C241 Homework Assignment 10

1. Performance estimation for recursive programs often involves *recurrence relations* like the one below. Let $a \in \mathbb{N}$. The function $T\colon \mathbb{N} \to \mathbb{N}$ is defined recursively by

$$\begin{aligned} T(0) &= a \\ T(k+1) &= T(k) + k + 1 \end{aligned}$$

We would like to find a *closed form* for T, that is, and an algebraic expression that does not involve recursion

Prove that for all $n \in \mathbb{N}$, $T(n) = a + \dfrac{n^2 + n}{2}$.

SOLUTION

PROOF. The proof is by induction on $n \in \mathbb{N}$.

BASE CASE.

$$T(0) = a = a + \frac{0 + 0^2}{2}$$

INDUCTION CASE. Assume that $T(k) = a + \dfrac{k^2 + k}{2}$.

$$\begin{aligned} T(k+1) &= T(k) + k + 1 && \text{(Defn. } T\text{)} \\ &= a + \frac{k^2 + k}{2} + k + 1 && \text{(I.H.)} \\ &= a + \frac{k^2 + k}{2} + \frac{2k + 2}{2} && \text{(multiply } k+1 \text{ by } 1 = \tfrac{2}{2}\text{)} \\ &= a + \frac{k^2 + 3k + 2}{2} && \text{(adding fractions)} \\ &= a + \frac{(k^2 + 2k + 1) + (k+1)}{2} && \text{(algebra)} \\ &= a + \frac{(k+1)^2 + (k+1)}{2} && \text{(factoring } k^2 + 2k + 1\text{)} \end{aligned}$$

as needed. This completes the induction. □

2. Using the definition of $\mathcal{V}_3$, check that the expression shown in Example 8.3 evaluates to 17. Then evaluate the following words of L_3:

(a) # $ 3 # 8 9 $ 2 5

(b) # # # $ 3 4 5 6 7

(c) # 3 # 4 # 5 $ 6 7

SOLUTION

(a)

$$
\begin{aligned}
&\mathcal{V}_3[\,\#\ \$\ 3\ \#\ 8\ 9\ \$\ 2\ 5] \\
&\overset{2a}{=} \mathcal{V}_3[\,\$\ 3\ \#\ 8\ 9] + \mathcal{V}_3[\,\$\ 2\ 5] \\
&\overset{2b}{=} \mathcal{V}_3[\,\$\ 3\ \#\ 8\ 9] + \big(\mathcal{V}_3[2] \times \mathcal{V}_3[5]\big) \\
&\overset{2b}{=} \big(\mathcal{V}_3[3] \times \mathcal{V}_3[\,\#\ 8\ 9]\big) + \big(\mathcal{V}_3[2] \times \mathcal{V}_3[5]\big) \\
&\overset{2b}{=} \big(\mathcal{V}_3[3] \times (\mathcal{V}_3[8] + \mathcal{V}_3[9])\big) + \big(\mathcal{V}_3[2] \times \mathcal{V}_3[5]\big) \\
&\overset{1}{=} \big(3 \times (8 + 9)\big) + \big(2 \times 5\big) \\
&= 66
\end{aligned}
$$

(b)

$$
\begin{aligned}
&\mathcal{V}_3[\,\#\ \#\ \#\ \$\ 3\ 4\ 5\ 6\ 7] \\
&\overset{2a}{=} \mathcal{V}_3[\,\#\ \#\ \$\ 3\ 4\ 5\ 6] + V_3[7] \\
&\overset{2a}{=} \big(\mathcal{V}_3[\,\#\ \$\ 3\ 4\ 5] + \mathcal{V}_3[6]\big) + V_3[7] \\
&\overset{2a}{=} \Big(\big(\mathcal{V}_3[\,\$\ 3\ 4] + \mathcal{V}_3[5]\big) + \mathcal{V}_3[6]\Big) + V_3[7] \\
&\overset{2a}{=} \big(\big((\mathcal{V}_3[3] \times \mathcal{V}_3[4]) + \mathcal{V}_3[5]\big) + \mathcal{V}_3[6]\big) + V_3[7] \\
&\overset{1}{=} (((3 \times 4) + 5) + 6) + 7 \\
&= 30
\end{aligned}
$$

