POPLMark Reloaded Benchmark: An Introduction – Work in Progress –

Brigitte Pientka, McGill University
Aliya Hameer, McGill University
Alberto Momigliano, University of Milan
Andreas Abel, Chalmers

We discuss here an alternative proof method for proving normalization. We will focus here on a *semantic* proof method using *saturated sets* (see Luo [1990]). This proof method goes back to Girard [1972] building on some previous ideas by Tait [1967].

The key question is how to prove that given a lambda-term, its evaluation terminates, i.e. normalizes. We concentrate here on a typed operational semantics following Goguen [1995] and define a reduction strategy that transforms λ-terms into β normal form. This allows us to give a concise presentation of the important issues that arise.

We see this benchmark as a good jumping point to investigate and mechanize the meta-theory of dependently typed systems where a typed operational semantics simplifies the study of its meta-theory. The approach of typed operational semantics is however not limited to dependently typed systems, but it has been used extensively in studying subtyping, type-preserving compilation, and shape analysis. Hence, we believe it does describe an important approach to describing reductions.

Simply Typed Lambda Calculus with Type-directed Reduction

Recall the lambda-calculus together with its reduction rules.

$$\begin{array}{lrcl} \text{Terms} & M, N & ::= & x \mid \lambda x{:}A.M \mid M\ N \\ \text{Types} & A, B & ::= & i \mid A \Rightarrow B \end{array}$$

We consider as the main rule for reduction (or evaluation) applying a term to an abstraction, called β-*reduction*. We use the judgment $\Gamma \vdash M \longrightarrow N : A$ to mean that both M and N have type A in the context Γ and the term M reduces to the term N.

$$\frac{\Gamma \vdash \lambda x{:}A.M : A \Rightarrow B \quad \Gamma \vdash N : A}{\Gamma \vdash (\lambda x{:}A.M)\ N \longrightarrow [N/x]M : B}\ \beta$$

$$\frac{\Gamma \vdash M \longrightarrow M' : A \Rightarrow B \quad \Gamma \vdash N : A}{\Gamma \vdash M\,N \longrightarrow M'\,N : B} \qquad \frac{\Gamma \vdash M : A \Rightarrow B \quad \Gamma \vdash N \longrightarrow N' : A}{\Gamma \vdash M\,N \longrightarrow M\,N' : B}$$

$$\frac{\Gamma, x{:}A \vdash M \longrightarrow M' : B}{\Gamma \vdash \lambda x{:}A.M \longrightarrow \lambda x{:}A.M' : A \Rightarrow B}$$

Our typed reduction relation is inspired by the type-directed definition of algorithmic equality for λ-terms (see for example Crary [2005] or Harper and Pfenning [2005]). Keeping track of types in the definition of equality or reduction becomes quickly necessary as soon as want to add η-expansion or

add a unit type where every term of type unit reduces to the unit element. We do not add these rules at this point.

In addition, we have that typed reductions are only defined on well-typed terms, i.e. if M steps then M is well-typed.

Lemma. [Properties about Typed Reductions and Typing]

- If $\Gamma \vdash M \longrightarrow N : A$ then $\Gamma \vdash M : A$ and $\Gamma \vdash N : A$.
- If $\Gamma \vdash M : A$ then A is unique.

The typing and typed reduction strategy satisfies weakening and strengthening.

Lemma. [Weakening and Strengthening of Typing and Typed Reductions]

- If $\Gamma, \Gamma' \vdash M : B$ Then $\Gamma, x{:}A, \Gamma' \vdash M : B$.
- If $\Gamma, x{:}A, \Gamma' \vdash M : B$ and $x \notin \mathsf{FV}(M)$ then $\Gamma, \Gamma' \vdash M : B$.
- If $\Gamma, \Gamma' \vdash M \longrightarrow N : B$ then $\Gamma, x{:}A, \Gamma' \vdash M \longrightarrow N : B$.
- If $\Gamma, x{:}A, \Gamma' \vdash M \longrightarrow N : B$ and $x \notin \mathsf{FV}(M)$ then $x \notin \mathsf{FV}N$ and $\Gamma, \Gamma' \vdash M \longrightarrow N : B$.

Proof. By induction on the first derivation. □

When is a term in normal form?

We define here briefly when a term is in β-normal form. We define the grammar of normal terms as given below

$$\begin{array}{lllll} \text{Normal Terms} & M, N & ::= & \lambda x{:}\, A.M \mid R \\ \text{Neutral Terms} & R, P & ::= & x \mid R\ M \end{array}$$

This grammar does not enforce η-long.

Proving normalization

The question then is, how do we know that we can normalizing a well-typed lambda-term into its β normal form? - This is equivalent to asking whether 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.

As syntactic arguments are not sufficient to argue that we can always compute a β normal form, we hence need to find a different inductive argument. For the simply-typed lambda-calculus, we could prove that while the expression itself does not get smaller, the type of an expression does[1]. This is a syntactic argument; it however does not scale to polymorphic lambda-calculus or full dependent type theories. 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*.

[1] This is the essential idea of hereditary substitutions Watkins et al. [2002]

Throughout this tutorial, we stick to the simply typed lambda-calculus and its extension. This allows us to give a concise presentation of the important issues that arise. However the most important benefits of typed operational semantics and our approach are demonstrated in systems with dependent types where our development of the metatheoretic simpler than the existing techniques. We see this benchmark hence as a good jumping point to investigate and mechanize the meta-theory of dependently typed systems.

1 Semantic Interpretation

Working with well-typed terms means we need to be more careful to consider a term within its typing context. In particular, when we define the semantic interpretation of $\Gamma \vdash M \in \mathcal{R}_{A \Rightarrow B}$ we must consider all extensions of Γ (described by $\Gamma' \geq_\rho \Gamma$) in which we may use M.

- $\Gamma \vdash M \in \mathcal{R}_i$ iff $\Gamma \vdash M : i$ and M is strongly normalizing
- $\Gamma \vdash M \in \mathcal{R}_{A \Rightarrow B}$ iff for all $\Gamma' \geq_\rho \Gamma$ and $\Gamma' \vdash N : A$, if $\Gamma' \vdash N \in \mathcal{R}_A$ then $\Gamma' \vdash [\rho]M\ N \in \mathcal{R}_B$.

2 General idea

We prove that if a term is well-typed, then it is strongly normalizing in two steps:

Step 1 If $\Gamma \vdash M \in \mathcal{R}_A$ then $\Gamma \vdash M : A$ and M is strongly normalizing.

Step 2 If $\Gamma \vdash M : A$ and $\Gamma' \vdash \sigma \in \mathcal{R}_\Gamma$ then $\Gamma' \vdash [\sigma]M \in \mathcal{R}_A$.

Therefore, we can conclude that if a term M has type A then M is strongly normalizing and its reduction is finite, choosing σ to be the identity substitution.

3 Defining strongly normalizing terms

3.1 Definition of strong normalization via accessibility relation

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

Definition 3.1. *A term M of type A is strongly normalizing, if all its reducts are strongly normalizing.*

$$\frac{\Gamma \vdash M : A \quad \forall M'.\ \Gamma \vdash M \longrightarrow M' : A \Longrightarrow \Gamma \vdash M' : A \in \mathsf{sn}}{\Gamma \vdash M : A \in \mathsf{sn}}$$

The usual definition of strong normalization via accessibility does not only consider well-typed terms. However, as we follow a type-directed reduction strategy, it is natural to define strong normalization on well-typed terms.

To check strong normalizability of a term M it is sufficient to consider every one-step reduct of M instead of all possible (potentially infinite) reduction sequences. In particular, we can show that it enjoys the expected closure and substitution properties, namely:

- $\Gamma \vdash R : A \Rightarrow B \in \mathsf{sn}$ and $\Gamma \vdash N : A \in \mathsf{sn}$ iff $\Gamma \vdash R\ N : B \in \mathsf{sn}$;

- $\Gamma, x{:}A \vdash M : B \in \mathsf{sn}$ iff $\Gamma \vdash \lambda x{:}A.M : A \Rightarrow B \in \mathsf{sn}$;
- Let $\Gamma \vdash N : A \in \mathsf{sn}$. Then $\Gamma, x{:}A \vdash M : B \in \mathsf{sn}$ if $\Gamma \vdash [N/x]M : B \in \mathsf{sn}$.

We first show that our definition of sn satisfies weakening.

Lemma 3.1 (Weakening of strongly normalizing terms)**.** *If* $\Gamma \vdash M : B \in \mathsf{sn}$ *then* $\Gamma, x{:}A \vdash M : B \in \mathsf{sn}$.

Proof. By induction on $\Gamma \vdash M : B \in \mathsf{sn}$.

$\Gamma \vdash M : B$	by assumption $\Gamma \vdash M : B \in \mathsf{sn}$
$\Gamma, x{:}A \vdash M : B$	by weakening of typing
Assume $\Gamma, x{:}A \vdash M \longrightarrow M' : B$	
$\Gamma \vdash M \longrightarrow M' : B$	by strengthening (Lemma)
$\Gamma \vdash M' : B \in \mathsf{sn}$	by assumption $\Gamma \vdash M : B \in \mathsf{sn}$
$\Gamma, x{:}A \vdash M' : B \in \mathsf{sn}$	by IH
$\Gamma, x{:}A \vdash M : B \in \mathsf{sn}$	since M' was arbitrary

□

Lemma 3.2 (Properties of strongly normalizing terms)**.**

1. *If* $\Gamma \vdash R : A \Rightarrow B \in \mathsf{sn}$ *where* R *is not a lambda-abstraction and* $\Gamma \vdash N : A \in \mathsf{sn}$ *then* $\Gamma \vdash R\ N : B \in \mathsf{sn}$.
2. *If* $\Gamma, x{:}A \vdash M : B \in \mathsf{sn}$ *then* $\Gamma \vdash \lambda x{:}A.M : A \Rightarrow B \in \mathsf{sn}$
3. *If* $\Gamma \vdash M\ N : B \in \mathsf{sn}$ *then* $\Gamma \vdash M : A \Rightarrow B \in \mathsf{sn}$ *and* $\Gamma \vdash N : A \in \mathsf{sn}$.
4. *If* $\Gamma \vdash \lambda x{:}A.M : A \Rightarrow B \in \mathsf{sn}$ *then* $\Gamma, x{:}A \vdash M : B \in \mathsf{sn}$.

Proof. Property 1 is proven by mutual induction on the derivations; properties 3, 4, and 2 are proven by induction on the first derivation.

In all the proofs below we silently exploit type uniqueness and do not track explicitly the reasoning about well-typed terms below.

1. If $\Gamma \vdash R : A \Rightarrow B \in \mathsf{sn}$ and $\Gamma \vdash N : A \in \mathsf{sn}$ then $\Gamma \vdash R\ N : B \in \mathsf{sn}$. where R is not a lambda-abstraction.

By simultaneous induction on $\Gamma \vdash R : A \Rightarrow B \in \mathsf{sn}$, $\Gamma \vdash N : A \in \mathsf{sn}$.

