Lecture: Program analysis
Exercise 6
http://proglang.informatik.uni-freiburg.de/teaching/programanalysis/2010ss/

1 Coinduction

1.1 Generating Functions

Suppose a generating function $F : \mathcal{P}(\{a,b,c\}) \to \mathcal{P}(\{a,b,c\})$ on the universe $\{a,b,c\}$ is defined by the following inference rules:

$$\frac{}{a} \qquad \frac{c}{b} \qquad \frac{a \quad b}{c}$$

1. Write out the set of pairs in the relation F explicitly.
2. List all the F-closed and F-consistent sets.
3. What are $lfp(F)$ and $gfp(F)$?

Solution

X	$F(X)$
$\emptyset$	$\{a\}$
$\{a\}$	$\{a\}$
$\{b\}$	$\{a\}$
$\{c\}$	$\{a,b\}$
$\{a,b\}$	$\{a,c\}$
$\{a,c\}$	$\{a,b\}$
$\{b,c\}$	$\{a,b\}$
$\{a,b,c\}$	$\{a,b,c\}$

The F-closed sets are $\{a\}, \{a,b,c\}$.
The F-consistent sets are $\emptyset, \{a\}, \{a,b,c\}$.
The least fixed point of F is $\{a\}$, the greatest fixed point is $\{a,b,c\}$.

1.2 Relations

Consider a context free grammar with start symbol N and productions $N ::= Zero \,|\, Succ(N)$. It can be rephrased as an inductive definition:

$$Zero \in N \qquad \frac{n \in N}{Succ(n) \in N}$$

1. What set N is defined if you interpret the rules inductively? What does a coinductive interpretation yield?
2. Let us now define a relation $\leq$ on N in the following way:

   $$Zero \leq n \quad \forall n \in S \qquad \frac{n \leq m}{Succ(n) \leq Succ(m)}$$

   Let $R = \{(x,y) | x, y \in N : x \leq y\} \subseteq N \times N$.

   - Define the generating function $S : R \to R$ for this relation. Check that S is a monotone function.
   - Can you find a pair (x,y) such that $(x,y) \in gfp(S)$, but$(x,y) \notin lfp(S)$?
   - Prove that $gfp(S)$ is transitive and reflexive.

Solution

1. The inductive definition yields the natural numbers $\mathbb{N}_0$, the coinductive definition gives $\mathbb{N}_0 \cup \infty$.

2.
   - We define $S(R) = \{(Zero, n) \mid n \in N\} \cup \{(Succ(n), Succ(m)) \mid (n, m) \in R\}$.
     Let $P \subseteq R$. Then,

$$
\begin{aligned}
S(P) &= \{(Zero, n) \mid n \in N\} \cup \{(Succ(n), Succ(m)) \mid (n, m) \in P\} \\
&\subseteq \{(Zero, n) \mid n \in N\} \cup \{(Succ(n), Succ(m)) \mid (n, m) \in R\}
\end{aligned}
$$

   - Apparently, $(n, \infty) \notin \mathit{lfp}(S)$, but $(n, \infty) \in \mathit{gfp}(S)$ for all $n \in N$.
   - **Transitivity:** Since the $\mathit{gfp}(S)$ is S-consistent, its transitive closure $\mathit{gfp}(S)^+$ is also S-consistent (cf. Lemma in the lecture). Therefore, $\mathit{gfp}(S)^+ \subseteq \mathit{gfp}(S)$.
     By definition of the transitive closure, it holds that $\mathit{gfp}(S) \subseteq \mathit{gfp}(S)^+$. Hence, $\mathit{gfp}(S) = \mathit{gfp}(S)^+$, and the transitive closure is obviously transitive.
     Reflexivity: Let $I = \{(x, x) \mid x \in N\}$ be the identity relation. I is S-consistent:

$$
\begin{aligned}
I \subseteq S(I) &= \{(Zero, n) \mid n \in N\} \cup \{(Succ(n), Succ(m)) \mid (n, m) \in I\} \\
&= \{(Zero, n) \mid n \in N\} \cup \{(Succ(x), Succ(x)) \mid x \in N\}
\end{aligned}
$$

     Hence, $I \subseteq \mathit{gfp}(S)$ by the coinduction principle. Therefore, $\mathit{gfp}(S)$ is reflexive.

2 Control Flow Analysis

2.1 Analyzing a program by hand

Consider the following program:

let f = fn $y \Rightarrow y$ in
    let g = fn $x \Rightarrow f$ in
        let h = fn $v \Rightarrow v$ in
            g (g h)

Add labels to the program, and guess an analysis result. Use Table 3.1 in the book, p. 146, to verify that it is indeed an acceptable guess.