(c)

$$
\begin{aligned}
&\mathcal{V}_3[\,\#\ 3\ \#\ 4\ \#\ 5\ \$\ 6\ 7] \\
&\overset{2a}{=} \mathcal{V}_3[3] + \mathcal{V}_3[\,\#\ 4\ \#\ 5\ \$\ 6\ 7] \\
&\overset{2a}{=} \mathcal{V}_3[3] + \big(\mathcal{V}_3[4] + \mathcal{V}_3[\,\#\ 5\ \$\ 6\ 7]\big) \\
&\overset{2a}{=} \mathcal{V}_3[3] + \big(\mathcal{V}_3[4] + (\mathcal{V}_3[5] + \mathcal{V}_3[\,\$\ 6\ 7])\big) \\
&\overset{2b}{=} \mathcal{V}_3[3] + \big(\mathcal{V}_3[4] + (\mathcal{V}_3[5] + (\mathcal{V}_3[6] \times \mathcal{V}_3[7]))\big) \\
&\overset{1}{=} 3 + (4 + (5 + (6 \times 7))) \\
&= 54
\end{aligned}
$$

3. Consider the following language, $L_4 \subseteq V^+$, for $V = \mathbb{N} \cup \{$ `#` , `$` $\}$.

	$L_4 \subseteq V^+$
1.	$\mathbb{N} \subseteq L_4$
2*a*.	$u, v \in L_4 \Rightarrow$ `#` $u\ v \in L_4$
2*b*.	$u, v \in L_4 \Rightarrow u\ v$ `$` $\in L_4$
3.	nothing else

Define an interpretation function for L_4 under which ‘ `#` ’ stands for addition and ‘ `$` ’ for multiplication.

SOLUTION

	$L_4 \subseteq V^+$	$\mathcal{V}_4 \colon L_4 \to \mathbb{N}$
1.	$\mathbb{N} \subseteq L_4$	$\mathcal{V}_4[k] = k,$ for $k \in \mathbb{N}$
2*a*.	$u, v \in L_4 \Rightarrow$ `#` $u\ v \in L_4$	$\mathcal{V}_4[$`#` $u\ v] = \mathcal{V}_4[u] + \mathcal{V}_4[v]$
2*b*.	$u, v \in L_4 \Rightarrow u\ v$ `$` $\in L_4$	$\mathcal{V}_4[u\ v$ `$`$] = \mathcal{V}_4[u] \times \mathcal{V}_4[v]$
3.	nothing else	

4. Determine whether the following words are in L_4, and if so evaluate them:

(a) # # 2 3 4 $ 4

(b) # 2 3 $ 4 5 $

(c) 2 # 3 # 5 $ 6

(d) 2 # 3 # 5 $ 6

(e) 2 3 # 4 # 5 6 $ 7 $ $

(f) 1 # # 2 3 4 5 6 $ 7 8 $ $ 9 $

SOLUTION

The subscript on V_4 is omitted below.

(a)
$$\begin{aligned}
&\mathcal{V}[\ \#\ \ \#\ 234\ \$\ 4] \\
&\overset{2a}{=} \mathcal{V}[\ \#\ 234\ \$\ ] + \mathcal{V}[4] \\
&\overset{2b}{=} (\mathcal{V}[\ \#\ 23] \times \mathcal{V}[4]) + \mathcal{V}[4] \\
&\overset{2a}{=} ((\mathcal{V}[2] + \mathcal{V}[3]) \times \mathcal{V}[4]) + \mathcal{V}[4] \\
&\overset{1}{=} ((2+3) \times 4) + 4 \\
&= 24
\end{aligned}$$