Assume $\Gamma \vdash R\ N \longrightarrow Q : B$

Sub-case: $\mathcal{D} = \dfrac{\Gamma \vdash R \longrightarrow R' : A \Rightarrow B \qquad \Gamma \vdash N : A}{\Gamma \vdash R\,N \longrightarrow R'\,N : B}$ and $Q = R'\ N$

$\Gamma \vdash R' : A \Rightarrow B \in \mathsf{sn}$	by using assumption $\Gamma \vdash R : A \Rightarrow B \in \mathsf{sn}$
$\Gamma \vdash R'\ N : B \in \mathsf{sn}$	by IH
$\Gamma \vdash Q : B \in \mathsf{sn}$	since $Q = R'\ N$

Sub-case: $\mathcal{D} = \dfrac{\Gamma \vdash N \longrightarrow N' : A \qquad \Gamma \vdash R : A \Rightarrow B}{\Gamma \vdash R\,N \longrightarrow R\,N' : B}$ and $Q = R\,N'$

$\Gamma \vdash N' : A \in \mathsf{sn}$ by using assumption $\Gamma \vdash N : A \in \mathsf{sn}$
$\Gamma \vdash R\,N' : B \in \mathsf{sn}$ by IH
$\Gamma \vdash Q : B \in \mathsf{sn}$ since $Q = R\,N'$

2. If $\Gamma, x{:}A \vdash M : B \in \mathsf{sn}$ then $\Gamma \vdash \lambda x{:}A.M : A \Rightarrow B \in \mathsf{sn}$

Induction on $\Gamma, x{:}A \vdash M : B \in \mathsf{sn}$

Assume $\Gamma \vdash \lambda x{:}A.M \longrightarrow Q : A \Rightarrow B$ $\Gamma, x{:}A \vdash M \longrightarrow M' : B$ and $Q = \lambda x{:}A.M'$ by reduction rule for λ.
$\Gamma, x{:}A \vdash M' : B \in \mathsf{sn}$ by assumption $\Gamma, x{:}A \vdash M : B \in \mathsf{sn}$
$\Gamma \vdash \lambda x{:}A.M' : A \Rightarrow B \in \mathsf{sn}$ by IH
$\Gamma \vdash Q : A \Rightarrow B \in \mathsf{sn}$ since $Q = \lambda x{:}A.M'$
$\Gamma \vdash \lambda x.M : A \Rightarrow B \in \mathsf{sn}$ since $\Gamma \vdash \lambda x.M \longrightarrow Q : A \Rightarrow B$ was arbitrary

3. If $\Gamma \vdash M\,N : B \in \mathsf{sn}$ then $\Gamma \vdash M : A \Rightarrow B \in \mathsf{sn}$ and $\Gamma \vdash N : A \in \mathsf{sn}$.

We prove first: If $\Gamma \vdash M\,N : B \in \mathsf{sn}$ then $\Gamma \vdash M : A \Rightarrow B \in \mathsf{sn}$. Proving $\Gamma \vdash M\,N : B \in \mathsf{sn}$ implies also $\Gamma \vdash N : A \in \mathsf{sn}$ is similar.
By induction on $\Gamma \vdash M\,N : B \in \mathsf{sn}$.

Assume $\Gamma \vdash M \longrightarrow M' : A \Rightarrow B$
$\Gamma \vdash M\,N \longrightarrow M'\,N : B$ by reduction rule for application
$\Gamma \vdash M'\,N : B \in \mathsf{sn}$ by assumption $\Gamma \vdash M\,N \in \mathsf{sn}$
$\Gamma \vdash M' : A \Rightarrow B \in \mathsf{sn}$ by IH
$\Gamma \vdash M : A \Rightarrow B \in \mathsf{sn}$ since $\Gamma \vdash M \longrightarrow M' : A \Rightarrow B$ was arbitrary

4. If $\Gamma \vdash \lambda x{:}A.M : A \Rightarrow B \in \mathsf{sn}$ then $\Gamma, x{:}A \vdash M : B \in \mathsf{sn}$.

By induction on $\Gamma \vdash \lambda x{:}A.M : A \Rightarrow B \in \mathsf{sn}$.

Assume $\Gamma, x{:}A \vdash M \longrightarrow M' : B$
$\Gamma \vdash \lambda x{:}A.M \longrightarrow \lambda x{:}A.M' : A \Rightarrow B$ by reduction rules for λ
$\Gamma \vdash \lambda x{:}A.M' : A \Rightarrow B \in \mathsf{sn}$ by assumption $\Gamma \vdash \lambda x{:}A.M \in \mathsf{sn}$
$\Gamma, x{:}A \vdash M' : B \in \mathsf{sn}$ by IH
$\Gamma, x{:}A \vdash M : B \in \mathsf{sn}$ since $\Gamma, x{:}A \vdash M \longrightarrow M'$ was arbitrary

□

Closure properties of strongly normalizating terms

Let us begin by contrasting weak and strong normalization. A term M is said to be *weakly* normalising if there is a rewrite sequence starting in M that eventually ends in a normal form. A term M is said to be *strongly* normalising if all rewrite sequences starting in M end eventually in a normal form.

As pointed out by van Raamsdonk and Severi [1995], we can easily characterize all weakly normalising terms as follows: a weakly normalising term is a normal form or can be obtained as the

result of some expansion starting in a normal form. Following this idea, we can then characterize elegantly strongly normalizing terms also as the closure under expansion where expansion is subject to two restrictions: first, the argument of the redex introduced by the expansion step should be in the set of strongly normalising terms, and second, the expansion step should yield a new head redex (backwards closure) or a new outermost redex in a term without a head redex. This idea will form the essence of the closure properties we state next and also gives rise to an inductive definition of strongly normalizing terms which we give in the next section.

To compactly state closure properties, we rely on evaluation contexts which we define below:

$$\text{Evaluation Context } C \quad ::= \quad \_ \mid C\ M$$

An evaluation context is a term with a hole, written as an underscore.

Using evaluation contexts, we can describe the term $x\ M_1 \dots M_n$ using the evaluation context $C = \_\ M_1 \dots M_n$ and simply instantiate the hole with x writing $C[x]$ for $x\ M_1 \dots M_n$. We can also represent the term $x\ M_1 \dots M_n$ choosing the evaluation context $C' = \_\ M_1 \dots M_{n-1}$ writing $C'[x]\ M_n = C[x]$.

Similarly, choosing $C = \_\ N_1 \dots N_k$ and instantiating the hole with $\lambda x{:}A.M$ we describe a term $C[\lambda x{:}A.M] = (\lambda x{:}A.M)\ N_1 \dots N_k$ which has a redex. Moreover, when choosing the evaluation context $C' = \_\ N_2 \dots N_k$ we have $C'[(\lambda x{:}A.M)\ N_1] = C[\lambda x{:}A.M]$.

Evaluation contexts are inductively defined – they are either a hole or built by $C\ M$ where C is a smaller evaluation context containing a hole.

> [*We may want to explain the notation* $C[x]$*, as the induction structure is not crystal clear to me. Also confused why weak head reduction suffices -am*]

Lemma 3.3 (Evaluation Contexts)**.** *If* $\Gamma \vdash C[x]\ N \longrightarrow R : B$ *then there exists an evaluation context* C' *s.t.* $R = C'[x]$.

Proof. By induction on the structure of evaluation contexts C.

Case $C = \_$

$\Gamma \vdash x\ N \longrightarrow R : B$ by assumption since $C[x] = x$
Impossible since $x\ N$ does not step.

Case $C = C_0\ M$

$\Gamma \vdash (C_0[x]\ M)\ N \longrightarrow R : B$ by assumption since $C[x] = C_0[x]\ M$

$$\textbf{Sub-case}\ \frac{\Gamma \vdash (C_0[x]\ M) \longrightarrow R : A \Rightarrow B \qquad \Gamma \vdash N : A}{\Gamma \vdash (C_0[x]\ M)\ N \longrightarrow R\ N : B}$$

There exists an evaluation context $C_1[x] = R$ by IH
Therefore there exists an evaluation context $C'[x] = C_1[x]\ N$

$$\textbf{Sub-case}\ \frac{\Gamma \vdash (C_0[x]\ M) : A \Rightarrow B \qquad \Gamma \vdash N \longrightarrow N' : A}{\Gamma \vdash (C_0[x]\ M)\ N \longrightarrow (C_0[x]\ M)\ N' : B}$$

Hence there exists an evaluation context C' s.t. $C'[x] = (C_0[x]\ M)\ N'$.

□

Using evaluation contexts we can now state elegantly that strongly normalizing terms are closed under expansion.

Lemma 3.4 (Closure properties of strongly normalizing terms)**.**

1. *For all variables* $x : A \in \Gamma$, $\Gamma \vdash x : A \in \mathsf{sn}$.
2. *If* $\Gamma \vdash C[x] : A \Rightarrow B \in \mathsf{sn}$ *and* $\Gamma \vdash N : A \in \mathsf{sn}$ *then* $\Gamma \vdash C[x]\,N : B \in \mathsf{sn}$.
3. *If* $\Gamma \vdash C[x]\,M \longrightarrow R : B$ *and* $\Gamma \vdash C[x] : A \Rightarrow B \in \mathsf{sn}$ *and* $\Gamma \vdash M : A \in \mathsf{sn}$ *then* $\Gamma \vdash R : B \in \mathsf{sn}$.

Proof.

1. For all variables $x : A \in \Gamma$, $\Gamma \vdash x : A \in \mathsf{sn}$.

$\forall M'.\ \Gamma \vdash x \longrightarrow M' : A \Longrightarrow \Gamma \vdash M' : A \in \mathsf{sn}$ since $\Gamma \vdash x \longrightarrow M'$ is impossible
$\Gamma \vdash x : A$ since $x : A \in \Gamma$
$\Gamma \vdash x : A \in \mathsf{sn}$

2. If $\Gamma \vdash C[x] : A \Rightarrow B \in \mathsf{sn}$ and $\Gamma \vdash N : A \in \mathsf{sn}$ then $\Gamma \vdash C[x]\,N : B \in \mathsf{sn}$.

Assume $\Gamma \vdash C[x]\,N \longrightarrow R : B$
$\Gamma \vdash C[x] : A \Rightarrow B \in \mathsf{sn}$ and $\Gamma \vdash N : A \in \mathsf{sn}$ by assumption
$\Gamma \vdash R : B \in \mathsf{sn}$ by Lemma 3.2(1) since $C[x]$ is not a lambda-abstraction
$\Gamma \vdash C[x]\,N : B \in \mathsf{sn}$ since $\Gamma \vdash C[x]\,N \longrightarrow R : B$ was arbitrary

3. If $\Gamma \vdash C[x]\,M \longrightarrow R : B$ and $\Gamma \vdash C[x] : A \Rightarrow B \in \mathsf{sn}$ and $\Gamma \vdash M : A \in \mathsf{sn}$ then $\Gamma \vdash R : B \in \mathsf{sn}$.

Proof by simultaneous induction on $\Gamma \vdash C[x] : A \Rightarrow B \in \mathsf{sn}$ and $\Gamma \vdash M : A \in \mathsf{sn}$.

