrightarrow_{\mathsf{SN}} [\sigma]M_z$ by $\longrightarrow_{\mathsf{SN}}$
$\mathsf{rec}\ z\ \mathsf{with}\ f\ z \to [\sigma]M_z \mid f\ (\mathsf{suc}\, n) \to [\sigma, n/n, f\ n/f\ n]M_s = [\sigma](\mathsf{rec}\ M\ \mathsf{with}\ f\ z \to M_z \mid f\ (\mathsf{suc}\, n) \to M_s)$ by subst. def. and $M = z$
$[\sigma](\mathsf{rec}\ M\ \mathsf{with}\ f\ z \to M_z \mid f\ (\mathsf{suc}\, n) \to M_s \in [\![C]\!]$ by CR3.

Subcase $[\sigma]M = \mathsf{suc}\, M'$ where $M' \in [\![\mathsf{nat}]\!]$.

$M' \in [\![\mathsf{nat}]\!]$ by assumption
$M' \in \mathsf{SN}$ by CR1
$[\sigma]M_z \in [\![C]\!]$ by outer i.h.
$[\sigma]M_z \in \mathsf{SN}$ by CR1
$[\sigma, n/n, \mathsf{f}\, n/\mathsf{f}\, n]M_s \in [\![C]\!]$ by outer i.h.
$[\sigma, n/n, \mathsf{f}\, n/\mathsf{f}\, n]M_s \in \mathsf{SN}$ by CR1
$\mathsf{rec}\ M' \ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to [\sigma]M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to [\sigma, n/n, \mathsf{f}\, n/\mathsf{f}\, n]M_s \in [\![C]\!]$ by inner i.h.
$[\sigma, M'/x,\ \mathsf{rec}\ M' \ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to [\sigma]M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to [\sigma, n/n, \mathsf{f}\, n/\mathsf{f}\, n]M_s/\mathsf{f}\, n] \in [\![\Gamma, n : \mathsf{nat}, \mathsf{f}\, n : C]\!]$ by definition
$[\sigma, M'/x,\ \mathsf{rec}\ M' \ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to [\sigma]M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to [\sigma, n/n, \mathsf{f}\, n/\mathsf{f}\, n]M_s/\mathsf{f}\, n]M_s \in [\![C]\!]$ by outer i.h.
$\mathsf{rec}\ (\mathsf{suc}\, M') \ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to [\sigma]M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to [\sigma, n/n, \mathsf{f}\, n/\mathsf{f}\, n]M_s$
$\quad \longrightarrow_{\mathsf{SN}} [\sigma, M'/x,\ \mathsf{rec}\ M' \ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to [\sigma]M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to [\sigma, n/n, \mathsf{f}\, n/\mathsf{f}\, n]M_s/\mathsf{f}\, n]M_s$
by $\longrightarrow_{\mathsf{SN}}$
$[\sigma](\mathsf{rec}\ M \ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to M_s) \in [\![C]\!]$ by CR3.

Subcase $[\sigma]M \in \mathsf{SNe}$.

$[\sigma]M_z \in [\![C]\!]$ by outer i.h.
$[\sigma]M_z \in \mathsf{SN}$ by CR1
$[\sigma, n/n, \mathsf{f}\, n/\mathsf{f}\, n]M_s \in [\![C]\!]$ by outer i.h.
$[\sigma, n/n, \mathsf{f}\, n/\mathsf{f}\, n]M_s \in \mathsf{SN}$ by CR1
$\mathsf{rec}\ [\sigma]M \ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to [\sigma]M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to [\sigma, n/n, \mathsf{f}\, n/\mathsf{f}\, n]M_s \in \mathsf{SNe}$ by SNe
$[\sigma](\mathsf{rec}\ M \ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to M_s) \in \mathsf{SNe}$ by subst. def.
$[\sigma](\mathsf{rec}\ M \ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to M_s) \in [\![C]\!]$ by CR2.

Subcase $[\sigma]M \in [\![\mathsf{nat}]\!]$, if $[\sigma]M \longrightarrow_{\mathsf{SN}} M'$ and $M' \in [\![\mathsf{nat}]\!]$.

$[\sigma]M \longrightarrow_{\mathsf{SN}} M'$ and $M' \in [\![\mathsf{nat}]\!]$ by assumption.
$\mathsf{rec}\ M' \ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to [\sigma]M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to [\sigma, n/n, \mathsf{f}\, n/\mathsf{f}\, n]M_s \in [\![C]\!]$ by inner i.h.
$\mathsf{rec}\ [\sigma]M \ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to [\sigma]M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to [\sigma, n/n, \mathsf{f}\, n/\mathsf{f}\, n]M_s$
$\quad \longrightarrow_{\mathsf{SN}} \mathsf{rec}\ M' \ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to [\sigma]M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to [\sigma, n/n, \mathsf{f}\, n/\mathsf{f}\, n]M_s$ by $\longrightarrow_{\mathsf{SN}}$
$[\sigma](\mathsf{rec}\ M \ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to M_s) \in [\![C]\!]$ by CR3.

□