(b)
$$\begin{aligned}
&\mathcal{V}[\ \#\ 23\ \$\ 45\ \ \$\ ] \\
&\overset{2b}{=} \mathcal{V}[\ \#\ 23\ \$\ 4] \times \mathcal{V}[5] \\
&\overset{2a}{=} (\mathcal{V}[23\ \$\ ] + \mathcal{V}[4]) \times \mathcal{V}[5] \\
&\overset{2b}{=} ((\mathcal{V}[2] \times \mathcal{V}[3]) + \mathcal{V}[4]) \times \mathcal{V}[5] \\
&\overset{1}{=} ((2 \times 3) + 4) \times 5 \\
&\overset{x}{=} 50
\end{aligned}$$

or

$$\begin{aligned}
&\mathcal{V}[\ \ \#\ \ 23\ \$\ 45\ \$\ ] \\
&\overset{2a}{=} \mathcal{V}[23\ \$\ ] + \mathcal{V}[45\ \$\ ] \\
&\overset{2b}{=} (\mathcal{V}[2] \times \mathcal{V}[3]) + (\mathcal{V}[4] \times \mathcal{V}[5]) \\
&\overset{1}{=} (2 \times 3) + (4 \times 5) \\
&= 26
\end{aligned}$$

(c) 2 # 3 # 5 $ 6 $\notin L_4$

(d) 2 # 3 # 5 $ 6 $\notin L_4$

(e)

$$\begin{aligned}
&\mathcal{V}[23\ \#\ 4\ \#\ 56\ \$\ 7\ \$\ \ \$\ ] \\
&\overset{2b}{=} \mathcal{V}[2] \times \mathcal{V}[3\ \#\ 4\ \#\ 56\ \$\ 7\ \$\ ] \\
&\overset{2b}{=} \mathcal{V}[2] \times (\mathcal{V}[3\ \#\ 4\ \#\ 56\ \$\ ] \times \mathcal{V}[7]) \\
&\overset{2b}{=} \mathcal{V}[2] \times ((\mathcal{V}[3] \times \mathcal{V}[\ \#\ 4\ \#\ 56]) \times \mathcal{V}[7]) \\
&\overset{2a}{=} \mathcal{V}[2] \times ((\mathcal{V}[3] \times (\mathcal{V}[4] + \mathcal{V}[\ \#\ 56])) \times \mathcal{V}[7]) \\
&\overset{2a}{=} \mathcal{V}[2] \times ((\mathcal{V}[3] \times (\mathcal{V}[4] + (\mathcal{V}[5] + \mathcal{V}[6]))) \times \mathcal{V}[7]) \\
&\overset{1}{=} 2 \times ((3 \times (4 + (5+6))) \times 7) \\
&= 630
\end{aligned}$$

or

$$\begin{aligned}
&\mathcal{V}[23\ \#\ 4\ \#\ 56\ \$\ 7\ \$\ \ \$\ ] \\
&\overset{2b}{=} \mathcal{V}[2] \times \mathcal{V}[3\ \#\ 4\ \#\ 56\ \$\ 7\ \$\ ] \\
&\overset{2b}{=} \mathcal{V}[2] \times (\mathcal{V}[3] \times \mathcal{V}[\ \#\ 4\ \#\ 56\ \$\ 7]) \\
&\overset{2b}{=} \mathcal{V}[2] \times (\mathcal{V}[3] \times (\mathcal{V}[4] + \mathcal{V}[\ \#\ 56\ \$\ 7])) \\
&\overset{2b}{=} \mathcal{V}[2] \times (\mathcal{V}[3] \times (\mathcal{V}[4] + (\mathcal{V}[56\ \$\ ] + \mathcal{V}[7]))) \\
&\overset{2b}{=} \mathcal{V}[2] \times (\mathcal{V}[3] \times (\mathcal{V}[4] + ((\mathcal{V}[5] \times \mathcal{V}[6]) + \mathcal{V}[7]))) \\
&\overset{1}{=} 2 \times (3 \times (4 + ((5 \times 6) + 7))) \\
&= 246
\end{aligned}$$

(f) 1 # # 2 3 4 5 6 $ 7 8 $ $ 9 $ $\notin L_4$

5. A language *TERM* of Boolean terms and their meaning $\mathcal{T}$ are defined below. $\mathcal{B} = \langle \{0,1\};\ \wedge, \vee, \neg;\ =;\ 0, 1 \rangle$.