Sub-case $\dfrac{\Gamma \vdash C[x] \longrightarrow M' : A \Rightarrow B \quad \Gamma \vdash N : A}{\Gamma \vdash C[x]\,N \longrightarrow M'\,N : B}$

$\Gamma \vdash M' : A \Rightarrow B \in \mathsf{sn}$ by assumption $\Gamma \vdash C[x] : A \Rightarrow B \in \mathsf{sn}$
$M'\,N = C_0[x]$ by lemma 3.3
$M' = C_1[x]$ and hence $\Gamma \vdash C_1[x] : A \Rightarrow B \in \mathsf{sn}$ by def. evaluation contexts
$\Gamma \vdash N : A \in \mathsf{sn}$ by assumption
$\Gamma \vdash C_1[x]\,N : B \in \mathsf{sn}$ by IH(2) since $\Gamma \vdash C_1[x] : A \Rightarrow B \in \mathsf{sn}$ is smaller than $\Gamma \vdash C[x] \in \mathsf{sn}$

Sub-case $\dfrac{\Gamma \vdash C[x] : A \Rightarrow B \quad \Gamma \vdash N \longrightarrow N' : A}{\Gamma \vdash C[x]\,N \longrightarrow C[x]\,N' : B}$

$\Gamma \vdash N' : A \in \mathsf{sn}$ by assumption $\Gamma \vdash N : A \in \mathsf{sn}$
$\Gamma \vdash C[x]\,N' : B \in \mathsf{sn}$ by IH(2)

□

Neutral terms

$$\frac{x{:}A \in \Gamma}{\Gamma \vdash x : A \in \mathsf{SNe}} \qquad \frac{\Gamma \vdash R : A \Rightarrow B \in \mathsf{SNe} \qquad \Gamma \vdash M : A \in \mathsf{SN}}{\Gamma \vdash R\,M : B \in \mathsf{SNe}}$$

Normal terms

$$\frac{\Gamma \vdash R : A \in \mathsf{SNe}}{\Gamma \vdash R : A \in \mathsf{SN}} \qquad \frac{\Gamma, x{:}A \vdash M : A \Rightarrow B \in \mathsf{SN}}{\Gamma \vdash \lambda x{:}A.M : A \Rightarrow B \in \mathsf{SN}} \qquad \frac{\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : A \qquad \Gamma \vdash M' : A \in \mathsf{SN}}{\Gamma \vdash M : A \in \mathsf{SN}}$$

Strong head reduction

$$\frac{\Gamma \vdash N : A \in \mathsf{SN} \quad \Gamma, x{:}A \vdash M : B}{\Gamma \vdash (\lambda x.M)\ N \longrightarrow_{\mathsf{SN}} [N/x]M : B} \qquad \frac{\Gamma \vdash R \longrightarrow_{\mathsf{SN}} R' : A \Rightarrow B \quad \Gamma \vdash M : A}{\Gamma \vdash R\,M \longrightarrow_{\mathsf{SN}} R'\,M}$$

Figure 1: Inductive definition of strongly normalizing terms

3.2 Inductive Definition of Strongly Normalizing Terms

Following van Raamsdonk and Severi [1995] and Joachimski and Matthes [2003] we define inductively the set of normal terms, SN, and the set of neutral terms, SNe, using the following judgments:

$\Gamma \vdash M : A \in \mathsf{SN}$	M is in the set of normal terms of type A
$\Gamma \vdash M : A \in \mathsf{SNe}$	M is in the set of neutral terms of type A

Our inductive definition given in Fig. 1 tracks typing information, as before. This will allow us to easily extend our framework with the unit type. As van Raamsdonk and Severi [1995] observed, many proofs, not only normalization proofs, become simpler using the inductive definition, since it allows us to prove properties by structural induction. This is in contrast to the accessibility notion of strong normalization where we often have to reason about reduction sequences and about positions of terms. As Joachimski and Matthes [2003] put it: "the reduct analysis becomes increasingly annoying in normalization proofs for more and more complex systems." Using the inductive definition of normal and neutral terms, we reduce the task of checking all one-step reducts to analysing no more than one standard reduct and some subterms. The proof of equivalence between the inductive notion of normalization and the accessibility notion given earlier is in fact the only place where reduct analysis has to be carried out. Hence this approach seems particularly amendable to mechanizing proofs.

Lemma 3.5 (SN and SNe characterize well-typed terms)**.**

1. *If* $\Gamma \vdash M : A \in \mathsf{SN}$ *then* $\Gamma \vdash M : A$.
2. *If* $\Gamma \vdash M : A \in \mathsf{SNe}$ *then* $\Gamma \vdash M : A$.
3. *If* $\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : A$ *then* $\Gamma \vdash M : A$ *and* $\Gamma \vdash M' : A$.

Proof. By induction on the definition of SN, SNe, and $\longrightarrow_{\mathsf{SN}}$. □

Lemma 3.6 (Renaming)**.**

1. *If* $\Gamma \vdash M : A \in \mathsf{SN}$ *and* $\Gamma' \geq_\rho \Gamma$ *then* $\Gamma' \vdash [\rho]M : A \in \mathsf{SN}$
2. *If* $\Gamma \vdash M : A \in \mathsf{SNe}$ *and* $\Gamma' \geq_\rho \Gamma$ *then* $\Gamma' \vdash [\rho]M : A \in \mathsf{SNe}$
3. *If* $\Gamma \vdash M \longrightarrow_{\mathsf{SN}} N : A$ *and* $\Gamma' \geq_\rho \Gamma$ *then* $\Gamma' \vdash [\rho]M \longrightarrow_{\mathsf{SN}} [\rho]N : A$.

Proof. By induction on the first derivation.

Case: $\mathcal{D} = \dfrac{\Gamma \vdash R : A \in \mathsf{SNe}}{\Gamma \vdash R : A \in \mathsf{SN}}$

$\Gamma' \vdash [\rho]R : A \in \mathsf{SNe}$ by IH (2)
$\Gamma' \vdash [\rho]R : A \in \mathsf{SN}$ by def. of SN

Case: $\mathcal{D} = \dfrac{\Gamma, x{:}A \vdash M : B \in \mathsf{SN}}{\Gamma \vdash \lambda x{:}A.M : A \Rightarrow B \in \mathsf{SN}}$

$\Gamma', x{:}A \geq_{\rho, x/x} \Gamma, x{:}A$ by def. of $\geq_\rho$
$\Gamma', x{:}A \vdash [\rho, x/x]M : B \in \mathsf{SN}$ by IH (1)
$\Gamma' \vdash \lambda x{:}A.[\rho, x/x]M : A \Rightarrow B \in \mathsf{SN}$ by def. of SN
$\Gamma' \vdash [\rho](\lambda x{:}A.M) : A \Rightarrow B \in \mathsf{SN}$ by subst. def.

Case: $\mathcal{D} = \dfrac{\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : A \qquad \Gamma \vdash M' : A \in \mathsf{SN}}{\Gamma \vdash M : A \in \mathsf{SN}}$

$\Gamma' \vdash [\rho]M \longrightarrow_{\mathsf{SN}} [\rho]M' : A$ by IH (3)
$\Gamma' \vdash [\rho]M' : A \in \mathsf{SN}$ by IH (1)
$\Gamma' \vdash [\rho]M : A \in \mathsf{SN}$ by def. of SN

Case: $\mathcal{D} = \dfrac{x{:}A \in \Gamma}{\Gamma \vdash x : A \in \mathsf{SNe}}$

$\Gamma' \geq_\rho \Gamma$ by assumption
$\Gamma' \vdash [\rho]x : A$ by renaming of typing
$\Gamma' \vdash [\rho]x : A \in \mathsf{SNe}$ by def. of SNe

Case: $\mathcal{D} = \dfrac{\Gamma \vdash R : A \Rightarrow B \in \mathsf{SNe} \qquad \Gamma \vdash M : A \in \mathsf{SN}}{\Gamma \vdash R\,M : A \Rightarrow B \in \mathsf{SNe}}$

$\Gamma' \vdash [\rho]R : A \Rightarrow B \in \mathsf{SNe}$ by IH (2)
$\Gamma' \vdash [\rho]M : A \in \mathsf{SN}$ by IH (1)
$\Gamma' \vdash [\rho]R\ [\rho]M : A \Rightarrow B \in \mathsf{SNe}$ by def. of SNe
$\gamma' \vdash [\rho](R\ M) : B \in \mathsf{SNe}$ by subst. def.

Case: $\mathcal{D} = \dfrac{\Gamma, x{:}A \vdash M : B \qquad \Gamma \vdash N : A \in \mathsf{SN}}{\Gamma \vdash (\lambda x{:}A.M)\ N \longrightarrow_{\mathsf{SN}} [N/x]M : B}$

$\Gamma' \vdash [\rho]N : A \in \mathsf{SN}$	by IH (1)
$\Gamma' \geq_\rho \Gamma$	by assumption
$\Gamma', x{:}A \geq_\rho \Gamma$	by weakening
$\Gamma', x{:}A \geq_{\rho, x/x} \Gamma, x{:}A$	by def. of weakening subst
$\Gamma', x{:}A \vdash [\rho, x/x]M : B$	by weakening lemma
$\Gamma' \vdash (\lambda x{:}A.[\rho, x/x]M)\ [\rho]N \longrightarrow_{\mathsf{SN}} [\rho, [\rho]N/x]M : B$	by def. of $\longrightarrow_{\mathsf{SN}}$
$\Gamma' \vdash [\rho]((\lambda x{:}AM)\ N) \longrightarrow_{\mathsf{SN}} [\rho]([N/x]M) : B$	by def. of subst

Case: $\mathcal{D} = \dfrac{\Gamma \vdash R \longrightarrow_{\mathsf{SN}} R' : A \Rightarrow B \quad \Gamma \vdash M : A}{\Gamma \vdash R\,M \longrightarrow_{\mathsf{SN}} R'\,M : B}$

$\Gamma' \vdash [\rho]R \longrightarrow_{\mathsf{SN}} [\rho]R' : A \Rightarrow B$	by IH(3)
$\Gamma' \vdash [\rho]M : A$	by weakening of typing
$\Gamma \vdash [\rho]R\ [\rho]M \longrightarrow_{\mathsf{SN}} [\rho]R'\ [\rho]M : B$	by def. of $\longrightarrow_{\mathsf{SN}}$
$\Gamma \vdash [\rho](R\ M) \longrightarrow_{\mathsf{SN}} [\rho](R'\ M) : B$	by def. of subst.

□

Lemma 3.7 (Anti-Renaming)**.**

1. *If* $\Gamma' \vdash [\rho]M : A \in \mathsf{SN}$ *and* $\Gamma' \geq_\rho \Gamma$ *then* $\Gamma \vdash M : A \in \mathsf{SN}$
2. *If* $\Gamma' \vdash [\rho]M : A \in \mathsf{SNe}$ *and* $\Gamma' \geq_\rho \Gamma$ *then* $\Gamma \vdash M : A \in \mathsf{SNe}$
3. *If* $\Gamma' \vdash [\rho]M \longrightarrow_{\mathsf{SN}} [\rho]N : A$ *and* $\Gamma' \geq_\rho \Gamma$ *then* $\Gamma \vdash M \longrightarrow_{\mathsf{SN}} N : A$.

