Models of Computation

Midterm Exam on April 03, 2012

Exercise 1 (11)

Fibonacci numbers $F(n)$, $n \in \omega$, are defined as follows:

$$F(0) = 0,\ \ F(1) = 1,\ \ F(n+2) = F(n) + F(n+1),\ n \geq 0.$$

Given the command:

$$w \ = \ \textbf{while}\ z \neq n\ \textbf{do}\, v := y;\ y := x + y;\ x := v;\ z := z + 1.$$

prove by computational induction on its denotational semantics that if $\mathcal{C}[\![w]\!]\sigma = \sigma'$ then

$$\sigma(x) = F(\sigma(z)),\ \sigma(y) = F(\sigma(z) + 1)$$

$$\text{implies}\ \ \sigma'(x) = F(n),\ \sigma'(y) = F(n+1).$$

Finally notice that, if $\mathcal{C}[\![w]\!]\sigma = \sigma'$, then $\sigma(x) = 0,\ \sigma(y) = 1,\ \sigma(z) = 0$ implies $\sigma'(x) = F(n)$.

Exercise 2 (11)

Consider the inference system R corresponding to the rules of the grammar (with $V = \{a, b\}$):

$$S ::= aSa|bSb|aa|bb$$

where the well formed formulas are of the form $\alpha \in L$, with the meaning that string α belongs to the language generated by the grammar. Write down explicitly the rules in R.

Prove by rule induction - in one direction - and by mathematical induction on the length of the strings - in the other direction - that the strings generated by S are all the *nonempty palindromes of even length.* These palindromes are recursively defined as:

$$\alpha\ rev(\alpha) \quad \text{where} \quad rev(x) = x \ \text{ and } \ rev(x\alpha) = rev(\alpha)x \ \text{ with } x \in V \ \ \alpha \in V^*,\ |\alpha| = 1, 2, \ldots$$

Finally prove by induction on derivations that $P(d/(x \in L)) \stackrel{def}{=} |x| = 2|d|$, i.e. the lenght of a string $\in L$ is twice the length of its derivation.

Exercise 3 (8)

Consider the following recursive definition :

$$sq1(n) = \textbf{if}\ n = 0\ \textbf{then}\ 1\ \textbf{else}\ sq1(n-1) + 2 \times n + 1.$$

Write a term $sq1$ in HOFL with corresponds to this recursive definition and find its type.

Then, using symbolic goal reduction, prove by mathematical induction on $k, k \geq 0$, that $P(k) \stackrel{def}{=} t \to k$ implies $(sq1\ t) \to (k+1)^2$.

(1)

Midterm Exam - April 3, 2012

Exercise 1

$\mathcal{C}[\![w]\!] = fix\ \Gamma$

$\Gamma\varphi\sigma = \sigma z \neq n \to \varphi\sigma\left[{}^{\sigma y}/_{\sigma}, {}^{\sigma x+\sigma y}/_{y}, {}^{\sigma y}/_{x}, {}^{\sigma z+1}/_{z}\right], \sigma$

$P(\varphi) \overset{def}{=} \varphi\sigma = \sigma' \Rightarrow \underbrace{\left(\sigma x = F(\sigma z), \sigma y = F(\sigma z+1) \Rightarrow \sigma' x = F(n), \sigma'(y) = F(n+1)\right)}_{Q}$

P admissible?

$\varphi_0 \sqsubseteq \varphi_1 \sqsubseteq \dots$

$\forall i.\ P\varphi_i \overset{?}{\Rightarrow} P \bigsqcup \varphi_i$

Let us assume $\bigsqcup \varphi_i \sigma = \sigma'$. Then we have to prove that Q holds.

But if $\bigsqcup \varphi_i \sigma = \sigma'$, then $\exists k.\ \varphi_k \sigma = \sigma'$. Then Q holds.

$P\varphi \overset{?}{\Rightarrow} P(\Gamma\varphi)$.

Let us assume $P(\varphi)$. We have to prove $P(\Gamma\varphi)$.

$P(\varphi) \overset{def}{=} \varphi\sigma'' = \sigma' \Rightarrow (\sigma x = F(\sigma'' z), \sigma y = F(\sigma'' z+1) \Rightarrow \sigma' x = F(n), \sigma'(y) = F(n+1))$

$P(\Gamma\varphi) \overset{def}{=} \forall\sigma.\ \sigma z \neq n \to \varphi\sigma\left[{}^{\sigma y}/_{\sigma}, {}^{\sigma x+\sigma y}/_{y}, {}^{\sigma y}/_{x}, {}^{\sigma z+1}/_{z}\right], \sigma = \sigma' \Rightarrow Q$

$\boxed{\text{Case } \sigma z = n}$ $\sigma = \sigma'$ $Q = \sigma x = F(n), \sigma y = F(n+1) \Rightarrow \sigma x = F(n)\ \sigma(y) = F(n+1)$

QED.