$IVS = \{\mathtt{a}, \mathtt{b}, \mathtt{c}, \ldots\}$	$ENV = \{\sigma \mid \sigma \colon IVS \to \{1,0\}\}$
$TERM \subseteq \big(IVS \cup \{\ \mathtt{+}\ ,\ \mathtt{(},\ \mathtt{)}\ \}\big)^*$	$\mathcal{T} \colon ENV \times TERM \to \{1,0\}$
1*a*. $\mathtt{0} \in TERM$	$\mathcal{T}\sigma\,[\,\mathtt{0}\,] = 0$
1*b*. $\mathtt{1} \in TERM$	$\mathcal{T}\sigma\,[\,\mathtt{1}\,] = 1$
1*c*. $IVS \subseteq TERM$	$\mathcal{T}\sigma\,[\,v\,] = \sigma(v)$ for $v \in IVS$
2*a*. $t \in TERM \Rightarrow \mathtt{-}t \in TERM$	$\mathcal{T}\sigma\,[\,\mathtt{-}t\,] = \neg\mathcal{T}\sigma\,[\,t\,]$
2*b*. $t_1, t_2 \in TERM \Rightarrow \mathtt{(}t_1 \mathtt{+} t_2\mathtt{)} \in TERM$	$\mathcal{T}\sigma\,[\,\mathtt{(}t_1 \mathtt{+} t_2\mathtt{)}\,] = \mathcal{T}\sigma\,[\,t_1\,] \vee \mathcal{T}\sigma\,[\,t_2\,]$
2*b*. $t_1, t_2 \in TERM \Rightarrow \mathtt{(}t_1 \mathtt{*} t_2\mathtt{)} \in TERM$	$\mathcal{T}\sigma\,[\,\mathtt{(}t_1 \mathtt{*} t_2\mathtt{)}\,] = \mathcal{T}\sigma\,[\,t_1\,] \wedge \mathcal{T}\sigma\,[\,t_2\,]$

The *DeMorgan Dual* of $T \in TERM$ is obtained by switching all '`0`'s and '`1`'s; switching all '`+`'s and '`*`'s; and inserting a '`-`' just before every variable symbol. For instance, the DeMorgan Dual of

```
-( a *  b) + (( c + 0) * ( -b +  a))
```

is

```
-(-a + -b) * ((-c * 1) + (--b * -a))
```

(a) Define a recursive function $\mathcal{D} \colon TERM \to TERM$ that gives the DeMorgan Dual of any $T \in TERM$.

(b) Prove that the DeMorgan Dual of a term is its logical negation:
For all $\sigma \in ENV$ *and* $T \in TERM$, $\mathcal{T}\sigma\,[\,\mathcal{D}[T]\,] = \neg\mathcal{T}\sigma\,[\,T\,]$.

SOLUTION

(a)

1*a*.	$\mathcal{D}\,[\,\mathtt{0}\,]$	$=$	$\mathtt{1}$	
1*b*.	$\mathcal{D}\,[\,\mathtt{1}\,]$	$=$	$\mathtt{0}$	
1*c*.	$\mathcal{D}\,[v]$	$=$	$\mathtt{-}\,v,\ v \in IVS$	
2*a*.	$\mathcal{D}\,[\,\mathtt{-}\,T]$	$=$	$\mathtt{-}\,\mathcal{D}\,[T]$	
2*b*.	$\mathcal{D}\,[\,\mathtt{(}T_1 \mathtt{+} T_2\mathtt{)}\,]$	$=$	$\mathtt{(}\mathcal{D}\,[T_1] \mathtt{*} \mathcal{D}\,[T_2]\,\mathtt{)}$	
2*c*.	$\mathcal{D}\,[\,\mathtt{(}T_1 \mathtt{*} T_2\mathtt{)}\,]$	$=$	$\mathtt{(}\mathcal{D}\,[T_1] \mathtt{+} \mathcal{D}\,[T_2]\,\mathtt{)}$	

(b) CLAIM B. *For all* $\sigma \in ENV$ *and* $T \in TERM$, $\mathcal{T}\sigma\,[\,\mathcal{D}\,[T]\,] = \neg\mathcal{T}\sigma\,[\,T\,]$.