Proof. By induction on the first derivation. [to check] □

Lemma 3.8 (Stable under Substitution)**.**

1. *If* $\Gamma, x{:}A \vdash M : B \in \mathsf{SN}$ *and* $\Gamma \vdash N : A \in \mathsf{SN}$ *then* $\Gamma \vdash [N/x]M : B \in \mathsf{SN}$.
2. *If* $\Gamma, x{:}A \vdash R : B \in \mathsf{SNe}$ *and* $\Gamma \vdash N : A \in \mathsf{SN}$ *then* $\Gamma \vdash [N/x]R : B \in \mathsf{SN}$.
3. *If* $\Gamma, x{:}A \vdash M \longrightarrow_{\mathsf{SN}} M' : B$ *and* $\Gamma \vdash N : A \in \mathsf{SN}$ *then* $\Gamma \vdash [N/x]M \longrightarrow_{\mathsf{SN}} [N/x]M' : B$.

Proof. Simultaneous induction on $\Gamma, x{:}A \vdash M \in \mathsf{SN}$.

□

Lemma 3.9 (SN is closed under application)**.** *If* $\Gamma \vdash M : A \Rightarrow B \in \mathsf{SN}$ *and* $\Gamma \vdash N : A \in \mathsf{SN}$ *then* $\Gamma \vdash M\ N : B \in \mathsf{SN}$.

Proof. By induction on SN.

Case: $\mathcal{D} = \dfrac{\Gamma \vdash R : A \in \mathsf{SNe}}{\Gamma \vdash R : A \in \mathsf{SN}}$

$\Gamma \vdash R\ N : B \in \mathsf{SNe}$	by def. of SNe
$\Gamma \vdash R\ N : B \in \mathsf{SN}$	by def. of SN

Case $\mathcal{D} = \dfrac{\Gamma, y{:}A \vdash M : B \in \mathsf{SN}}{\Gamma \vdash \lambda y{:}A.M : A \Rightarrow B \in \mathsf{SN}}$

$\Gamma \vdash [N/y]M : B \in \mathsf{SN}$ by substitution lemma 3.8
$\Gamma \vdash N : A \in \mathsf{SN}$ by assumption
$\Gamma \vdash (\lambda y{:}A.M)\ N \longrightarrow_{\mathsf{SN}} [N/y]M : B$ by def. of $\longrightarrow_{\mathsf{SN}}$
$\Gamma \vdash (\lambda y{:}A.M)\ N : B \in \mathsf{SN}$ by def. of SN

Case $\mathcal{D} = \dfrac{\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : A \Rightarrow B \qquad \Gamma \vdash M' : A \Rightarrow B \in \mathsf{SN}}{\Gamma \vdash M : A \Rightarrow B \in \mathsf{SN}}$

$\Gamma \vdash N : A \in \mathsf{SN}$ by assumption
$\Gamma \vdash N : A$ by typing
$\Gamma \vdash M\ N \longrightarrow_{\mathsf{SN}} M'\ N : B$ by def. of $\longrightarrow_{\mathsf{SN}}$
$\Gamma \vdash M'\ N : B \in \mathsf{SN}$ by IH
$\Gamma \vdash M\ N : B \in \mathsf{SN}$ by def. of SN. □

Lemma 3.10 (SN is closed under application to variables)**.** *If* $\Gamma \vdash M : A \Rightarrow B \in \mathsf{SN}$ *and* $x{:}A \in \Gamma$ *then* $\Gamma \vdash M\ x : B \in \mathsf{SN}$.

Proof. Follows from the previous lemma 3.9[2].

□

We will use the extensionality of SN for function types in the proof of CR1:

Lemma 3.11 (Extentionality of SN)**.** *If* $x{:}A \in \Gamma$ *and* $\Gamma \vdash M\ x : B \in \mathsf{SN}$ *then* $\Gamma \vdash M : A \Rightarrow B \in \mathsf{SN}$.

Proof. By induction on SN

Case: $\mathcal{D} = \dfrac{\Gamma \vdash M\ x : B \in \mathsf{SNe}}{\Gamma \vdash M\ x : B \in \mathsf{SN}}$

$\Gamma \vdash M : A \Rightarrow B \in \mathsf{SNe}$ by def. of SNe
$\Gamma \vdash M : A \Rightarrow B \in \mathsf{SN}$ by def. of SN

Case: $\mathcal{D} = \dfrac{\Gamma \vdash M\ x \longrightarrow_{\mathsf{SN}} Q : B \qquad \Gamma \vdash Q : B \in \mathsf{SN}}{\Gamma \vdash M\ x : B \in \mathsf{SN}}$

Sub-case: $\Gamma \vdash (\lambda y{:}A.M')\ x \longrightarrow_{\mathsf{SN}} [x/y]M' : B$

$\Gamma \vdash [x/y]M' : B \in \mathsf{SN}$ by assumption
$\Gamma, y{:}A \vdash M' : B \in \mathsf{SN}$ by Anti-Renaming Property (Lemma 3.7)
$\Gamma \vdash \lambda y{:}A.M' : A \Rightarrow B \in \mathsf{SN}$ by def. of SN

Sub-case: $\Gamma \vdash M\ x \longrightarrow_{\mathsf{SN}} M'\ x : B$ and $Q = M'\ x$

[2]For proving the CR properties this lemma suffices and our mechanization in Beluga proves this lemma inductively; we need the more general lemma to show completeness of SN with respect to sn.

$\Gamma \vdash M \longrightarrow_{SN} M' : A \Rightarrow B$ by def. of $\longrightarrow_{SN}$
$\Gamma \vdash M' : A \Rightarrow B \in SN$ by IH
$\Gamma \vdash M : A \Rightarrow B \in SN$ by def. of SN
□

3.3 Soundness and Completeness

We can now prove that the two definitions of strongly normalizing terms coincide (soundness and completeness). For proving normalization, soundness of the inductive definition of SN suffices.

Lemma 3.12. *If* $\Gamma \vdash M \longrightarrow_{SN} M_1 : A$ *and* $\Gamma \vdash M_1 : A \in SN$ *and* $\Gamma \vdash M_1 : A \in sn$ *and* $\Gamma \vdash M \longrightarrow M_2$ *then* $\Gamma \vdash M_2 : A \in sn$.

Proof. Proof by case analysis and induction on evaluation context ?.

Case $\dfrac{\Gamma \vdash N : A \in SN \quad \Gamma, x{:}A \vdash M : B}{\Gamma \vdash (\lambda x.M)\ N \longrightarrow_{SN} [N/x]M : B}$ and $\dfrac{\Gamma \vdash \lambda x{:}A.M : A \Rightarrow B \quad \Gamma \vdash N : A}{\Gamma \vdash (\lambda x.M)\ N \longrightarrow [N/x]M : B}$

$\Gamma \vdash [N/x]M : B \in sn$ by assumption (and $M_1 = M_2$)

Case $\dfrac{\Gamma \vdash N : A \in SN \quad \Gamma, x{:}A \vdash M : B}{\Gamma \vdash (\lambda x.M)\ N \longrightarrow_{SN} [N/x]M : B}$ and $\dfrac{\Gamma \vdash \lambda x.M \longrightarrow \lambda x.M' : A \Rightarrow B \qquad \Gamma \vdash N : A}{\Gamma \vdash (\lambda x.M)\ N \longrightarrow (\lambda x.M')\ N : B}$

$\Gamma, x : A \vdash M \longrightarrow M' : B$ by inversion on $\longrightarrow$
TO SHOW: $\Gamma \vdash (\lambda x.M')\ N : B \in sn$

Case $\dfrac{\Gamma \vdash N : A \in SN \quad \Gamma, x{:}A \vdash M : B}{\Gamma \vdash (\lambda x.M)\ N \longrightarrow_{SN} [N/x]M : B}$ and $\dfrac{\Gamma \vdash \lambda x.M : A \Rightarrow B \quad \Gamma \vdash N \longrightarrow N' : A}{\Gamma \vdash (\lambda x.M)\ N \longrightarrow (\lambda x.M)\ N' : B}$

TO SHOW: $\Gamma \vdash (\lambda x.M)\ N' : B \in sn$

Case $\dfrac{\Gamma \vdash R \longrightarrow_{SN} R' : A \Rightarrow B \quad \Gamma \vdash N : A}{\Gamma \vdash R\,N \longrightarrow_{SN} R'\,N}$ and $\dfrac{\Gamma \vdash R \longrightarrow R'' : A \Rightarrow B \quad \Gamma \vdash N : A}{\Gamma \vdash R\,N \longrightarrow R''\,N : B}$

where R is not a λ-abstraction

TO SHOW: $\Gamma \vdash R''\ N : B \in sn$

Case $\dfrac{\Gamma \vdash R \longrightarrow_{SN} R' : A \Rightarrow B \quad \Gamma \vdash N : A}{\Gamma \vdash R\,N \longrightarrow_{SN} R'\,N}$ and $\dfrac{\Gamma \vdash N \longrightarrow N' : A \Rightarrow B \quad \Gamma \vdash R : A \Rightarrow B}{\Gamma \vdash R\,N \longrightarrow R\,N' : B}$

where R is not a λ-abstraction

TO SHOW: $\Gamma \vdash R\ N' : B \in sn$ □

Corollary 3.13. *If* $\Gamma \vdash M \longrightarrow_{SN} M' : A$ *and* $\Gamma \vdash M' : A \in SN$ *and* $\Gamma \vdash M' : A \in sn$ *then* $\Gamma \vdash M : A \in sn$.

Proof. Direct by previous lemma 3.12 □

Theorem 3.14 (Soundness of SN)**.**

1. *If* $\Gamma \vdash M : A \in \mathsf{SN}$ *then* $\Gamma \vdash M : A \in \mathsf{sn}$.
2. *If* $\Gamma \vdash C[x] : A \in \mathsf{SNe}$ *then* $\Gamma \vdash C[x] : A \in \mathsf{sn}$.

