A Proof of the Strong Normalization of the Simply-Typed Lambda Calculus

Thiago F Cesar

This proof uses the reducibility technique and is based on the one given in Proofs and Types, by Jean-Yves Girard. Only a small number of changes was made.

1 Basic Definitions

Definition 1.1 (Lambda terms) *Let $\mathcal{C}$ be an infinite countable set of constants and $\mathcal{X}$ an infinite countable set of variables. We define the terms of the simply-typed lambda calculus by the grammar*

$$M, N ::= x \in \mathcal{X} \mid c \in \mathcal{C} \mid M\ N \mid \lambda x.M$$

Reduction on the lambda-calculus is given by the rules

$$\frac{M \longrightarrow M'}{MN \longrightarrow M'N}\ \mathsf{appL} \qquad \frac{N \longrightarrow N'}{MN \longrightarrow MN'}\ \mathsf{appR}$$

$$\frac{M \longrightarrow M'}{\lambda x.M \longrightarrow \lambda x.M'}\ \xi \qquad \frac{}{(\lambda x.M)N \longrightarrow M(N/x)}\ \beta$$

Definition 1.2 (Simple types) *Let $\mathcal{B}$ be an infinite countable set of base types. We define the grammar of simple types by*

$$A, B ::= p \in \mathcal{B} \mid A \to B$$

A context Γ is a set of or pairs $x : A$, where x is a variable and A is a type, such that any variable can only appear once. A signature Σ is a set of pairs $c : A$, where c is a constant, A is a type and every constant can only appear once.

If M is a lambda term, we define the type judgment $\Sigma; \Gamma \vdash M : A$ inductively by

$$\frac{x : A \in \Gamma}{\Sigma; \Gamma \vdash x : A}\ \mathsf{ax} \qquad \frac{\Sigma; \Gamma, x : A \vdash M : B}{\Sigma; \Gamma \vdash \lambda x.M : A \to B}\ \mathsf{abs}$$

$$\frac{c : A \in \Sigma}{\Sigma; \Gamma \vdash c : A}\ \mathsf{cons} \qquad \frac{\Sigma; \Gamma \vdash M : A \to B \qquad \Sigma; \Gamma \vdash N : A}{\Sigma; \Gamma \vdash MN : B}\ \mathsf{app}$$

We assume an underlying signature and we write $\Gamma \vdash M : A$ for simplification reasons.

The following lemmas are standard and will be used on the strong normalization proof. Their proofs are omitted.

Lemma 1.1 *If $M \longrightarrow^* M'$ and $N \longrightarrow^* N'$ then $M(N/x) \longrightarrow^* M'(N'/x)$.*

Lemma 1.2 *If M is a term, we define its reduction tree as follows. A node is a term N with $M \longrightarrow^* N$ and there is an edge from N to N' when $N \longrightarrow N'$. Then its reduction tree is finite iff M is SN.*

Lemma 1.3 *Let MN be a term and $MN \longrightarrow^* Q$ a reduction in which β is never applied at the outer application. Then $Q = M'N'$ with $M \longrightarrow^* M'$ and $N \longrightarrow^* N'$.*

2 Strong Normalization

Definition 2.1 *If A is a type, we define $[\![A]\!]$ by induction on its structure as*

- *if $A = p \in \mathcal{B}$, then $[\![p]\!] = \mathit{SN}$*
- *if $A = B \to C$, then $[\![B \to C]\!] = \{M \in \mathit{SN} \mid \forall N \in [\![B]\!], MN \in [\![C]\!]\}$*

where SN denotes the set of strongly normalizing terms.

Lemma 2.1 *Let A be any type. If $M \longrightarrow M'$, then $M \in [\![A]\!]$ implies $M' \in [\![A]\!]$.*

Proof. By induction on the structure of A. For the base case, note that if M is SN then M' is also SN.

For the induction step we have $A = B \to C$. First note that the previous observation also holds, thus M' is SN. It is left to prove that for all $N \in [\![B]\!]$ we have $M'N \in [\![C]\!]$. But $MN \longrightarrow M'N$, where $MN \in [\![C]\!]$ and C is structurally smaller then A. We thus conclude by the induction hypothesis that $M'N \in [\![C]\!]$. ■

Proposition 2.1 *Let A be a type and let M be a variable, constant or of the form M_1M_2. If for all N with $M \longrightarrow N$ we have $N \in [\![A]\!]$ then $M \in [\![A]\!]$.*

Proof. By induction on the structure of A. For the base case $A = p$, note that as every reduction path goes through a SN term, then M must also be SN.