PROOF. The proof is by induction on $u \in TERM$, $H[t] \equiv \mathcal{T}\sigma\,[\,\mathcal{D}\,[t]\,] = \neg\mathcal{T}\sigma\,[\,t\,]$.

BASE CASE.

$(\mathtt{0})$ $\mathcal{T}\sigma\,[\,\mathcal{D}\,[\,\mathtt{0}\,]\,] \overset{D1}{=} \mathcal{T}\sigma\,[\,\mathtt{1}\,] \overset{T1}{=} 1 = \neg 0 \overset{T1}{=} \neg(\mathcal{T}\sigma\,[\,\mathtt{0}\,])$

(1) $\mathcal{T}\sigma\,[\,\mathcal{D}\,[\,\mathtt{1}\,]\,] \overset{D1}{=} \mathcal{T}\sigma\,[\,\mathtt{0}\,] \overset{T1}{=} 0 = \neg 1 \overset{T1}{=} \neg(\mathcal{T}\sigma\,[\,\mathtt{1}\,])$

(v) $\mathcal{T}\sigma\,[\,\mathcal{D}\,[v]\,] \overset{D1}{=} \mathcal{T}\sigma\,[\,\mathtt{-}\,v\,] \overset{T2}{=} \neg\mathcal{T}\sigma\,[\,v\,] \overset{D1}{=} \neg\sigma(v) \overset{T1}{=} \neg(\mathcal{T}\sigma\,[\,v\,])$

INDUCTION. Induction cases are all straighforward applications of DeMorgan's Law.

(¬) $\mathcal{T}\sigma\,[\,\mathcal{D}\,[\,\mathtt{-}\,t]\,] \overset{D2}{=} \mathcal{T}\sigma\,[\,\mathtt{-}\,\mathcal{D}\,[t]\,] \overset{T2}{=} \neg\mathcal{T}\sigma\,[\,\mathcal{D}\,[t]\,] \overset{IH}{=} \neg(\neg\mathcal{T}\sigma\,[\,t\,]) \overset{T2}{=} \neg(\neg\mathcal{T}\sigma\,[\,t\,])$

(+)

$$
\begin{aligned}
& \mathcal{T}\sigma\,[\,\mathcal{D}\,[t_1 \mathtt{+} t_2]\,] \\
\overset{D2}{=}\ & \mathcal{T}\sigma\,[\,\mathcal{D}\,[t_1] \mathtt{*} \mathcal{D}\,[t_2]\,] \\
\overset{T2}{=}\ & \mathcal{T}\sigma\,[\,\mathcal{D}\,[t_1]\,] \wedge \mathcal{T}\sigma\,[\,\mathcal{D}\,[t_2]\,] \\
\overset{IH}{=}\ & (\neg\mathcal{T}\sigma\,[\,t_1\,] \wedge \mathcal{T}\sigma\,[\,\mathcal{D}\,[t_2]\,] \\
\overset{IH}{=}\ & (\neg\mathcal{T}\sigma\,[\,t_1\,]) \wedge (\neg\mathcal{T}\sigma\,[\,t_2\,]) \\
\overset{DM}{=}\ & \neg(\mathcal{T}\sigma\,[\,t_1\,] \vee \mathcal{T}\sigma\,[\,t_2\,]) \\
\overset{T2}{=}\ & \neg(\mathcal{T}\sigma\,[\,t_1 \mathtt{+} t_2\,]
\end{aligned}
$$

(*) Similar to case (+).