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

1. If $\Gamma \vdash M : A \in \mathsf{SN}$ then $\Gamma \vdash M : A \in \mathsf{sn}$.

Case $\mathcal{D} = \dfrac{\Gamma \vdash R : A \in \mathsf{SNe}}{\Gamma \vdash R : A \in \mathsf{SN}}$

$R = C[x]$ since $\Gamma \vdash R : A \in \mathsf{SNe}$
$\Gamma \vdash R : A \in \mathsf{sn}$ by IH(1)

Case $\mathcal{D} = \dfrac{\Gamma, x{:}A \vdash M : B \in \mathsf{SN}}{\Gamma \vdash \lambda x{:}A.M : A \Rightarrow B \in \mathsf{SN}}$

$\Gamma, x{:}A \vdash M : B \in \mathsf{sn}$ by IH(1)
$\Gamma \vdash \lambda x{:}A.M : A \Rightarrow B \in \mathsf{sn}$ by Property 3.2(2)

Case $\mathcal{D} = \dfrac{\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : A \qquad \Gamma \vdash M' : A \in \mathsf{SN}}{\Gamma \vdash M : A \in \mathsf{SN}}$

$\Gamma \vdash M' : A \in \mathsf{sn}$ by IH(1)
$\Gamma \vdash M : A \in \mathsf{sn}$ by Lemma 3.12

2. If $\Gamma \vdash C[x] : A \in \mathsf{SNe}$ then $\Gamma \vdash C[x] : A \in \mathsf{sn}$.

Case $\mathcal{D} = \dfrac{x{:}A \in \Gamma}{\Gamma \vdash x : A \in \mathsf{SNe}}$

$C = \_$ since $C[x] = x$
$\forall M'.\ \Gamma \vdash x \longrightarrow M' : A \Longrightarrow \Gamma \vdash M' : A \in \mathsf{sn}$ since $\Gamma \vdash x \longrightarrow M' : A$ is impossible
$\Gamma \vdash x \in \mathsf{sn}$

Case $\mathcal{D} = \dfrac{\Gamma \vdash R : A \Rightarrow B \in \mathsf{SNe} \qquad \Gamma \vdash M : A \in \mathsf{SN}}{\Gamma \vdash R\,M : B \in \mathsf{SNe}}$

$C'[x] = R$ since $C[x] = R\ M$
$\Gamma \vdash C'[x] : A \Rightarrow B \in \mathsf{sn}$ by IH(2)
$\Gamma \vdash M : A \in \mathsf{sn}$ by IH(1)
$\Gamma \vdash C'[x]\ M : B \in \mathsf{sn}$ by Closure Property 3.4(2)
$\Gamma \vdash C[x] : A \Rightarrow B \in \mathsf{sn}$ since $C[x] = C'[x]\ M$

□

Theorem 3.15 (Completeness of SN)**.**

1. *If* $\Gamma \vdash C[x] : A \in \mathsf{sn}$ *then* $\Gamma \vdash C[x] : A \in \mathsf{SNe}$.
2. *If* $\Gamma \vdash C[(\lambda x.M)\ N] : A \in \mathsf{sn}$ *then* $\Gamma \vdash C[(\lambda x.M)\ N] \longrightarrow_{\mathsf{SN}} C[[N/x]M] : A$ *and* $\Gamma \vdash C[[N/x]M] : A \in \mathsf{SN}$.
3. *If* $\Gamma \vdash M : A \in \mathsf{sn}$ *then* $\Gamma \vdash M : A \in \mathsf{SN}$.

Proof. 1. If $\Gamma \vdash C[x] : A \in \mathsf{sn}$ then $\Gamma \vdash C[x] : A \in \mathsf{SNe}$.

By structural induction on $C[x]$.

Case $C = \_$

$\Gamma \vdash x : A$	by assumption $\Gamma \vdash x : A \in \mathsf{sn}$
$\Gamma \vdash x : A \in \mathsf{SNe}$	by def. of SNe

Case $C = C'\ M$

$\Gamma \vdash C'[x]\ M : B \in \mathsf{sn}$	by assumption
$\Gamma \vdash C'[x] : A \Rightarrow B \in \mathsf{sn}$ and $\Gamma \vdash M : A \in \mathsf{sn}$	by Lemma 3.2 (Property 3)
$\Gamma \vdash C'[x] : A \Rightarrow B \in \mathsf{SNe}$	by IH(1)
$\Gamma \vdash M : A \in \mathsf{SN}$	by IH (3)
$\Gamma \vdash C'[x]\ M : B \in \mathsf{SNe}$	by def. of SNe

2. If $\Gamma \vdash C[(\lambda x{:}A.M)\ N] : B \in \mathsf{sn}$ then $\Gamma \vdash C[(\lambda x{:}A.M)\ N] \longrightarrow_{\mathsf{SN}} C[[N/x]M] : B$ and $\Gamma \vdash C[[N/x]M] : B \in \mathsf{SN}$.

By structural induction on $C[(\lambda x.M)\ N]$. We again leave some of the reasoning about well-typed terms implicit.

Case $C = \_$

$\Gamma \vdash (\lambda x{:}A.M)\ N : B \in \mathsf{sn}$	by assumption
$\Gamma \vdash \lambda x{:}A.M : A \Rightarrow B \in \mathsf{sn}$ and $\Gamma \vdash N : A \in \mathsf{sn}$	by Lemma 3.2(Property 3)
$\Gamma \vdash N : A \in \mathsf{SN}$	by IH (3)
$\Gamma \vdash \lambda x{:}A.M : A \Rightarrow B \in \mathsf{SN}$	by IH (3)
$\Gamma, x{:}A \vdash M : B \in \mathsf{SN}$	by def. of SN
$\Gamma \vdash [N/x]M : B \in \mathsf{SN}$	by subst. lemma 3.8
$\Gamma \vdash (\lambda x{:}A.M)\ N \longrightarrow_{\mathsf{SN}} [N/x]M : B$	by def. of $\longrightarrow_{\mathsf{SN}}$

Case $C = C'\ M'$

$\Gamma \vdash C'[(\lambda x{:}A.M)\ N]\ M' : B \in \mathsf{sn}$	by assumption
$\Gamma \vdash C'[(\lambda x{:}A.M)\ N] : B' \Rightarrow B \in \mathsf{sn}$ and $\Gamma \vdash M' : B' \in \mathsf{sn}$	by Lemma 3.2(Property 3)
$\Gamma \vdash N : A \in \mathsf{sn}$	by Lemma 3.2(Property 3) (iterated)
$\Gamma \vdash C'[(\lambda x{:}A.M)\ N] \longrightarrow_{\mathsf{SN}} C'[[N/x]M] : B' \Rightarrow B$ and $\Gamma \vdash C'[[N/x]M] : B' \Rightarrow B \in \mathsf{SN}$	by IH (2)
$\Gamma \vdash C'[(\lambda x{:}A.M)\ N]\ M' : B \longrightarrow_{\mathsf{SN}} C'[[N/x]M]\ M' : B$	by def. $\longrightarrow_{\mathsf{SN}}$
$\Gamma \vdash M' : B' \in \mathsf{SN}$	by IH (3)
$\Gamma \vdash C'[[N/x]M]\ M' : B \in \mathsf{SN}$	by Closure property (Lemma 3.9)

If $\Gamma \vdash M : A \in \mathsf{sn}$ then $\Gamma \vdash M : A \in \mathsf{SN}$.

Induction on M.

Case $M = x$ where $x{:}A \in \Gamma$.

$\Gamma \vdash x : A \in \mathsf{SNe}$ by def. of SNe
$\Gamma \vdash x : A \in \mathsf{SN}$ by def. of SN.

Case $M = \lambda x{:}A.M'$

$\Gamma \vdash \lambda x{:}A.M' : A \Rightarrow B \in \mathsf{sn}$ by assumption
$\Gamma, x{:}A \vdash M' : B \in \mathsf{sn}$ by Lemma 3.2 (Property 4)
$\Gamma, x{:}A \vdash M' : B \in \mathsf{SN}$ by IH
$\Gamma \vdash \lambda x{:}A.M' : A \Rightarrow B \in \mathsf{SN}$ by def. of SN

Case $M = M_1\ M_2$

$\Gamma \vdash M_1\ M_2 : B \in \mathsf{sn}$ by assumption
$\Gamma \vdash M_1 : A \Rightarrow B \in \mathsf{sn}$ and $\Gamma \vdash M_2 : A \in \mathsf{sn}$ by Lemma 3.2 (Property 3)

Sub-case: $C[x] = M_1\ M_2$

$\Gamma \vdash M_1\ M_2 : B \in \mathsf{SNe}$ by IH (1) (this is valid, since (1) is strictly decreasing when we refer to (3))
$\Gamma \vdash M_1\ M_2 : B \in \mathsf{SN}$ by def. of SN

Sub-case: $C[(\lambda x.M)\ N] = M_1\ M_2$

$\Gamma \vdash C[(\lambda x.M)\ N] \longrightarrow_{\mathsf{SN}} C[[N/x]M] : B$ and $\Gamma \vdash C[[N/x]M] : B \in \mathsf{SN}$ by IH(2)
$\Gamma \vdash C[(\lambda x.M)\ N] : B \in \mathsf{SN}$ by def of SN

□

4 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.

Theorem 4.1.

1. *CR1: If* $\Gamma \vdash M \in \mathcal{R}_A$ *then* $\Gamma \vdash M : A \in \mathsf{SN}$.
2. *CR2: If* $\Gamma \vdash M : A \in \mathsf{SNe}$ *then* $\Gamma \vdash M \in \mathcal{R}_A$.
3. *CR3: If* $\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : A$ *and* $\Gamma \vdash M' \in \mathcal{R}_A$ *then* $\Gamma \vdash M \in \mathcal{R}_A$*, i.e. backwards closure.*

Proof. We prove these three properties simultaneously.

CR1. If $\Gamma \vdash M \in \mathcal{R}_C$ then $\Gamma \vdash M : A \in \mathsf{SN}$.

By induction on the structure of C.

Case: $C = \mathbf{i}$.

$\Gamma \vdash M \in \mathcal{R}_i$	by assumption
$\Gamma \vdash M : i \in \mathsf{SN}$	by def. of sem. interpretation for i

Case: $C = A \Rightarrow B$.

$\Gamma, x{:}A \vdash x : A \in \mathsf{SNe}$	by def. of SNe
$\Gamma.x{:}A \vdash x \in \mathcal{R}_A$	by IH (2)
$\Gamma, x{:}A \geq_{\mathsf{wk}} \Gamma$	by def. of context extensions
$\Gamma, x{:}A \vdash [\mathsf{wk}]M\ x \in \mathcal{R}_B$	by def. of $\Gamma, x{:}A \vdash M \in \mathcal{R}_{A \Rightarrow B}$
$\Gamma, x{:}A \vdash [\mathsf{wk}]M\ x : B \in \mathsf{SN}$	by IH (CR1)
$\Gamma, x{:}A \vdash [\mathsf{wk}]M : A \Rightarrow B \in \mathsf{SN}$	by Extensionality Lemma 3.11
$\Gamma \vdash M : A \Rightarrow B \in \mathsf{SN}$	by Anti-renaming Lemma 3.7

CR2. If $\Gamma \vdash M : C \in \mathsf{SNe}$ then $\Gamma \vdash M \in \mathcal{R}_C$.

By induction on $\Gamma \vdash M : C \in \mathsf{SNe}$.

Case: $C = \mathbf{i}$.

$\Gamma \vdash M : C \in \mathsf{SNe}$	by assumption
$\Gamma \vdash M : C \in \mathsf{SN}$	by def. of SN
$\Gamma \vdash M \in \mathcal{R}_i$	by def. of semantic typing

Case: $C = A \Rightarrow B$.