Solution

When adding labels, the program is given by:

$$
\begin{aligned}
&\big(\text{let } f = (\text{fn } y \Rightarrow y^1)^2 \text{ in} \\
&\quad \big[\text{let } g = (\text{fn } x \Rightarrow f^3)^4 \text{ in} \\
&\quad\quad \big(\text{let } h = (\text{fn } v \Rightarrow v^5)^6 \text{ in} \\
&\quad\quad\quad [g^7 (g^8\ h^9)^{10}]^{11}\big)^{12}\big]^{13}\big)^{14}
\end{aligned}
$$

A solution might be:

	$(\widehat{C}, \widehat{\rho})$
1,5	$\emptyset$
2,3	{fn y $\Rightarrow y^1$}
4,7,8	{fn x $\Rightarrow f^3$}
6,9	{fn v $\Rightarrow v^5$}
10,11,12,13,14	{fn y $\Rightarrow y^1$}
f	{fn y $\Rightarrow y^1$}
g	{fn x $\Rightarrow f^3$}
h	{fn v $\Rightarrow v^5$}
v, y	$\emptyset$
x	{fn v $\Rightarrow v^5$, fn y $\Rightarrow y^1$}

To prove its validity, the following constraints need to hold:

$$
\begin{aligned}
&(\widehat{C},\widehat{\rho}) \models (\quad)^{14} \text{ iff}\\
&\qquad (\widehat{C},\widehat{\rho}) \models (\quad)^{2} \wedge (\widehat{C},\widehat{\rho}) \models [\quad]^{13} \wedge \widehat{C}(2) \subseteq \widehat{\rho}(f) \wedge \widehat{C}(13) \subseteq \widehat{C}(14)\\
&(\widehat{C},\widehat{\rho}) \models (\quad)^{2} \text{ iff } \{\text{fn } y \Rightarrow y^1\} \subseteq \widehat{C}(2)\\
&(\widehat{C},\widehat{\rho}) \models [\quad]^{13} \text{ iff}\\
&\qquad (\widehat{C},\widehat{\rho}) \models (\quad)^{4} \wedge (\widehat{C},\widehat{\rho}) \models (\quad)^{12} \wedge \widehat{C}(4) \subseteq \widehat{\rho}(g) \wedge \widehat{C}(12) \subseteq \widehat{C}(13)\\
&(\widehat{C},\widehat{\rho}) \models (\quad)^{4} \text{ iff } \{\text{fn } x \Rightarrow f^3\} \subseteq \widehat{C}(4)\\
&(\widehat{C},\widehat{\rho}) \models (\quad)^{12} \text{iff}\\
&\qquad (\widehat{C},\widehat{\rho}) \models (\quad)^{6} \wedge (\widehat{C},\widehat{\rho}) \models [\quad]^{11} \wedge \widehat{C}(6) \subseteq \widehat{\rho}(h) \wedge \widehat{C}(11) \subseteq \widehat{C}(12)\\
&(\widehat{C},\widehat{\rho}) \models (\quad)^{6} \text{ iff } \{\text{fn } v \Rightarrow v^5\} \subseteq \widehat{C}(6)\\
&(\widehat{C},\widehat{\rho}) \models [g^7(\quad)^{10}]^{11} \text{ iff}\\
&\qquad (\widehat{C},\widehat{\rho}) \models g^7 \wedge (\widehat{C},\widehat{\rho}) \models (g^8\ h^9)^{10} \wedge\\
&\qquad (\widehat{C},\widehat{\rho}) \models f^3 \wedge \widehat{C}(10) \subseteq \widehat{\rho}(x) \wedge \widehat{C}(3) \subseteq \widehat{C}(11)\\
&(\widehat{C},\widehat{\rho}) \models (g^8\ h^9)^{10} \text{ iff}\\
&\qquad (\widehat{C},\widehat{\rho}) \models g^8 \wedge (\widehat{C},\widehat{\rho}) \models h^9 \wedge\\
&\qquad (\widehat{C},\widehat{\rho}) \models f^3 \wedge \widehat{C}(9) \subseteq \widehat{\rho}(x) \wedge \widehat{C}(3) \subseteq \widehat{C}(10)
\end{aligned}
$$

2.2 Enhancing the analysis

Modify the Control Flow Analysis of Table 3.1. to take account of the left to right evaluation order imposed by a call-by-value semantics: In the clause [*app*] there is no need to analyze the operand it the operator cannot produce any closures. Try to find a program where the modified analysis accepts a result which is rejected by Table 3.1.

Solution

The constraint $(\widehat{C},\widehat{\rho}) \models t_2^{l_2}$ only needs to be fulfilled if $t_1^{l_1}$ evaluates to a function.

$$
\begin{aligned}
[app] \quad & (\widehat{C},\widehat{\rho}) \models (t_1^{l_1}\ t_2^{l_2})^{l} \text{ iff}\\
& (\widehat{C},\widehat{\rho}) \models t_1^{l_1} \wedge\\
& \Big(\forall [\text{fn } x \Rightarrow t_0^{l_0} \in \widehat{C}(l_1)] :\\
& \qquad (\widehat{C},\widehat{\rho}) \models t_0^{l_0} \wedge (\widehat{\mathbf{C}},\widehat{\rho}) \models \mathbf{t_2^{l_2}} \wedge\\
& \qquad \widehat{C}(l_2) \subseteq \widehat{\rho}(x) \wedge \widehat{C}(l_0) \subseteq \widehat{C}(l)\Big)\\
& \wedge \Big(\forall [\text{fun } f\, x \Rightarrow t_0^{l_0} \in \widehat{C}(l_1)] :\\
& \qquad (\widehat{C},\widehat{\rho}) \models t_0^{l_0} \wedge (\widehat{\mathbf{C}},\widehat{\rho}) \models \mathbf{t_2^{l_2}} \wedge\\
& \qquad \widehat{C}(l_2) \subseteq \widehat{\rho}(x) \wedge \widehat{C}(l_0) \subseteq \widehat{C}(l) \wedge\\
& \qquad\quad \{\text{fun } fx \Rightarrow t_0^{l_0}\} \subseteq \widehat{\rho}(f)\Big)
\end{aligned}
$$