□

6. Chapter 8 briefly outlines of the proof of the Substitution Lemma (Lemma 8.2, p. 150) for the language PROP of propositional formulas (Fig. 8.2, p. 147).

Substution Lemma. Let $\mathcal{S}$ be a substitution and σ an environment. Define a new environment σ' as follows:

$$\sigma'(v) = \mathcal{P}\sigma\,[\mathcal{S}(v)] \text{ for } v \in IVS$$

Then for all PROPs P,

$$\mathcal{P}\sigma'\,[P] = \mathcal{P}\sigma\,[\mathcal{S}\,[P]]$$

PROOF. The proof is a straightforward structural induction on PROP. The inductive cases hold because the operations are functions. The interesting base case is the one for a variable $v \in IVS$. In that case, we have

$$\mathcal{P}\sigma'\,[v] = \mathcal{P}\sigma\,[\mathcal{S}\,[v]]$$

which is exactly what we need to make the theorem true. □

Write a detailed outline of the proof, stating all the cases that need to be proved. You do not need to complete the proofs.

SOLUTION

Let $\mathcal{S}$, σ, and σ' be given as stated.

(BASE CASES)

1a $\mathcal{P}\sigma'\,[\texttt{0}] = \mathcal{P}\sigma\,[\mathcal{S}\,[\texttt{0}]]$.

1b $\mathcal{P}\sigma'\,[\texttt{1}] = \mathcal{P}\sigma\,[\mathcal{S}\,[\texttt{1}]]$.

1c $\forall x \in \text{PVAR}\colon \mathcal{P}\sigma'\,[x] = \mathcal{P}\sigma\,[\mathcal{S}\,[x]]$.

(INDUCTION CASES)

2a If $\mathcal{P}\sigma'\,[u] = \mathcal{P}\sigma\,[\mathcal{S}\,[u]]$ then $\mathcal{P}\sigma'\,[\texttt{(}\,u\,\texttt{)}\,] = \mathcal{P}\sigma\,[\mathcal{S}\,[\texttt{(}\,u\,\texttt{)}\,]]$.

2b If $\mathcal{P}\sigma'\,[u] = \mathcal{P}\sigma\,[\mathcal{S}\,[u]]$ then $\mathcal{P}\sigma'\,[\texttt{-}u] = \mathcal{P}\sigma\,[\mathcal{S}\,[\texttt{-}u]]$.

2c If $\mathcal{P}\sigma'\,[u] = \mathcal{P}\sigma\,[\mathcal{S}\,[u]]$ and $\mathcal{P}\sigma'\,[v] = \mathcal{P}\sigma\,[\mathcal{S}\,[v]]$ then $\mathcal{P}\sigma'\,[u\,\texttt{\&}\,v] = \mathcal{P}\sigma\,[\mathcal{S}\,[u\,\texttt{\&}\,v]]$.

2d If $\mathcal{P}\sigma'\,[u] = \mathcal{P}\sigma\,[\mathcal{S}\,[u]]$ and $\mathcal{P}\sigma'\,[v] = \mathcal{P}\sigma\,[\mathcal{S}\,[v]]$ then $\mathcal{P}\sigma'\,[u\,\texttt{|}\,v] = \mathcal{P}\sigma\,[\mathcal{S}\,[u\,\texttt{|}\,v]]$.

7. Let $F \equiv p \wedge (q \vee r)$. Perform the following substitutions

(a) $F\begin{bmatrix} r, q, p \\ p, q, r \end{bmatrix}$

(b) $F\begin{bmatrix} p \vee r \\ p \end{bmatrix}$

(c) $F\begin{bmatrix} p \vee r, & q \Rightarrow r \\ p, & r \end{bmatrix}$

(d) $\left(F\begin{bmatrix} p \vee r \\ p \end{bmatrix}\right)\begin{bmatrix} q \\ p \end{bmatrix}$

(e) $\left(F\begin{bmatrix} q \\ p \end{bmatrix}\right)\begin{bmatrix} p \vee r \\ p \end{bmatrix}$

SOLUTION

(a) $F\begin{bmatrix} r, q, p \\ p, q, r \end{bmatrix} \equiv r \wedge (q \vee p)$.