Assume $\Gamma' \geq_\rho \Gamma$ and $\Gamma' \vdash N \in \mathcal{R}_A$

$\Gamma' \vdash N : A \in \mathsf{SN}$	by IH (CR1)
$\Gamma \vdash M : A \Rightarrow B \in \mathsf{SNe}$	by assumption
$\Gamma' \vdash [\rho]M : A \Rightarrow B \in \mathsf{SNe}$	by Renaming Lemma 3.6
$\Gamma' \vdash [\rho]M\ N : B \in \mathsf{SNe}$	by def. of SNe
$\Gamma' \vdash [\rho]M\ N \in \mathcal{R}_B$	by IH (CR2)
$\Gamma \vdash M \in \mathcal{R}_{A \Rightarrow B}$	since $\Gamma' \vdash N \in \mathcal{R}_A$ was arbitrary

CR3. If $\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : C$ and $\Gamma \vdash M' \in \mathcal{R}_C$ then $\Gamma \vdash M \in \mathcal{R}_C$

By induction on C.

Case: $C = \mathbf{i}$.

$\Gamma \vdash M' : i \in \mathsf{SN}$	since $\Gamma \vdash M' \in \mathcal{R}_i$
$\Gamma \vdash M : i \in \mathsf{SN}$	by closure rule for SN
$\Gamma \vdash M \in \mathcal{R}_i$	by definition of semantic typing

Case: $C = A \Rightarrow B$.

Assume $\Gamma' \geq_\rho \Gamma$, $\Gamma' \vdash N \in \mathcal{R}_A$

$\Gamma' \vdash M'[\rho]\ N \in \mathcal{R}_B$	by assumption $\Gamma \vdash M' \in \mathcal{R}_{A \Rightarrow B}$
$\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : A \Rightarrow B$	by assumption
$\Gamma' \vdash [\rho]M \longrightarrow_{\mathsf{SN}} [\rho]M' : A \Rightarrow B$	by Renaming Lemma 3.6
$\Gamma' \vdash [\rho]M\ N \longrightarrow_{\mathsf{SN}} [\rho]M'\ N : B$	by $\longrightarrow_{\mathsf{SN}}$
$\Gamma \vdash [\rho]M\ N \in \mathcal{R}_B$	by IH (CR3)
$\Gamma \vdash M \in \mathcal{R}_{A \Rightarrow B}$	since $\Gamma' \vdash N \in \mathcal{R}_A$ was arbitrary

□

5 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 $\Gamma \vdash M \in \mathcal{R}_A$ then $\Gamma \vdash M : A \in \mathsf{SN}$.

Step 2 If $\Gamma \vdash M : A$ and $\Gamma' \vdash \sigma \in \mathcal{R}_\Gamma$ then $\Gamma' \vdash [\sigma]M \in \mathcal{R}_A$.

The first part described in Step 1, is satisfied by the fact that $\Gamma \vdash M \in \mathcal{R}_A$ must be a reducibility candidate (Theorem 4.1) and by CR1) all terms in $\mathcal{R}_A$ 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 $\Gamma \vdash [\sigma]M \in \mathcal{R}_A$.

Lemma 5.1 (Fundamental lemma)**.** *If* $\Gamma \vdash M : A$ *and* $\Gamma' \vdash \sigma \in \mathcal{R}_\Gamma$ *then* $\Gamma' \vdash [\sigma]M \in \mathcal{R}_A$.

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

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

$\Gamma' \vdash \sigma \in \mathcal{R}_\Gamma$	by assumption
$\Gamma' \vdash [\sigma]x \in \mathcal{R}_A$	by definition of $[\sigma]x$ and $\Gamma' \vdash \sigma \in \mathcal{R}_\Gamma$

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

$\Gamma' \vdash \sigma \in \mathcal{R}_\Gamma$	by assumption
$\Gamma' \vdash [\sigma]M \in \mathcal{R}_{A \to B}$	by IH
$\Gamma' \vdash [\sigma]N \in \mathcal{R}_A$	by IH
$\Gamma' \vdash [\sigma]M\ [\sigma]N \in \mathcal{R}_B$	by $\Gamma' \vdash [\sigma]M \in \mathcal{R}_{A \to B}$
$\Gamma' \vdash [\sigma](M\ N) \in \mathcal{R}_B$	by subst. definition

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

$\Gamma' \vdash \sigma \in \mathcal{R}_\Gamma$	by assumption
Assume $\Gamma'' \geq_\rho \Gamma'$ and $\Gamma'' \vdash N : A$	
$\Gamma'' \vdash [\rho]\sigma \in \mathcal{R}_\Gamma$	by weakening
$\Gamma'' \vdash ([\rho]\sigma, N/x) \in \mathcal{R}_{\Gamma, x:A}$	by definition of semantic substitutions
$\Gamma'' \vdash [[\rho]\sigma, N/x]M \in \mathcal{R}_B$	by IH
$\Gamma'' \vdash (\lambda x.[[\rho]\sigma, x/x]M)\ N \longrightarrow_{\mathsf{SN}} [[\rho]\sigma, N/x]M$	by reduction $\longrightarrow_{\mathsf{SN}}$
$(\lambda x.[[\rho]\sigma, x/x]M) = [[\rho]\sigma](\lambda x.M)$	by subst. def
$\Gamma'' \vdash ([[\rho]\sigma]\lambda x.M)\ N \in \mathcal{R}_B$	by CR3
$\Gamma' \vdash [\sigma](\lambda x.M) \in \mathcal{R}_{A \Rightarrow B}$	since $\Gamma'' \geq_\rho \Gamma'$ and $\Gamma'' \vdash N : A$ was arbitrary

□

Corollary 5.2. *If* $\Gamma \vdash M : A$ *then* $\Gamma \vdash M : A \in \mathsf{SN}$.

Proof. Using the fundamental lemma with the identity substitution $\Gamma \vdash \mathsf{id} \in \mathcal{R}_\Gamma$, we obtain $\Gamma \vdash M \in \mathcal{R}_A$. By CR1, we know $\Gamma \vdash M \in \mathsf{SN}$. □

6 Extension: Unit type

We will now extend our simply-typed lambda-calculus the unit type, written as 1.

$$\begin{array}{llll} \text{Types} & A & ::= & \ldots \mid 1 \\ \text{Terms} & M & ::= & \ldots \mid () \end{array}$$

In particular, we extend our type-directed reduction rules and allow any term M of type 1 to be reduced to $()$.

$$\frac{M \neq ()}{\Gamma \vdash M \longrightarrow () : 1}$$

We extend our definition of SN and $\longrightarrow_{\mathsf{SN}}$ as follows:

$$\frac{}{\Gamma \vdash () : 1 \in \mathsf{SN}} \qquad \frac{\Gamma \vdash M : 1}{\Gamma \vdash M \longrightarrow_{\mathsf{SN}} () : 1}$$

We omit here the extensions in the proofs about SN, in particular the renaming, anti-renaming and substitution lemmas.

As 1 is simply a new base type, we simply say

$$\Gamma \vdash M \in \mathcal{R}_1 \quad \text{iff} \quad \Gamma \vdash M : 1 \in \mathsf{SN}$$

We revisit our previous theorem 4.1 and highlight the cases for unit.

Theorem. CR1: If $\Gamma \vdash M \in \mathcal{R}_A$ then $\Gamma \vdash M : A \in \mathsf{SN}$.

Proof. Induction on type A.

Case $A = 1$.

$\Gamma \vdash M : 1 \in \mathsf{SN}$ by def. of $\Gamma \vdash M \in \mathcal{R}_A$

□

Theorem. CR2: If $\Gamma \vdash M : A \in \mathsf{SNe}$ then $\Gamma \vdash M \in \mathcal{R}_A$.

Proof. Induction on A.

Case $A = 1$.

$\Gamma \vdash M : 1 \in \mathsf{SNe}$ by assumption
$\Gamma \vdash M : 1 \in \mathsf{SN}$ by def. of SN
$\Gamma \vdash M \in \mathcal{R}_1$ by def. of semantic interpretation of 1

□

Theorem. CR3: If $\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : A$ and $\Gamma \vdash M' \in \mathcal{R}_A$ then $\Gamma \vdash M \in \mathcal{R}_A$, i.e. backwards closure.

Proof. Induction on A.

Case $A = 1$

$\Gamma \vdash M' : 1 \in \mathsf{SN}$ by assumption $\Gamma \vdash M' \in \mathcal{R}_1$
$\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : 1$ by assumption $\Gamma \vdash M : 1 \in \mathsf{SN}$ by def. of SN

□

We can now revisit the fundamental lemma.

Lemma 6.1 (Fundamental lemma)**.** *If* $\Gamma \vdash M : C$ *and* $\Gamma' \vdash \sigma \in \mathcal{R}_\Gamma$ *then* $\Gamma' \vdash [\sigma]M \in \mathcal{R}_C$.

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

Case $\mathcal{D} = \dfrac{}{\Gamma \vdash () : 1}$

$\Gamma \vdash () : 1 \in \mathsf{SN}$ by def. of SN
$\Gamma \vdash () \in \mathcal{R}_1$ by def. of $\mathcal{R}_1$

□

Neutral terms

$$\frac{\Gamma \vdash M : A + B \in \mathsf{SNe} \quad \Gamma, x{:}A \vdash N_1 : C \in \mathsf{SN} \quad \Gamma, y{:}B \vdash N_2 : C \in \mathsf{SN}}{\Gamma \vdash \mathsf{case}\, M\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow N_1 \mid \mathsf{inr}\, y \Rightarrow N_2 : C \in \mathsf{SNe}}$$

Normal terms

$$\frac{\Gamma \vdash M : A \in \mathsf{SN}}{\Gamma \vdash \mathsf{inl}\, M : A + B \in \mathsf{SN}} \qquad \frac{\Gamma \vdash M : B \in \mathsf{SN}}{\Gamma \vdash \mathsf{inr}\, M : A + B \in \mathsf{SN}}$$

Strong head reduction

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

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

$$\frac{\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : A + B}{\Gamma \vdash \mathsf{case}\, M\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow N_1 \mid \mathsf{inr}\, y \Rightarrow N_2 \longrightarrow_{\mathsf{SN}} \mathsf{case}\, M'\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow N_1 \mid \mathsf{inr}\, y \Rightarrow N_2 : C}$$

Figure 2: Inductive definition of strongly normalizing terms - extended for case-expressions and injections

7 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. 2).

Next, we extend our definition of semantic type to disjoint sums. A first attempt might be to define $\mathcal{R}_{A+B}$ as follows:

Attempt 1

$$\begin{aligned} \Gamma \vdash M \in \mathcal{R}_{A+B} \text{ iff} \quad & M = \mathsf{inl}\, M' \text{ and } \Gamma \vdash M' \in \mathcal{R}_A, \\ & \textit{or } M = \mathsf{inr}\, M' \text{ and } \Gamma \vdash M' \in \mathcal{R}_B. \end{aligned}$$

However, this definition would not satisfy the key property CR3 and hence would fail to be a reducibility candidate. For example, while we have $y : A \vdash \mathsf{inl}\, y \in \mathcal{R}_{A+B}$, it is not the case that $y : A \vdash (\lambda x.\mathsf{inl}\, x)\, y \in \mathcal{R}_{A+B}$, despite the fact that $(\lambda x.\mathsf{inl}\, x)\, y \longrightarrow_{\mathsf{SN}} \mathsf{inl}\, y$.