$\boxed{\text{Case } \sigma z \neq n}$ $\varphi\sigma'' = \sigma'$ $P(\varphi)$ implies:

$\sigma y = F(\sigma z+1)$ $\sigma x + \sigma y = F(\sigma z+2) \Rightarrow \sigma' x = F(n), \sigma'(y) = F(n+1)$

Let us assume the premises of Q:

$\sigma x = F(\sigma z)$ $\sigma y = F(\sigma z+1)$

We have to prove:

$\sigma' x \stackrel{?}{=} F(n)$ $\sigma'(y) \stackrel{?}{=} F(n+1)$

But $\sigma x + \sigma y = F(\sigma z) + F(\sigma z+1) = F(\sigma z+1)$!

Thus the premise of the inductive hypothesis holds. But the conclusion of the induction is what we have to prove

QED

Letting $\sigma x = 0$, $\sigma y = 1$, $\sigma z = 0$ satisfies the premise of what we just proved: $\sigma x = F(0)$ $\sigma y = F(1)$.

Thus $\sigma' x = F(n)$.

Exercise 2

$$\frac{\alpha \in L}{a\alpha a \in L} \qquad \frac{\alpha \in L}{b\alpha b \in L} \qquad aa \in L \qquad bb \in L$$

Rule induction

$P(\alpha \in L) \stackrel{def}{=} \alpha = \beta rev(\beta)$

$P(aa \in L) \stackrel{def}{=} aa \stackrel{?}{=} \beta rev(\beta)$

$a = \beta \quad a = rev(\beta) = rev(a)$ OK

Idem for $bb \in L$

$P(aSa \in L) \stackrel{def}{=} aSa \stackrel{?}{=} \beta rev(\beta)$

But we know that

$P(S \in L) \stackrel{def}{=} S = \beta' rev(\beta')$

We let $\beta = a\beta'$. Thus

$\beta rev(\beta) = a\beta' rev(a\beta') = a\beta' rev(\beta') a = aSa$ QED.

Mathematical induction

On strings of length $(2n+1)$

$P(n) \stackrel{def}{=} \alpha\, rev(\alpha) \in L \qquad |\alpha| = n+1$

$P(0) = a\, rev(a) = aa \in L$, QED similarly for bb

Let us assume $P(n)$. We have to prove:

$P(n+1) = \beta\, rev(\beta) \stackrel{?}{\in} L$ for all β with $|\beta| = n+2$

We can have only $\beta = a\alpha$ or $\beta = b\alpha$

With $\beta = a\alpha$ we have $a\alpha\, rev(a\alpha) = a\alpha\, rev(\alpha)\, a$

with $|\alpha\, rev(\alpha)| = n+1$. Thus $\alpha rev(\alpha) \in L$ and we

can apply the inference rule with $\beta rev(\beta) \in L$. The same if $\beta = b\alpha$.

Induction on derivations

$P(d/x \in L) \stackrel{def}{=} |x| = 2|d|$

Axioms: $d = 1$

$P(\phi/aa \in L) \stackrel{def}{=} |aa| = 2$ QED

$P(\phi/bb \in L) \stackrel{def}{=} |bb| = 2$ QED

Inference rules

$P((d/\alpha \in L)/a\alpha a \in L) \stackrel{def}{=} |a\alpha a| \stackrel{?}{=} 2|(d/\alpha \in L)/a\alpha a \in L|$

But we assume $|\alpha| = 2|(d/\alpha \in L)|$

We have $|(d/\alpha \in L)/a\alpha a \in L| = |(d/\alpha \in L)| + 1$

$|a\alpha a| = |\alpha| + 2$

Thus $|\alpha| + 2 = 2|d/\alpha \in L| + 2 = 2(|d/\alpha \in L| + 1)$

$= 2((d/\alpha \in L)/a\alpha a \in L)$

Similarly for the other rule

Exercise 3

$$sq1 = \underbrace{\mathrm{rec}\,f}_{int\to int}.\ \lambda \overset{int}{n}.\ \text{if } n \text{ then } 1 \text{ else } \underbrace{(f\,(n-1))}_{int} + \underbrace{2\times n + 1}_{int} \quad : int \to int$$

int

int

$int \to int$

$int \to int$

Mathematical induction

$P(k) \overset{def}{=} t \to k$ implies $(sq1\ t) \to (k+1)^2$

$(sq1\ t) \to c \leftarrow$ we assume $\boxed{t \to k}$

$\leftarrow$ if t then 1 else $(sq1\ (t-1)) + 2\times k + 1 \to c$

$\boxed{\text{Case } k=0}$ $\quad 1 \to c \overset{c=1}{\leftarrow} \square \qquad 1 = 1^2$ QED.

$\boxed{\text{case } k\neq 0}$ $\quad (sq1\ (t-1)) + 2\times k + 1 \to c \leftarrow$

$\xleftarrow{c = c' + 2k+1} (sq1\ (t-1)) \to c'$

Assume the inductive hypothesis

$t' \to k-1$ implies $(sq1\ t') \to k^2$

But we have $\quad t-1 \to c'' \xleftarrow[c''=k-1]{} t \to k \leftarrow \square$

Thus we can conclude $(sq1\ (t-1)) \to k^2$

Thus $c = k^2 + 2k + 1 = (k+1)^2 \qquad$ QED.