(b) $F\begin{bmatrix} p \vee r \\ p \end{bmatrix} \equiv (p \vee r) \wedge (q \vee r)$.

(c) $F\begin{bmatrix} p \vee r, & q \Rightarrow r \\ p, & r \end{bmatrix} \equiv (p \vee r) \wedge (q \vee (q \Rightarrow r))$.

(d) $\left(F\begin{bmatrix} p \vee r \\ p \end{bmatrix}\right)\begin{bmatrix} q \\ p \end{bmatrix} \equiv (q \vee r) \wedge (q \vee r)$.

(e) $\left(F\begin{bmatrix} q \\ p \end{bmatrix}\right)\begin{bmatrix} p \vee r \\ p \end{bmatrix} \equiv q \wedge (q \vee r)$.

8. Given a program fragment

$$\{\text{PRE}\}$$
$$\texttt{while}\ \text{TEST}\ \texttt{do}\ \{\text{INV}\}\ \text{BODY}$$
$$\{\text{POST}\}$$

The *Theorem on Loop Invariants* from Chapter 5 implies that to prove assertion POST holds after the while-loop executes, it suffices to prove three things:

1. INITIALIZATION: PRE $\Rightarrow$ INV.

   Assertion INV must hold when the program first reaches the loop, so whatever condition PRE that does hold must imply POST also holds.

2. INVARIANCE: $\{\text{INV} \wedge \text{TEST}\}\,\text{BODY}\,\{\text{IMV}\}$

   If assertion INV holds and the loop TEST is true, then after executing the loop BODY, INV will again hold.

3. TERMINATION: INV $\wedge \neg$TEST $\Rightarrow$ INV.

   When (and if) the loop terminates, INV will be true and the loop TEST will have failed. These two conditions should imply that the final assertion, POST, also holds.

In the program to the right, the final assertion states that program variable x holds the greatest common divisor of A and B.

Write down exactly what must be proven to verify this program and do the proofs. If you are not able to finish the proofs, clearly indicate what is left to be proven.

$\{x = A \in \mathbb{N} \wedge y = B \in \mathbb{N}\}$
while $x \neq y$ **do**
  $\{\gcd(x, y) = \gcd(A, B)\}$
  if $x < y$
    then $y := y - x$
    else $x := x - y$
$\{x = \gcd(A, B)\}$

SOLUTION

1. INITIALIZATION: *If* $x = A$ *and* $y = B$ *then* $\gcd(x, y) = \gcd(A, B)$.

   PROOF. This follows immediately by substitution of equals for equals.

2. INVARIANCE: *If* $\gcd(x, y) = \gcd(A, B)$ *and* $x \neq y$ *then after executing*

   $$\texttt{if}\, x < y\ \texttt{then}\ y := y - x\ \texttt{else}\, x := x - y$$

   it will again be the case that $\gcd(x, y) = \gcd(A, B)$.

   PROOF: There are two cases to consider:

   A. If $x < y$ then BODY assigns $y - x$ to y, so we must show that $\gcd(x, y - x) = \gcd(x, y)$.

      Toward this end, let $d = \gcd(x, y)$. Since d divides x, $x = d \cdot q_x$ for some q_x. Likewise, $y = d \cdot q_y$ for some q_y. Hence, $y - x = d \cdot q_y - d \cdot q_x = d \cdot (q_y - q_x)$. Thus, d is a common divisor of x and $y - x$.

We must now show that d is greater than any common divisor of x and $y - x$. Suppose d' is a common divisor, so that for some p_x and p_{xy}, $x = d' \cdot p_x$ and $y - x = d' \cdot p_{xy}$. Adding $x = d' \cdot q_x$ to both sides of the latter equation, we get $y = d' \cdot p_{xy} + d' \cdot p_x = d' \cdot (p_{xy} - p_x)$. Thus d' is a common divisor of x and y. Therefore, $d' \leq gcd(x, y) = d$.

