Prof. P. Thiemann, M. Geffken Summer Term 2014

Static Program Analysis

http://proglang.informatik.uni-freiburg.de/teaching/programanalysis/2014ss/

Solution Sheet 7

10.07.2014

Definitions

$t ::=$	*terms :*
x	*variable*
$\lambda x.t$	*abstraction*
$t\ t$	*application*

Figure 1: Syntactic forms of the lambda calculus

1. Let $\mathcal{V}$ be a countable set of variable names. The set of terms is the smallest set $\mathcal{T}$ such that
   a) $x \in \mathcal{T}$ for every $x \in \mathcal{V}$
   b) if $\mathtt{t}_1 \in \mathcal{T}$ and $x \in \mathcal{V}$, then $\lambda.\mathtt{t}_1 \in \mathcal{T}$;
   c) if $\mathtt{t}_1 \in \mathcal{T}$ and $\mathtt{t}_2 \in \mathcal{T}$, then $\mathtt{t}_1\ \mathtt{t}_2 \in \mathcal{T}$;
2. The *size* of a term is defined as

$$\begin{aligned}\text{size}(x) &= 1\\ \text{size}(\lambda.\mathtt{t}_1) &= \text{size}(\mathtt{t}_1) + 1\\ \text{size}(\mathtt{t}_1\ \mathtt{t}_2) &= \text{size}(\mathtt{t}_1) + \text{size}(\mathtt{t}_2) + 1\end{aligned}$$

3. The set of *free variables* of a term $\mathtt{t}$, written $\text{FV}(\mathtt{t})$, is defined inductively as follows:

$$\begin{aligned}\text{FV}(x) &= x\\ \text{FV}(\lambda x.\mathtt{t}_1) &= \text{FV}(\mathtt{t}_1) \setminus x\\ \text{FV}(\mathtt{t}_1\ \mathtt{t}_2) &= \text{FV}(\mathtt{t}_1) \cup \text{FV}(\mathtt{t}_2)\end{aligned}$$

4. The set of *bound variables* of a term $\mathtt{t}$, written $\text{BV}(\mathtt{t})$, is defined inductively as follows:

$$\begin{aligned}\text{BV}(x) &= \emptyset\\ \text{BV}(\lambda x.\mathtt{t}_1) &= x \cup \text{BV}(\mathtt{t}_1)\\ \text{BV}(\mathtt{t}_1\ \mathtt{t}_2) &= \text{BV}(\mathtt{t}_1) \cup \text{BV}(\mathtt{t}_2)\end{aligned}$$

Exercise 1 (Properties of FV)

1. Give a proof that $|\text{FV}(\mathtt{t})| \le \text{size}(\mathtt{t})$ for every term $\mathtt{t}$.
2. Provide an example for a term $\mathtt{t}$ such that $\text{FV}(\mathtt{t}) \cap \text{BV}(\mathtt{t}) \neq \emptyset$.

Solution

1. *Proof.* By induction on the size of $\mathtt{t}$. Assuming the desired property for terms smaller than $\mathtt{t}$, we must prove it for $\mathtt{t}$ itself; if we succeed, we may conclude that the property holds for all $\mathtt{t}$. There are three cases to consider:

   Case $\quad \mathtt{t} = x$:
   $|\operatorname{FV}(\mathtt{t})| = |\{x\}| = 1 = \operatorname{size}(\mathtt{t})$.
   Case $\quad \mathtt{t} = \lambda x.\mathtt{t}_1$:
   By IH we have that $|\operatorname{FV}(\mathtt{t}_1)| \leq \operatorname{size}(\mathtt{t}_1)$. Now we can show that $|\operatorname{FV}(\mathtt{t})| = |\operatorname{FV}(\mathtt{t}_1 \setminus x)| \leq |\operatorname{FV}(\mathtt{t}_1| IH \leq \operatorname{size}(\mathtt{t}_1) < \operatorname{size}(\mathtt{t})$.
   Case $\quad \mathtt{t} = \mathtt{t}_1\ \mathtt{t}_2$:
   By IH we have that $|\operatorname{FV}(\mathtt{t}_1)| \leq \operatorname{size}(\mathtt{t}_1)$ and $|\operatorname{FV}(\mathtt{t}_2)| \leq \operatorname{size}(\mathtt{t}_2)$. Thus, $|\operatorname{FV}(\mathtt{t})| = |\operatorname{FV}(\mathtt{t}_1) \cup \operatorname{FV}(\mathtt{t}_2)| \leq |\operatorname{FV}(\mathtt{t}_1)| + |\operatorname{FV}(\mathtt{t}_2)| \leq \operatorname{size}(\mathtt{t}_1) + \operatorname{size}(\mathtt{t}_2) < \operatorname{size}(\mathtt{t})$. □

2. $\lambda x.x\ x$

Exercise 2 (Equality on traces)
We are now looking at a universe $\mathcal{U} = \mathbf{Trace} \times \mathbf{Trace}$, where $\mathbf{Trace} = \Sigma^*$ is just the set of all finite traces over the alphabet $\Sigma = (\mathbf{Var} \times \mathbf{Lab})$. Let EQ be the equality relation on Σ^*:

$$EQ = \{(v, v) \mid v \in \Sigma^*\}$$

Given the monotone function $F : \mathcal{P}(\mathcal{U}) \to \mathcal{P}(\mathcal{U})$:

$$F(R) = \{(\epsilon, \epsilon)\} \cup \{(av, aw) \mid a \in \Sigma \text{ and } (v, w) \in R\}$$