For the induction step we have $A = B \to C$. The previous remark also holds, so we are left to prove that for all $Q \in [\![B]\!]$, $MQ \in [\![C]\!]$. As Q is SN, then by Lemma 1.2 its reduction tree is finite. We show the result by induction on its height. As we now have nested inductions, we let IH 1 be the induction hypothesis of the outer induction and IH 2 the one of the inner one.

- For the base case, Q is in normal form and thus every reduction $MQ \longrightarrow Q'$ takes place on M. We thus have $Q' = NQ$ with $M \longrightarrow N$. By hypothesis, $N \in [\![B \to C]\!]$, and thus $NQ \in [\![C]\!]$. Therefore, every Q' with $MQ \longrightarrow Q'$ is in $[\![C]\!]$. As C is structurally smaller then A, we apply IH 1 to find $MQ \in [\![C]\!]$.
- For the induction step, we consider all the reductions $MQ \longrightarrow N$ and we do a case analysis on the rules that can be applied on the head, which are only appL and appR. We show that each N is in $[\![C]\!]$.

  If the rule is appR we have $MQ \longrightarrow MQ'$ with $Q \longrightarrow Q'$. As the tree of Q' has a lower height, we apply IH 2 to conclude $MQ' \in [\![C]\!]$.

  If the rule is appL we have $MQ \longrightarrow NQ$ with $M \longrightarrow N$. By hypothesis, $N \in [\![B \to C]\!]$, and thus $NQ \in [\![C]\!]$.

We have show that for all N with $MQ \longrightarrow N$, $N \in [\![C]\!]$. As C is structurally smaller then A, by IH 1 we get $MQ \in [\![C]\!]$.

■

Corollary 2.1 *Let A be any type. If M is a variable or constant then $M \in [\![A]\!]$.*

Proof. As M is normal, there is no N with $M \longrightarrow N$, thus the hypothesis of Proposition 2.1 is verified trivially. ■

Lemma 2.2 *If $M \in [\![A]\!]$, $N \in [\![B]\!]$ and $M(N/x) \in [\![A]\!]$ then $(\lambda x.M)N \in$ SN.*

Proof. First note that no infinite reduction can happen with only appL and appR on the outer application, as this would imply that either N or M is not SN.

Now let $(\lambda x.M)N \longrightarrow M_1 \longrightarrow M_2 \longrightarrow \ldots$ be a reduction in which β is applied to the outer application at some point. We write $(\lambda x.M)N \longrightarrow^* (\lambda x.M')N' \longrightarrow_\beta M'(N'/x) \longrightarrow^* \ldots$ where β does not occur in the outer application in $(\lambda x.M)N \longrightarrow^* (\lambda x.M')N'$.

Thus, by Lemma 1.3 we have $M \longrightarrow^* M'$ and $N \longrightarrow^* N'$. By Lemma 1.1, $M(N/x) \longrightarrow^* M'(N'/x)$, and thus $M'(N'/x) \in [\![A]\!]$ by Lemma 2.1. In particular, $M'(N'/x) \in$ SN and thus $(\lambda x.M)N \longrightarrow^* (\lambda x.M')N' \longrightarrow M'(N'/x) \longrightarrow^* \ldots$ is finite. ■

Proposition 2.2 *If $M \in [\![A]\!]$, $N \in [\![B]\!]$ and $M(N/x) \in [\![A]\!]$ then $(\lambda x.M)N \in [\![A]\!]$.*

Proof. As $(\lambda x.M)N$ is SN, by Lemma 1.2 its reduction tree is finite. We show $(\lambda x.M)N \in [\![A]\!]$ by induction on the height of its reduction tree. For the base case of height zero, as $(\lambda x.M)N$ is a redex then we can derive absurdity, from which the conclusion follows trivially.

