Prof. Martin Hofmann
Dr. Ulrich Schöpp
Stephan Barth

Ludwig-Maximilians-Universität München
Institut für Informatik
SS 2015

Übungen zur Vorlesung
Formale Spezifikation und Verifikation

Blatt 10

Notation. Im Folgenden wird die benötigte Notation aus der Vorlesung zusammengefasst.

Erweiterte Typen sind Typen, in denen auch Variablen vorkommen können.

$$\begin{aligned} \tau_1, \tau_2 &::= \texttt{int} \mid \texttt{bool} \mid \tau_1 \to \tau_2 \mid \alpha \\ \alpha &::= \text{Typvariablen} \end{aligned}$$

Wir schreiben α, β, γ für Typvariablen und τ für erweiterte Typen.

Eine *Substitution* θ ist eine Abbildung, die endlich viele Typvariablen auf erweiterte Typen abbildet. Schreibe $[\alpha_1 \mapsto \tau_1, \dots, \alpha_n \mapsto \tau_n]$ für die Substitution, die α_i auf τ_i abbildet, für $i = 1, \dots, n$. Schreibe $\varnothing$ für die leere Substitution.

Schreibe $\theta[\alpha \mapsto \tau]$ für die Substituiton, die α auf τ abbildet und die alle anderen Typvariablen genau wie θ abbildet.

Schreibe $\tau[\theta]$ für den erweiterten Typ, der aus τ entsteht, wenn man die Abbildung θ als Umbenennung auffasst und diese auf auf die Variablen in τ anwendet. Formal ist $\tau[\theta]$ durch Induktion über τ definiert:

$$\begin{aligned} \texttt{int}[\theta] &= \texttt{int} \\ \texttt{bool}[\theta] &= \texttt{bool} \\ (\tau_1 \to \tau_2)[\theta] &= \tau_1[\theta] \to \tau_2[\theta] \\ \alpha[\theta] &= \begin{cases} \tau & \text{wenn } \theta \text{ die Variable } \alpha \text{ auf } \tau \text{ abbildet,} \\ \alpha & \text{wenn } \theta \text{ für die Variable } \alpha \text{ nicht definiert ist.} \end{cases} \end{aligned}$$

Aufgabe 10-1 Seien θ_1 und θ_2 Substitutionen. Dann gibt es eine Substitution $\theta_1;\theta_2$, so dass $\tau[\theta_1;\theta_2] = \tau[\theta_1][\theta_2]$ für alle erweiterten Typen τ gilt.

a) Geben Sie allgemein eine konkrete Definition der Substitution von $\theta_1;\theta_2$ an. Also: Welche Typvariablen werden von $\theta_1;\theta_2$ auf welche erweiterten Typen abgebildet?

b) Geben Sie die Substitution $[\gamma_1 \mapsto \beta, \alpha \mapsto (\beta \to \gamma_2)];[\gamma_2 \mapsto (\gamma_1 \to \beta)]$ an.

Aufgabe 10-2 Finden Sie Substitutionen gemäß der Spezifikation der Unifikation.

a) $\mathcal{U}(\alpha \to \beta, (\texttt{int} \to \texttt{bool}) \to \alpha)$

b) $\mathcal{U}(\alpha \to \beta, \alpha)$

c) $\mathcal{U}((\alpha \to \gamma) \to \beta, \beta \to (\gamma \to \alpha))$

Hinweis: Es gelten folgende Gleichungen, mit denen die Substitutionen berechnet werden können.

$$\begin{aligned}
\mathcal{U}(\texttt{int}, \texttt{int}) &= \varnothing \\
\mathcal{U}(\texttt{bool}, \texttt{bool}) &= \varnothing \\
\mathcal{U}(\alpha, \alpha) &= \varnothing \\
\mathcal{U}(\alpha, \tau) &= [\alpha \mapsto \tau] \text{ wenn } \alpha \text{ in } \tau \text{ nicht vorkommt} \\
\mathcal{U}(\tau, \alpha) &= [\alpha \mapsto \tau] \text{ wenn } \alpha \text{ in } \tau \text{ nicht vorkommt} \\
\mathcal{U}(\tau_1 \to \tau_2, \tau_1' \to \tau_2') &= \theta_1; \theta_2 \text{ wenn } \mathcal{U}(\tau_1, \tau_1') = \theta_1 \neq \text{“fail” und} \\
&\qquad\qquad \mathcal{U}(\tau_2[\theta_1], \tau_2'[\theta_1]) = \theta_2 \neq \text{“fail”} \\
\mathcal{U}(\tau_1, \tau_2) &= \text{“fail” sonst}
\end{aligned}$$

Aufgabe 10-3 Führen Sie die Typinferenz für den Term $\texttt{fn}\ f \Rightarrow \texttt{fn}\ x \Rightarrow x\ (f\ x)$ aus, d.h. berechnen Sie

$$\mathcal{W}(\varnothing, (\texttt{fn}\ f \Rightarrow \texttt{fn}\ x \Rightarrow x\ (f\ x)))\ .$$

Verwenden Sie zusätzlich zu den bereits in der Vorlesung angegebenen Definitionsregeln folgende Regel (App) für Funktionsapplikation.

