

LMSE

Logische Methoden des Software
Engineerings

Prof. Dr. Jakob Rehof
Lehrstuhl XIV, Software
Engineering

Aufgaben

1. Zeigen Sie, dass jeder Typ nur linear (in der Typlänge) viele Teiltypen hat.
2. Beweisen Sie Lemma 4.4.3 i) und ii)
3. Bereiten Sie den Beweis von Proposition 4.4.5 so vor, dass Sie ihn in der Übung vorstellen können.

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 fonctionnelle 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) $\text{SN}_\beta = \{M \in \Lambda \mid M \text{ is strongly normalizing}\}$.
- (ii) For $A, B \subseteq \Lambda$, define $A \rightarrow B = \{F \in \Lambda \mid \forall a \in A : F a \in B\}$.
- (iii) For every simple type σ , define $\llbracket \sigma \rrbracket \subseteq \Lambda$ by:

$$\begin{aligned}\llbracket \alpha \rrbracket &= \text{SN}_\beta \\ \llbracket \sigma \rightarrow \tau \rrbracket &= \llbracket \sigma \rrbracket \rightarrow \llbracket \tau \rrbracket\end{aligned}$$

Saturated sets

4.4.2. DEFINITION.

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

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

$$x M_1 \dots M_n \in X$$

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

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

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

Types are saturated sets under the interpretation

4.4.3. LEMMA.

- (i) $SN_{\beta} \in \mathcal{S}$;
- (ii) $A, B \in \mathcal{S} \Rightarrow A \rightarrow B \in \mathcal{S}$;
- (iii) $\sigma \in \Pi \Rightarrow \llbracket \sigma \rrbracket \in \mathcal{S}$.

Valuations, satisfaction, entailment

4.4.4. DEFINITION.

- (i) a *valuation* is a map $\rho : V \rightarrow \Lambda$, 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 $\llbracket M \rrbracket_\rho = M\{x_1 := \rho(x_1), \dots, x_n := \rho(x_n)\}$, where $\text{FV}(M) = \{x_1, \dots, x_n\}$.
- (iii) Let ρ be a valuation. Then $\rho \models M : \sigma$ iff $\llbracket M \rrbracket_\rho \in \llbracket \sigma \rrbracket$. Also, $\rho \models \Gamma$ iff $\rho(x) \in \llbracket \sigma \rrbracket$ 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 $\llbracket x \rrbracket_\rho = \rho(x) \in \llbracket \sigma \rrbracket$.

2. The derivation ends in

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

Suppose $\rho \models \Gamma$. By the induction hypothesis $\Gamma \models M : \sigma \rightarrow \tau$ and $\Gamma \models N : \sigma$, so $\rho \models M : \sigma \rightarrow \tau$ and $\rho \models N : \sigma$, i.e., $\llbracket M \rrbracket_\rho \in \llbracket \sigma \rrbracket \rightarrow \llbracket \tau \rrbracket$ and $\llbracket N \rrbracket_\rho \in \llbracket \sigma \rrbracket$. Then $\llbracket M N \rrbracket_\rho = \llbracket M \rrbracket_\rho \llbracket N \rrbracket_\rho \in \llbracket \tau \rrbracket$, as required.

Soundness

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

3. The derivation ends in

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

Suppose $\rho \models \Gamma$. Also, suppose $N \in \llbracket \sigma \rrbracket$. Then $\rho(x := N) \models \Gamma, x : \sigma$. By the induction hypothesis $\Gamma, x : \sigma \vdash M : \tau$, so $\rho(x := N) \models M : \tau$, i.e., $\llbracket M \rrbracket_{\rho(x:=N)} \in \llbracket \tau \rrbracket$. Now,

$$\begin{aligned} \llbracket \lambda x.M \rrbracket_{\rho} N &\equiv (\lambda x.M) \{y_1 := \rho(y_1), \dots, y_n := \rho(y_n)\} N \\ &\rightarrow_{\beta} M \{y_1 := \rho(y_1), \dots, y_n := \rho(y_n), x := N\} \\ &\equiv \llbracket M \rrbracket_{\rho(x:=N)} \end{aligned}$$

Since $N \in \llbracket \sigma \rrbracket \subseteq \text{SN}_{\beta}$ and $\llbracket M \rrbracket_{\rho(x:=N)} \in \llbracket \tau \rrbracket \in \mathbb{S}$, it follows that $\llbracket \lambda x.M \rrbracket_{\rho} N \in \llbracket \tau \rrbracket$. Hence $\llbracket \lambda x.M \rrbracket_{\rho} \in \llbracket \sigma \rightarrow \tau \rrbracket$. \square

SN Q.E.D.

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

PROOF. If $\Gamma \vdash M : \sigma$, then $\Gamma \models M : \sigma$. For each $x : \tau \in \Gamma$, let $\rho(x) = x$. Then $x \in \llbracket \tau \rrbracket$ holds since $\llbracket \tau \rrbracket \in \mathbb{S}$. Then $\rho \models \Gamma$, and we have $M = \llbracket M \rrbracket_\rho \in \llbracket \sigma \rrbracket \subseteq \text{SN}_\beta$. \square

Soundness

Lemma 4.4.3

Proof uses stronger logical methods

4.4.3. LEMMA.

- (i) $SN_\beta \in \mathcal{S}$;
- (ii) $A, B \in \mathcal{S} \Rightarrow A \rightarrow B \in \mathcal{S}$;
- (iii) $\sigma \in \Pi \Rightarrow \llbracket \sigma \rrbracket \in \mathcal{S}$.

Quantification over sets