LMSE 1

Logische Methoden des Software Engineerings
Vertiefungsmodul 1

Prof. Dr. Jakob Rehof

Lehrstuhl XIV, Software Engineering

Strong normalization (SN)

- *All* reduction sequences are finite
- Not needed for most uses in proof theory (e.g., WN suffices for consistency)
- But important characterization of programs under various type disciplines
- Important uses in rewriting theory (e.g., Newman‘s Lemma)
- Often much harder to prove than WN

Strong normalization

- Method: Saturated sets (candidats de reducibilité)
- Invented by Tait (1967) for simple types
- Generalized to System **F** by Girard (1972)
- One of the most ingenious proofs in type theory

[104] W.W. Tait. Intensional interpretations of functionals of finite type I. *Journal of Symbolic Logic*, 32(2):190–212, 1967.

[44] J.-Y. Girard. Interprétation fonctionelle et élimination des coupures dans l'arithmétique d'ordre supérieur. Thèse d'État, Université Paris VII, 1972.

Interpretation of types in subsets of SN

4.4.1. Definition.

(i) $\mathrm{SN}_\beta = \{M \in \Lambda \mid M \text{ is strongly normalizing }\}$.

(ii) For $A, B \subseteq \Lambda$, define $A \to B = \{F \in \Lambda \mid \forall a \in A : F\ a \in B\}$.

(iii) For every simple type σ, define $[\![\sigma]\!] \subseteq \Lambda$ by:

$$\begin{aligned} [\![\alpha]\!] &= \mathrm{SN}_\beta \\ [\![\sigma \to \tau]\!] &= [\![\sigma]\!] \to [\![\tau]\!] \end{aligned}$$

Saturated sets

4.4.2. DEFINITION.

(i) A set $X \subseteq \mathrm{SN}_\beta$ is *saturated* if

1. For all $n \geq 0$ and $M_1, \ldots M_n \in \mathrm{SN}_\beta$:

$$x\, M_1 \ldots M_n \in X$$

2. For all $n \geq 1$ and $M_1, \ldots, M_n \in \mathrm{SN}_\beta$:

$$M_0\{x := M_1\}\, M_2 \ldots M_n \in X \Rightarrow (\lambda x.M_0)\, M_1\, M_2 \ldots M_n \in X$$

(ii) $\mathbb{S} = \{X \subseteq \Lambda \mid X \text{ is saturated } \}$.

Types are saturated sets under the interpretation

4.4.3. LEMMA.

(i) $\mathrm{SN}_\beta \in \mathbb{S}$;

(ii) $A, B \in \mathbb{S} \Rightarrow A \to B \in \mathbb{S}$;

(iii) $\sigma \in \Pi \Rightarrow [\![\sigma]\!] \in \mathbb{S}$.

Valuations, satisfaction, entailment

4.4.4. DEFINITION.

(i) a *valuation* is a map $\rho : V \to \Lambda$, where V is the set of term variables. The valuation $\rho(x := N)$ is defined by

$$\rho(x := N)(y) = \begin{cases} N & \text{if } x \equiv y \\ \rho(y) & \text{otherwise} \end{cases}$$

(ii) Let ρ be a valuation. Then $[\![M]\!]_\rho = M\{x_1 := \rho(x_1), \ldots, x_n := \rho(x_n)\}$, where $\mathrm{FV}(M) = \{x_1, \ldots, x_n\}$.

(iii) Let ρ be a valuation. Then $\rho \models M : \sigma$ iff $[\![M]\!]_\rho \in [\![\sigma]\!]$. Also, $\rho \models \Gamma$ iff $\rho(x) \in [\![\sigma]\!]$ for all $x : \sigma \in \Gamma$.

(iv) $\Gamma \models M : \sigma$ iff $\forall \rho : \rho \models \Gamma \Rightarrow \rho \models M : \sigma$.

Soundness

4.4.5. PROPOSITION (Soundness). $\Gamma \vdash M : \sigma \Rightarrow \Gamma \models M : \sigma$.

PROOF. By induction on the derivation of $\Gamma \vdash M : \sigma$.

1. The derivation is

$$\Gamma \vdash x : \sigma \quad x : \sigma \in \Gamma$$

If $\rho \models \Gamma$, then $[\![x]\!]_\rho = \rho(x) \in [\![\sigma]\!]$.

2. The derivation ends in

$$\frac{\Gamma \vdash M : \sigma \to \tau \quad \Gamma \vdash N : \sigma}{\Gamma \vdash M\ N : \tau}$$

Suppose $\rho \models \Gamma$. By the induction hypothesis $\Gamma \models M : \sigma \to \tau$ and $\Gamma \models N : \sigma$, so $\rho \models M : \sigma \to \tau$ and $\rho \models N : \sigma$, i.e., $[\![M]\!]_\rho \in [\![\sigma]\!] \to [\![\tau]\!]$ and $[\![N]\!]_\rho \in [\![\sigma]\!]$. Then $[\![M\ N]\!]_\rho = [\![M]\!]_\rho\ [\![N]\!]_\rho \in [\![\tau]\!]$, as required.

Soundness

4.4.5. Proposition (Soundness). $\Gamma \vdash M : \sigma \Rightarrow \Gamma \models M : \sigma$.

3. The derivation ends in

$$\frac{\Gamma, x : \sigma \vdash M : \tau}{\Gamma \vdash \lambda x.M : \sigma \to \tau}$$

Suppose $\rho \models \Gamma$. Also, suppose $N \in [\![\sigma]\!]$. Then $\rho(x := N) \models \Gamma, x : \sigma$. By the induction hypothesis $\Gamma, x : \sigma \models M : \tau$, so $\rho(x := N) \models M : \tau$, i.e., $[\![M]\!]_{\rho(x:=N)} \in [\![\tau]\!]$. Now,

$$\begin{array}{rcl} [\![\lambda x.M]\!]_\rho \, N & \equiv & (\lambda x.M) \, \{y_1 := \rho(y_1), \ldots, y_n := \rho(y_n)\} N \\ & \to_\beta & M\{y_1 := \rho(y_1), \ldots, y_n := \rho(y_n), x := N\} \\ & \equiv & [\![M]\!]_{\rho(x:=N)} \end{array}$$

Since $N \in [\![\sigma]\!] \subseteq \mathrm{SN}_\beta$ and $[\![M]\!]_{\rho(x:=N)} \in [\![\tau]\!] \in \mathbb{S}$, it follows that $[\![\lambda x.M]\!]_\rho \, N \in [\![\tau]\!]$. Hence $[\![\lambda x.M]\!]_\rho \in [\![\sigma \to \tau]\!]$. □

SN Q.E.D.

4.4.6. THEOREM. $\Gamma \vdash M : \sigma \Rightarrow M \in \mathrm{SN}_\beta$.

PROOF. If $\Gamma \vdash M : \sigma$, then $\Gamma \models M : \sigma$. For each $x : \tau \in \Gamma$, let $\rho(x) = x$. Then $x \in [\![\tau]\!]$ holds since $[\![\tau]\!] \in \mathbb{S}$. Then $\rho \models \Gamma$, and we have $M = [\![M]\!]_\rho \in [\![\sigma]\!] \subseteq \mathrm{SN}_\beta$. □

Soundness

Lemma 4.4.3

Proof uses stronger logical methods

4.4.3. LEMMA.

(i) $\mathrm{SN}_\beta \in \mathbb{S}$;

(ii) $A, B \in \mathbb{S} \Rightarrow A \to B \in \mathbb{S}$;

(iii) $\sigma \in \Pi \Rightarrow [\![\sigma]\!] \in \mathbb{S}$.

Quantification over sets