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

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

and we define

$$\Gamma \vdash M \in \mathcal{R}_{A+B} \quad \text{iff} \quad \Gamma \vdash M \in \overline{\{\mathsf{inl}\ M' \mid \Gamma \vdash M' \in \mathcal{R}_A\} \cup \{\mathsf{inr}\ M' \mid \Gamma \vdash M' \in \mathcal{R}_B\}}$$

7.1 Semantic type $\mathcal{R}_{A+B}$ is a reducibility candidate

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

Theorem 7.1. *For all types* C, $\mathcal{R}_C \in CR$.

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

Case $C = A + B$.

1. *Show* CR1. Assume that $\Gamma \vdash M \in \mathcal{R}_{A+B}$. We consider different subcases and prove by an induction on the closure defining $\mathcal{R}_{A+B}$ that $\Gamma \vdash M : A + B \in \mathsf{SN}$.

   Subcase: $\Gamma \vdash M \in \{\mathsf{inl}\ N \mid \Gamma \vdash N \in \mathcal{R}_A\}$. Therefore $M = \mathsf{inl}\ N$. Since $\Gamma \vdash N \in \mathcal{R}_A$ and by i.h. (CR1), $\Gamma \vdash N : A \in \mathsf{SN}$. By definition of SN, we have that $\Gamma \vdash \mathsf{inl}\ N : A + B \in \mathsf{SN}$.

   Subcase: $\Gamma \vdash M \in \{\mathsf{inr}\ N \mid \Gamma \vdash N \in \mathcal{R}_B\}$. Therefore $M = \mathsf{inr}\ N$. Since $\Gamma \vdash N \in \mathcal{R}_B$ and by i.h. (CR1), $\Gamma \vdash N : B \in \mathsf{SN}$. By definition of SN, we have that $\Gamma \vdash \mathsf{inr}\ N : A + B \in \mathsf{SN}$.

   Subcase: $\Gamma \vdash M : A + B \in \mathsf{SNe}$. By definition of SN, we conclude that $\Gamma \vdash M : A + B \in \mathsf{SN}$.

   Subcase: $\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : A + B$ and $\Gamma \vdash M' \in \mathcal{R}_{A+B}$.

$\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : A + B$ and $\Gamma \vdash M' \in \mathcal{R}_{A+B}$	by assumption
$\Gamma \vdash M' : A + B \in \mathsf{SN}$	by inner i.h.
$\Gamma \vdash M : A + B \in \mathsf{SN}$	by reduction $\longrightarrow_{\mathsf{SN}}$

2. *Show* CR2. If $\Gamma \vdash M : A + B \in \mathsf{SNe}$, then $\Gamma \vdash M \in \mathcal{R}_{A+B}$.
   By definition of the closure, if $\Gamma \vdash M : A + B \in \mathsf{SNe}$, we have $\Gamma \vdash M \in \mathcal{R}_{A+B}$.

3. *Show* CR3. If $\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : A + B$ and $\Gamma \vdash M' \in \mathcal{R}_{A+B}$ then $\Gamma \vdash M \in \mathcal{R}_{A+B}$.
   By definition of the closure, if $\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : A + B$ and $\Gamma \vdash M' \in \mathcal{R}_{A+B}$, we have $\Gamma \vdash M \in \mathcal{R}_{A+B}$.

□

7.2 Revisiting the fundamental lemma

We can now revisit the fundamental lemma.

Lemma 7.2 (Fundamental lemma)**.** *If* $\Gamma \vdash M : C$ *and* $\Gamma' \vdash \sigma \in \mathcal{R}_\Gamma$ *then* $\Gamma' \vdash [\sigma]M \in \mathcal{R}_C$.

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

Case $\mathcal{D} = \dfrac{\Gamma \vdash M : A}{\Gamma \vdash \mathsf{inl}\, M : A + B}$

$\Gamma' \vdash \sigma \in \mathcal{R}_\Gamma$ by assumption
$\Gamma' \vdash [\sigma]M \in \mathcal{R}_A$ by i.h.
$\Gamma' \vdash \mathsf{inl}\, [\sigma]M \in \mathcal{R}_{A+B}$ by definition of $\mathcal{R}_{A+B}$
$\Gamma' \vdash [\sigma]\mathsf{inl}\, M \in \mathcal{R}_{A+B}$ by subst. definition

Case $\mathcal{D} = \dfrac{\Gamma \vdash M : B}{\Gamma \vdash \mathsf{inr}\, M : A + B}$

similar to the case above.

Case $\mathcal{D} = \dfrac{\Gamma \vdash M : A + B \qquad \Gamma, x{:}A \vdash M_1 : C \qquad \Gamma, y{:}B \vdash M_2 : C}{\Gamma \vdash \mathsf{case}\, M\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow M_1 \mid \mathsf{inr}\, y \Rightarrow M_2 : C}$

$\Gamma' \vdash \sigma \in \mathcal{R}_\Gamma$ by assumption
$\Gamma' \vdash [\sigma]M \in \mathcal{R}_{A+B}$ by i.h.

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

Subcase $\Gamma' \vdash [\sigma]M \in \{\mathbf{inl}\ N \mid \Gamma' \vdash N \in \mathcal{R}_A\}$

$[\sigma]M = \mathsf{inl}\, N$ for some $\Gamma' \vdash N \in \mathcal{R}_A$ by assumption
$\Gamma' \vdash N : A \in \mathsf{SN}$ by CR1
$\Gamma' \vdash \mathsf{inl}\, N : A + B \in \mathsf{SN}$ by definition
$\Gamma' \vdash \sigma \in \mathcal{R}_\Gamma$ by assumption
$\Gamma' \vdash [\sigma, N/x] \in \mathcal{R}_{\Gamma, x:A}$ by definition
$\Gamma' \vdash [\sigma, N/x]M_1 \in \mathcal{R}_C$ by outer i.h
$\Gamma', y{:}B \vdash y \in \mathcal{R}_B$ by definition
$\Gamma', y{:}B \vdash [\sigma, y/y] \in \mathcal{R}_{\Gamma, y:B}$ by definition
$\Gamma', y{:}B \vdash [\sigma, y/y]M_2 \in \mathcal{R}_C$ by outer i.h.
$\Gamma', y{:}B \vdash [\sigma, y/y]M_2 : C \in \mathsf{SN}$ by CR1
$\Gamma' \vdash \mathsf{case}\, (\mathsf{inl}\, N)\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow [\sigma, x/x]M_1 \mid \mathsf{inr}\, y \Rightarrow [\sigma, y/y]M_2 \longrightarrow_{\mathsf{SN}} [\sigma, N/x]M_1 : C$ 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 $[\sigma]M = \mathsf{inl}\, N$
$\Gamma' \vdash [\sigma](\mathsf{case}\, M\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow M_1 \mid \mathsf{inr}\, y \Rightarrow M_2) \in \mathcal{R}_C$ by CR3

Subcase $\Gamma' \vdash [\sigma]M \in \{\mathbf{inr}\ N \mid \Gamma' \vdash N \in \mathcal{R}_B\}$

similar to the case above.

Subcase: $\Gamma' \vdash [\sigma]M : A + B \in \mathsf{SNe}$.
$\Gamma' \vdash \sigma \in \mathcal{R}_\Gamma$ by assumption
$\Gamma', x{:}A \vdash x \in \mathcal{R}_A$ by definition
$\Gamma', y{:}B \vdash y \in \mathcal{R}_B$ by definition

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

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

8 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

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

Normal terms

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

Strong head reduction

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

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

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

9 Extension: Natural numbers

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

9.1 Semantic type $\mathcal{R}_{\mathsf{nat}}$

We define the denotation of nat as follows:

$$\Gamma \vdash M \in \mathcal{R}_{\mathsf{nat}} \quad \text{iff} \quad \Gamma \vdash M \in \overline{\{z\} \cup \{\mathsf{suc}\, M' \mid \Gamma \vdash M' \in \mathcal{R}_{\mathsf{nat}}\}}$$

9.2 Semantic type $\mathcal{R}_{\mathsf{nat}}$ is a reducibility candidate

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

Theorem 9.1. *For all types* C, $\mathcal{R}_C \in CR$.

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

Case $C = \mathsf{nat}$**.**

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

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

Subcase: $M = \mathsf{suc}\, N$ where $\Gamma \vdash N \in \mathcal{R}_{\mathsf{nat}}$. By i.h. (CR1), $\Gamma \vdash N : \mathsf{nat} \in \mathsf{SN}$. By definition of SN, $\Gamma \vdash \mathsf{suc}\, N : \mathsf{nat} \in \mathsf{SN}$.

Subcase: $\Gamma \vdash M : \mathsf{nat} \in \mathsf{SNe}$. By definition of SN, $\Gamma \vdash M : \mathsf{nat} \in \mathsf{SN}$.

Subcase: $\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : \mathsf{nat}$ and $\Gamma \vdash M' \in \mathcal{R}_{\mathsf{nat}}$.

$\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : \mathsf{nat}$ and $\Gamma \vdash M' \in \mathcal{R}_{\mathsf{nat}}$	by assumption
$\Gamma \vdash M' : \mathsf{nat} \in \mathsf{SN}$	by inner i.h.
$\Gamma \vdash M : \mathsf{nat} \in \mathsf{SN}$	by reduction $\longrightarrow_{\mathsf{SN}}$

2. *Show* CR2. If $\Gamma \vdash M : \mathsf{nat} \in \mathsf{SNe}$, then $\Gamma \vdash M \in \mathcal{R}_{\mathsf{nat}}$.
   By definition of the closure, if $\Gamma \vdash M : \mathsf{nat} \in \mathsf{SNe}$, then $\Gamma \vdash M \in \mathcal{R}_{\mathsf{nat}}$.

3. *Show* If $\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : \mathsf{nat}$ and $\Gamma \vdash M' \in \mathcal{R}_{\mathsf{nat}}$, then $\Gamma \vdash M \in \mathcal{R}_{\mathsf{nat}}$.
   By definition of the closure, if $\Gamma \vdash M \longrightarrow_{\mathsf{SN}} M' : \mathsf{nat}$ and $\Gamma \vdash M' \in \mathcal{R}_{\mathsf{nat}}$, we have $\Gamma \vdash M \in \mathcal{R}_{\mathsf{nat}}$.

□

9.3 Revisiting the fundamental lemma

We can now revisit the fundamental lemma.

Lemma 9.2 (Fundamental lemma)**.** *If* $\Gamma \vdash M : C$ *and* $\Gamma' \vdash \sigma \in \mathcal{R}_\Gamma$ *then* $\Gamma' \vdash [\sigma]M \in \mathcal{R}_C$.

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

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

$[\sigma]\mathsf{z} = \mathsf{z}$	by subst. def
$\Gamma' \vdash \mathsf{z} \in \mathcal{R}_{\mathsf{nat}}$	by definition.