We have shown that d is a common divisor of x and $y - x$, and there is no greater common divisor. This makes d the greatest common divisor, $d = \gcd(x, y - x)$.

B. Similarly, if $y - x$ then we must show $\gcd(x - y, y) = \gcd(x, y)$.

The proof is the same as for Case A, exchanging x and y.

3. TERMINATION: *If* $\gcd(x, y) = \gcd(A, B)$ *and* $x = y$ *then* $x = \gcd(A, B)$.

PROOF. Since $x = y$, $\gcd(x, y) = \gcd(x, x) = x$. Therefore, $\gcd(A, B) = \gcd(x, y) = x$, as desired.

9. Proposition 8.7 (p. 154) states

$$\{\,P\,\}\ x := t\ \{\,Q\,\} \quad \text{if} \quad P \Rightarrow Q\begin{bmatrix} t \\ x \end{bmatrix}$$

where $Q\begin{bmatrix} t \\ x \end{bmatrix}$ is the formula that results from substituting term t for identifier x in proposition Q.

Use this transformation to reduce

$$\{\,A = qB + r \wedge r < B\,\}\ \texttt{begin}\ q := q + 1\ \texttt{;}\ r := r - B\ \texttt{end}\ \{\,A = qB + r\,\}$$

to a purely arithmetic (containing no program statements) proposition, as is done in Example 8.8 (p. 156.

SOLUTION

$$\{\,A = qB + r \wedge r < B\,\}\ \texttt{begin}\ q := q + 1\ \texttt{;}\ r := r - B\ \texttt{end}\ \{\,A = qB + r\,\}$$

reduces to

$$\{\,A = qB + r \wedge r < B\,\}\, q := q + 1\, \{\,(A = qB + r)\begin{bmatrix} r - B \\ r \end{bmatrix}\,\}$$

reduces to

$$(A = qB + r \wedge r < B) \Rightarrow (A = qB + r)\begin{bmatrix} r - B \\ r \end{bmatrix}\begin{bmatrix} q + 1 \\ q \end{bmatrix}$$

applying the substitution $\begin{bmatrix} r - B \\ r \end{bmatrix}$ first yields

$$(A = qB + r \wedge r < B) \Rightarrow (A = qB + r - B)\begin{bmatrix} q + 1 \\ q \end{bmatrix}$$

applying the substitution $\begin{bmatrix} q + 1 \\ q \end{bmatrix}$ next yields

$$(A = qB + r \wedge r < B) \Rightarrow (A = (q + 1)B + r - B)$$

Simplifying $(q + 1)B + (r - B)$ to $qB + r$ we get

$$(A = qB + r) \wedge r < B) \Rightarrow qB + r$$

which is true.

COMMENT. This derivation does not introduce before-and-after variables q' and r' as we did earlier for this example. In contrast, it uses purely syntactic transformations (e.g. substitution) to reduce an assertion about a program fragment to a purely mathematical proposition.

SUPPLEMENTAL PROBLEM. (Pill Problem) Once long ago, a man was tried and convicted of a crime, and he was sentenced to death by the Judge. He pleas for mercy. The Judge produces a vial containing twelve pills and a balance scale. He says,

> "Eleven of the pills in this vial are poisonous; you will die within minutes of taking one. One pill is non-poisonous; if you swallow that pill, nothing will happen and you are free to go.
>
> The pills are identical in every other respect, except that the non-poisonous pill has a different weight than any of the poisonous ones.
>
> I will grant you three tries with the balance scale, after which you must take one of the pills.

QUESTION: What are the man's best chances of going free?

ANSWER: If he is smart enough, he will be certain to take the non-poisonous pill and go free."

Explain how.

COMMENT: *To give yourself a real challenge: impose a time limit on solving this problem, and/or don't use pencil and paper (or exhaustive search by computer).*

SOLUTION

No solution is provided. This is such a nice problem I don't want to deprive anyone of the chance to solve it—$\mathcal{SDJ}$.