$$\text{(App)}\ \frac{\mathcal{W}(\Gamma, e_0) = (\theta_0, \tau_0) \qquad \mathcal{W}(\Gamma[\theta_0], e_1) = (\theta_1, \tau_1) \qquad \theta_2 = \mathcal{U}(\tau_0[\theta_1], \tau_1 \to \gamma) \qquad \gamma \text{ frisch}}{\mathcal{W}(\Gamma, e_0\ e_1) = (\theta_0; \theta_1; \theta_2, \gamma[\theta_2])}$$

Aufgabe 10-4 Welche der folgenden Typurteile sind im Typsystem mit Annotationen für die Kontrollflussanalyse korrekt?

a) $\texttt{fun}_X\ f\ x \Rightarrow x\ (\texttt{fn}_Y\ y \Rightarrow f\ x\ y) \colon ((\alpha \xrightarrow{\{X\}} \alpha) \xrightarrow{\{Z\}} (\alpha \xrightarrow{\{Y\}} \alpha)) \xrightarrow{\{X\}} (\alpha \xrightarrow{\{Y\}} \alpha)$

b) $\texttt{fun}_X\ f\ x \Rightarrow x\ (\texttt{fn}_Y\ y \Rightarrow f\ x\ y) \colon ((\alpha \xrightarrow{\{Y\}} \alpha) \xrightarrow{\{Z\}} (\alpha \xrightarrow{\{Y\}} \alpha)) \xrightarrow{\{X\}} (\alpha \xrightarrow{\{Y\}} \alpha)$

c) $\texttt{fun}_X\ f\ x \Rightarrow x\ (\texttt{fn}_Y\ y \Rightarrow f\ x\ y) \colon ((\alpha \xrightarrow{\{Y\}} \alpha) \xrightarrow{\{V\}} (\alpha \xrightarrow{\{Z\}} \alpha)) \xrightarrow{\{X\}} (\alpha \xrightarrow{\{Z\}} \alpha)$

d) $\texttt{fun}_X\ f\ x \Rightarrow x\ (\texttt{fn}_Y\ y \Rightarrow f\ x\ y) \colon ((\alpha \xrightarrow{\{X,Y\}} \alpha) \xrightarrow{\{X,V\}} (\alpha \xrightarrow{\{Z\}} \alpha)) \xrightarrow{\{X\}} (\alpha \xrightarrow{\{X,Z\}} \alpha)$

Als Hilfestellung ist eine Herleitung im einfachen Typsystem in Abbildung 1 bereits gegeben.

$$
\text{(Fun)}\;\dfrac{
\text{(App)}\;\dfrac{
\text{(Var)}\;\dfrac{\Gamma(x) = ((\alpha \to \alpha) \to (\alpha \to \alpha))}{\Gamma \vdash x\colon (\alpha \to \alpha) \to (\alpha \to \alpha)}
\qquad
\text{(Fn)}\;\dfrac{
\text{(App)}\;\dfrac{
\text{(App)}\;\dfrac{
\text{(Var)}\;\dfrac{\Delta(f) = ((\alpha \to \alpha) \to (\alpha \to \alpha)) \to (\alpha \to \alpha)}{\Delta \vdash f\colon ((\alpha \to \alpha) \to (\alpha \to \alpha)) \to (\alpha \to \alpha)}
\quad
\text{(Var)}\;\dfrac{\Delta(x) = (\alpha \to \alpha) \to (\alpha \to \alpha)}{\Delta \vdash x\colon (\alpha \to \alpha) \to (\alpha \to \alpha)}
}{\Delta \vdash f\ x\colon \alpha \to \alpha}
\quad
\text{(Var)}\;\dfrac{\Delta(y) = \alpha}{\Delta \vdash y\colon \alpha}
}{\Delta \vdash f\ x\ y\colon \alpha}
}{\Gamma \vdash \texttt{fn}_Y\ y \Rightarrow f\ x\ y\colon (\alpha \to \alpha)}
}{\Gamma \vdash x\ (\texttt{fn}_Y\ y \Rightarrow f\ x\ y)\colon (\alpha \to \alpha)}
}{\varnothing \vdash \texttt{fun}_X\ f\ x \Rightarrow x\ (\texttt{fn}_Y\ y \Rightarrow f\ x\ y)\colon ((\alpha \to \alpha) \to (\alpha \to \alpha)) \to (\alpha \to \alpha)}
$$

Hierbei werden folgende Abkürzungen verwendet:

$$
\begin{aligned}
\Gamma &:= [x \mapsto ((\alpha \to \alpha) \to (\alpha \to \alpha)), f \mapsto ((\alpha \to \alpha) \to (\alpha \to \alpha)) \to (\alpha \to \alpha)] \\
\Delta &:= [x \mapsto ((\alpha \to \alpha) \to (\alpha \to \alpha)), f \mapsto ((\alpha \to \alpha) \to (\alpha \to \alpha)) \to (\alpha \to \alpha), y \mapsto \alpha]
\end{aligned}
$$

Abbildung 1: Herleitung für Aufgabe 10-4