- What is $\operatorname{gfp} F$?
- Prove equality is the least fixpoint of F:

$$\operatorname{lfp} F \stackrel{?}{=} EQ$$

Hint: Considers the definitions of F-consistent (post-fixpoint), F-closed (pre-fixpoint), and the Knaster-Tarski-Theorem. In particular, you can use the principle of induction: if X is F-closed, then $\operatorname{lfp} F \subseteq X$. *You can also use Lemma 1.*

Lemma 1.

$$\forall j \in \mathbb{N} : F^{(j)}(\emptyset) \subseteq \operatorname{lfp} F.$$

Solution

- By construction of F, any post-fixpoint of F has to be a set of pairs of equal traces. Otherwise we have $F(R_{\neq}) \not\subseteq R_{\neq} \wedge F(R_{\neq}) \not\supseteq R_{\neq}$. We shall show both parts separately.

  Case $\quad F(R) \not\subseteq R$:
  It is easy to see that for all R there exist a word $av_1 \cdots v_n \in F(R)$ where $v_1 \cdots v_n$ is the longest word in R that is not in R which gives us $F(R) \not\subseteq R$

  Case $F(R_{\neq}) \not\supseteq R_{\neq}$:
  We cannot construct any set containing an unequal pair of traces $R_{\neq}$ such that $F(R_{\neq}) \supseteq R_{\neq}$ because for $R_{\neq}$ being a post-fixpoint of F all proper suffix pairs have to be in $R_{\neq}$ and all nonempty suffix pairs have to begin with the same

symbol in Σ to be in $F(R)$, which is, however, not possibe for an unqual pair of traces and we get $F(R_{\neq}) \not\supseteq R_{\neq}$.

For a set of pairs of equal traces that are not suffix-closed, e.g. $\{(\epsilon, \epsilon), (aa, aa)\}$ a similar argumentation can be used. All other (suffix-closed) sets of pairs of equal traces are post-fixpoints. By construction of F, each such pair $(v_1 \cdots v_n, v_1 \cdots v_n)$ is in $F^{(n+1)}(\emptyset)$ such that the union of all post-fixpoints is the same as $\bigsqcup_{n \geq 0} F^{(n)}(\emptyset)$.

According to Knaster-Tarski we obtain,

$$\bigsqcup_{n \geq 0} F^{(n)}(\emptyset)$$

is the $\text{gfp}\, F$. As proved earlier we have that $\bigsqcup_{n \geq 0} F^{(n)}(\emptyset) \subseteq \text{lfp}\, F$. Because we know that $\bigsqcup_{n \geq 0} F^{(n)}(\emptyset)$ is a fixpoint, we have that

$$\bigsqcup_{n \geq 0} F^{(n)}(\emptyset)$$

is also the $\text{lfp}\, F$. Thus $\text{lfp}\, F = \text{gfp}\, F$ is the unique fixpoint of F.

The set EQ is a fixpoint, and there is no bigger fixpoint in $\mathcal{P}(\mathcal{U})$. Thus, $\text{gfp}\, F = \Sigma^* \times \Sigma^*$.

- *Proof.* To show that $\text{lfp}\, F \stackrel{?}{=} EQ$ holds, we show $\text{lfp}\, F \subseteq EQ$ and $\text{lfp}\, F \supseteq EQ$.
  1. To show that $\text{lfp}\, F \subseteq EQ$ by the principle of induction it is sufficient to show that EQ is F-closed.

$$\begin{aligned} & F(EQ) \\ =\ & \{(av, aw) \mid a \in \Sigma \text{ and } (v, w) \in EQ\} \cup \{(\epsilon, \epsilon)\} \\ =\ & \{(av, av) \mid a \in \Sigma \text{ and } (v, v) \in \{(w, w) \mid w \in \Sigma^*\}\} \cup \{(\epsilon, \epsilon)\} \\ =\ & \{(av, av) \mid a \in \Sigma \text{ and } (v, v) \in (\Sigma^* \times \Sigma^*)\} \cup \{(\epsilon, \epsilon)\} \\ =\ & \{(av, av) \mid a \in \Sigma \text{ and } v \in \Sigma^*\} \cup \{(\epsilon, \epsilon)\} \\ =\ & \{(v, v) \mid v \in \Sigma^+\} \cup \{(\epsilon, \epsilon)\} \\ =\ & \{(v, v) \mid v \in \Sigma^*\} \\ =\ & EQ \end{aligned}$$

     By the principle of induction, we conclude $\text{lfp}\, F \subseteq EQ$.
  2. It remains to show that $\text{lfp}\, F \supseteq EQ$. Suppose that $(v_1 \cdots v_n, v_1 \cdots v_n) \in EQ \backslash \text{lfp}\, F$, i.e., $\text{lfp}\, F \supseteq EQ$ does not hold. In particular, $(v_1 \cdots v_n, v_1 \cdots v_n) \notin \text{lfp}\, F$.
     By construction of F, $(v_1 \cdots v_n, v_1 \cdots v_n) \in F^{(n+1)}(\emptyset)$, too. But using Lemma 1 we know that $F(\emptyset)^{(j)} \subseteq \text{lfp}\, F$. It follows that $(v_1 \cdots v_n, v_1 \cdots v_n) \in \text{lfp}\, F$ which contradicts our assumption.

Finally we obtain $\text{lfp}\, F = EQ$. □