For the induction step, we consider all the possible Q with $(\lambda x.M)N \longrightarrow Q$ and we do a case analysis on the rule applied at the head

- **AppL** : Then $Q = (\lambda x.M')N$ with $\lambda x.M \longrightarrow \lambda x.M'$ and $M \longrightarrow M'$. Using Lemma 1.1, this also implies $M(N/x) \longrightarrow^* M'(N/x)$. As $M, M(N/x) \in [\![A]\!]$, by Lemma 2.1, we have $M', M'(N/x) \in [\![A]\!]$. As the reduction tree of $(\lambda x.M')N$ is smaller, we can apply the induction hypothesis and conclude $(\lambda x.M')N \in [\![A]\!]$.
- **AppR** : Then $Q = (\lambda x.M)N'$ with $N \longrightarrow N'$. Using Lemma 1.1, this also implies $M(N/x) \longrightarrow^* M(N'/x)$. By Lemma 2.1, we have $N' \in [\![B]\!]$ and $M(N'/x) \in [\![A]\!]$. As the reduction tree of $(\lambda x.M)N'$ is smaller, we can apply the induction hypothesis and conclude $(\lambda x.M)N' \in [\![A]\!]$.
- $\boldsymbol{\beta}$: Then $Q = M(N/x)$, which by hypotheses is in $[\![A]\!]$.

We have shown that for all Q with $(\lambda x.M)N \longrightarrow Q$ we have $Q \in [\![A]\!]$. Hence, by Proposition 2.1 we have $(\lambda x.M)N \in [\![A]\!]$. ■

Theorem 2.1 *Let M be a term with $\Gamma \vdash M : A$ and let σ be a substitution with dom $\sigma = \{x \mid x : A_x \in \Gamma\}$ and with $\sigma(x) \in [\![A_x]\!]$. Then $\sigma(M) \in [\![A]\!]$.*

Proof. By induction on the type derivation.

Rule ax : The derivation ends with

$$\frac{x : A \in \Gamma}{\Gamma \vdash x : A}\ \mathsf{ax}$$

Thus $M = x$ and $\sigma(x) \in [\![A]\!]$ by hypothesis.

Rule cons : The derivation ends with

$$\frac{c : A \in \Sigma}{\Gamma \vdash c : A}\ \mathsf{cons}$$

Thus $M = c$ and $\sigma(c) = c$. By Corollary 2.1, $c \in [\![A]\!]$.

Rule app : The derivation ends with

$$\frac{\Gamma \vdash M : B \to A \qquad \Gamma \vdash N : B}{\Gamma \vdash MN : A}\ \mathsf{app}$$

By the induction hypothesis, $\sigma(M) \in [\![B \to A]\!]$ and $\sigma(N) \in [\![B]\!]$. By definition of $[\![B \to A]\!]$, we get $\sigma(M)\sigma(N) \in [\![A]\!]$, and thus $\sigma(MN) \in [\![A]\!]$.

Rule abs : The derivation ends with

$$\frac{\Gamma, x : B \vdash M : A}{\Gamma \vdash \lambda x.M : B \to A}\ \mathsf{abs}$$

For $N \in [\![B]\!]$, we need to show that $(\lambda x.\sigma(M))N \in [\![A]\!]$.

Consider the substitution $\sigma' := (\sigma; x \mapsto x)$. As x is a variable, then $x \in [\![B]\!]$ and thus we can apply the induction hypothesis on $\Gamma, x : B \vdash M : A$. We thus have $\sigma(M) = \sigma'(M) \in [\![A]\!]$.

Now consider the substitution $\tau := (\sigma; x \mapsto N)$. As $N \in [\![B]\!]$, we can apply the induction hypothesis once again and find that $\tau(M) = \sigma(M)(N/x) \in [\![A]\!]$.

We have all the hypothesis to apply Lemma 2.2, from which we get $(\lambda x.\sigma(M))N \in [\![A]\!]$. ∎

Corollary 2.2 *Let M be a term with $\Gamma \vdash M : A$, then $M \in SN$.*

Proof. Let $\sigma := (x_i \mapsto x_i)_{x_i : A_i \in \Gamma}$. As each x_i is a variable, then $x_i \in [\![A_i]\!]$ and we can apply the previous theorem. Thus, $M = \sigma(M) \in [\![A]\!]$, and in particular we deduce $M \in$ SN. ∎