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

$\Gamma' \vdash \sigma \in \mathcal{R}_\Gamma$	by assumption
$\Gamma' \vdash [\sigma]M \in \mathcal{R}_{\mathsf{nat}}$	by i.h.
$\Gamma' \vdash \mathsf{suc}\, [\sigma]M \in \mathcal{R}_{\mathsf{nat}}$	by definition
$\Gamma' \vdash [\sigma]\mathsf{suc}\, M \in \mathcal{R}_{\mathsf{nat}}$	by subst. def

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

$\Gamma' \vdash \sigma \in \mathcal{R}_\Gamma$	by assumption
$\Gamma' \vdash [\sigma]M \in \mathcal{R}_{\mathsf{nat}}$	by i.h.

We distinguish cases based on $\Gamma' \vdash [\sigma]M \in \mathcal{R}_{\mathsf{nat}}$ and prove by induction on $\Gamma' \vdash [\sigma]M \in \mathcal{R}_{\mathsf{nat}}$ that $\Gamma' \vdash [\sigma](\mathsf{rec}\ M\ \mathsf{with}\ \mathsf{f}\ \mathsf{z} \to M_z \mid \mathsf{f}\ (\mathsf{suc}\, n) \to M_s) \in \mathcal{R}_C$.

Subcase $[\sigma]M = z$.

$\Gamma', n : \mathsf{nat}, f\ n : C \vdash n \in \mathcal{R}_{\mathsf{nat}}$ by definition of SNe, $\mathcal{R}_{\mathsf{nat}}$

$\Gamma', n : \mathsf{nat}, f\ n : C \vdash f\ n \in \mathcal{R}_C$ by definition of SNe, $\mathcal{R}_{\mathsf{nat}}$

$\Gamma', n : \mathsf{nat}, f\ n : C \vdash [\sigma, n/n, f\ n/f\ n] \in \mathcal{R}_{\Gamma, n:\mathsf{nat}, f\ n:C}$ by definition

$\Gamma', n : \mathsf{nat}, f\ n : C \vdash [\sigma, n/n, f\ n/f\ n]M_s \in \mathcal{R}_C$ by outer i.h.

$\Gamma', n : \mathsf{nat}, f\ n : C \vdash [\sigma, n/n, f\ n/f\ n]M_s : C \in \mathsf{SN}$ by CR1

$\Gamma' \vdash [\sigma]M_z \in \mathcal{R}_C$ by outer i.h.

$\Gamma' \vdash \mathsf{rec}\ z\ \mathsf{with}\ f\ z \to [\sigma]M_z \mid f\ (\mathsf{suc}\, n) \to [\sigma, n/n, f\ n/f\ n]M_s \longrightarrow_{\mathsf{SN}} [\sigma]M_z : C$ 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 $[\sigma]M = z$

$\Gamma' \vdash [\sigma](\mathsf{rec}\ M\ \mathsf{with}\ f\ z \to M_z \mid f\ (\mathsf{suc}\, n) \to M_s \in \mathcal{R}_C$ by CR3.

Subcase $[\sigma]M = \mathsf{suc}\, M'$ where $\Gamma' \vdash M' \in \mathcal{R}_{\mathsf{nat}}$.

$\Gamma' \vdash M' \in \mathcal{R}_{\mathsf{nat}}$ by assumption

$\Gamma \vdash M' : \mathsf{nat} \in \mathsf{SN}$ by CR1

$\Gamma' \vdash [\sigma]M_z \in \mathcal{R}_C$ by outer i.h.

$\Gamma' \vdash [\sigma]M_z \in \mathsf{SN}$ by CR1

$\Gamma', n : \mathsf{nat}, f\ n : C \vdash [\sigma, n/n, f\ n/f\ n] \in \mathcal{R}_{\Gamma, n:\mathsf{nat}, f\ n:C}$ by definition

$\Gamma', n : \mathsf{nat}, f\ n : C \vdash [\sigma, n/n, f\ n/f\ n]M_s \in \mathcal{R}_C$ by outer i.h.

$\Gamma', n : \mathsf{nat}, f\ n : C \vdash [\sigma, n/n, f\ n/f\ n]M_s : C \in \mathsf{SN}$ by CR1

$\Gamma' \vdash \mathsf{rec}\ M'\ \mathsf{with}\ f\ z \to [\sigma]M_z \mid f\ (\mathsf{suc}\, n) \to [\sigma, n/n, f\ n/f\ n]M_s \in \mathcal{R}_C$ by inner i.h.

$\Gamma' \vdash [\sigma, M'/n, (\mathsf{rec}\ M'\ \mathsf{with}\ f\ z \to [\sigma]M_z \mid f\ (\mathsf{suc}\, n) \to [\sigma, n/n, f\ n/f\ n]M_s)/f\ n] \in \mathcal{R}_{\Gamma, n:\mathsf{nat}, f\ n:C}$ by definition

$\Gamma' \vdash [\sigma, M'/n, (\mathsf{rec}\ M'\ \mathsf{with}\ f\ z \to [\sigma]M_z \mid f\ (\mathsf{suc}\, n) \to [\sigma, n/n, f\ n/f\ n]M_s)/f\ n]M_s \in \mathcal{R}_C$ by outer i.h.

$\Gamma' \vdash \mathsf{rec}\ (\mathsf{suc}\, M')\ \mathsf{with}\ f\ z \to [\sigma]M_z \mid f\ (\mathsf{suc}\, n) \to [\sigma, n/n, f\ n/f\ n]M_s$
$\longrightarrow_{\mathsf{SN}} [\sigma, M'/n, (\mathsf{rec}\ M'\ \mathsf{with}\ f\ z \to [\sigma]M_z \mid f\ (\mathsf{suc}\, n) \to [\sigma, n/n, f\ n/f\ n]M_s)/f\ n]M_s : C$ by $\longrightarrow_{\mathsf{SN}}$

$\Gamma' \vdash [\sigma](\mathsf{rec}\ M\ \mathsf{with}\ f\ z \to M_z \mid f\ (\mathsf{suc}\, n) \to M_s) \in \mathcal{R}_C$ by CR3.

Subcase $\Gamma' \vdash [\sigma]M : \mathsf{nat} \in \mathsf{SNe}$.

$\Gamma' \vdash [\sigma]M_z \in \mathcal{R}_C$ by outer i.h.

$\Gamma' \vdash [\sigma]M_z : C \in \mathsf{SN}$ by CR1

$\Gamma', n : \mathsf{nat}, f\ n : C \vdash [\sigma, n/n, f\ n/f\ n] \in \mathcal{R}_{\Gamma, n:\mathsf{nat}, f\ n:C}$ by definition

$\Gamma', n : \mathsf{nat}, f\ n : C \vdash [\sigma, n/n, f\ n/f\ n]M_s \in \mathcal{R}_C$ by outer i.h.

$\Gamma', n : \mathsf{nat}, f\ n : C \vdash [\sigma, n/n, f\ n/f\ n]M_s : C \in \mathsf{SN}$ by CR1

$\Gamma \vdash \mathsf{rec}\ [\sigma]M\ \mathsf{with}\ f\ z \to [\sigma]M_z \mid f\ (\mathsf{suc}\, n) \to [\sigma, n/n, f\ n/f\ n]M_s : C \in \mathsf{SNe}$ by SNe

$\Gamma' \vdash [\sigma](\mathsf{rec}\ M\ \mathsf{with}\ f\ z \to M_z \mid f\ (\mathsf{suc}\, n) \to M_s) : C \in \mathsf{SNe}$ by subst. def.

$\Gamma' \vdash [\sigma](\mathsf{rec}\ M\ \mathsf{with}\ f\ z \to M_z \mid f\ (\mathsf{suc}\, n) \to M_s) \in \mathcal{R}_C$ by CR2.

Subcase $\Gamma' \vdash [\sigma]M \longrightarrow_{\mathsf{SN}} M' : \mathsf{nat}$ and $\Gamma' \vdash M' \in \mathcal{R}_{\mathsf{nat}}$.

$\Gamma' \vdash [\sigma]M \longrightarrow_{\mathsf{SN}} M' : \mathsf{nat}$ and $\Gamma' \vdash M' \in \mathcal{R}_{\mathsf{nat}}$ by assumption.

$\Gamma' \vdash \mathsf{rec}\ M'\ \mathsf{with}\ f\ z \to [\sigma]M_z \mid f\ (\mathsf{suc}\, n) \to [\sigma, n/n, f\ n/f\ n]M_s \in \mathcal{R}_C$ by inner i.h.

$\Gamma' \vdash \mathsf{rec}\ [\sigma]M\ \mathsf{with}\ f\ z \to [\sigma]M_z \mid f\ (\mathsf{suc}\, n) \to [\sigma, n/n, f\ n/f\ n]M_s$
$\longrightarrow_{\mathsf{SN}} \mathsf{rec}\ M'\ \mathsf{with}\ f\ z \to [\sigma]M_z \mid f\ (\mathsf{suc}\, n) \to [\sigma, n/n, f\ n/f\ n]M_s : C$ by $\longrightarrow_{\mathsf{SN}}$

$\Gamma' \vdash [\sigma](\mathsf{rec}\ M\ \mathsf{with}\ f\ z \to M_z \mid f\ (\mathsf{suc}\, n) \to M_s) \in \mathcal{R}_C$ by CR3.

□

References

Karl Crary. Logical relations and a case study in equivalence checking. In Bejamin C. Pierce, editor, *Advanced Topics in Types and Programming Languages*. The MIT Press, 2005.

J. Y Girard. *Interprtation fonctionnelle et elimination des coupures de l'arithmtique d'ordre suprieur*. These d'tat, Universit de Paris 7, 1972.

Healfdene Goguen. Typed operational semantics. In Mariangiola Dezani-Ciancaglini and Gordon Plotkin, editors, *2nd International Conference on Typed Lambda Calculi and Applications (TLCA'95)*, Lecture Notes in Computer Science (LNCS 902), pages 186–200. Springer, 1995. ISBN 978-3-540-49178-1. doi: 10.1007/BFb0014053. URL `https://doi.org/10.1007/BFb0014053`.

Robert Harper and Frank Pfenning. On equivalence and canonical forms in the LF type theory. *ACM Transactions on Computational Logic*, 6(1):61–101, 2005.

Felix Joachimski and Ralph Matthes. Short proofs of normalization for the simply- typed λ-calculus, permutative conversions and Gödel's T. *Archive for Mathematical Logic*, 42 (1):59–87, Jan 2003. ISSN 1432-0665. doi: 10.1007/s00153-002-0156-9. URL `https://doi.org/10.1007/s00153-002-0156-9`.

Z. Luo. *An Extended Calculus of Constructions*. PhD thesis, Department of Computer Science, University of Edinburgh, 1990. CST-65-90/ECS-LFCS-90-118.

William Tait. Intensional Interpretations of Functionals of Finite Type I. *J. Symb. Log.*, 32(2):198–212, 1967.

Femke van Raamsdonk and Paula Severi. On normalisation. Technical Report 95/20, Technische Universiteit Eindhoven, 1995.

Kevin Watkins, Iliano Cervesato, Frank Pfenning, and David Walker. A concurrent logical framework I: Judgments and properties. Technical Report CMU-CS-02-101, Department of Computer Science, Carnegie Mellon University, 2002.