Program Construction and Reasoning
Exercises

Shin-Cheng Mu

2010 Formosan Summer School on
Logic, Language, and Computation
June 28 – July 9, 2010

Guarded Command Language Basics

1. **Swapping Booleans** Verify:

$$
\begin{array}{l}
|[\ \mathbf{var}\ a, b : \mathit{bool};\\
\quad \{a \leftrightarrow A \wedge b \leftrightarrow B\}\\
\quad a := a \leftrightarrow b;\\
\quad b := a \leftrightarrow b;\\
\quad a := a \leftrightarrow b;\\
\quad \{a \leftrightarrow B \wedge b \leftrightarrow A\}\\
]|.
\end{array}
$$

Hint: recall the definition $\mathit{true} \leftrightarrow a = a$, and that $\leftrightarrow$ is associative: $(a \leftrightarrow b) \leftrightarrow c = a \leftrightarrow (b \leftrightarrow c)$.

Solution: The program can be annotated as

$$
\begin{array}{ll}
& \{a \leftrightarrow A \wedge b \leftrightarrow B\}\\
& a := a \leftrightarrow b\\
& \{b \leftrightarrow B\ \wedge\ a \leftrightarrow b \leftrightarrow A\}\\
; & b := a \leftrightarrow b\\
& \{a \leftrightarrow b \leftrightarrow B\ \wedge\ b \leftrightarrow A\}\\
; & a := a \leftrightarrow b\\
& \{a \leftrightarrow B \wedge b \leftrightarrow A\}.
\end{array}
$$

Proofs:

$$
\begin{array}{ll}
& (a \leftrightarrow B\ \wedge\ b \leftrightarrow A)[a \leftrightarrow b/a]\\
\Leftrightarrow & a \leftrightarrow b \leftrightarrow B\ \wedge\ b \leftrightarrow A,
\end{array}
$$

$$
\begin{array}{ll}
& (a \leftrightarrow b \leftrightarrow B\ \wedge\ b \leftrightarrow A)[a \leftrightarrow b/b]\\
\Leftrightarrow & a \leftrightarrow a \leftrightarrow b \leftrightarrow B\ \wedge\ a \leftrightarrow b \leftrightarrow A\\
\Leftrightarrow & b \leftrightarrow B\ \wedge\ a \leftrightarrow b \leftrightarrow A,
\end{array}
$$

$$
\begin{array}{ll}
& (b \leftrightarrow B\ \wedge\ a \leftrightarrow b \leftrightarrow A)[a \leftrightarrow b/a]\\
\Leftrightarrow & b \leftrightarrow B\ \wedge\ a \leftrightarrow b \leftrightarrow b \leftrightarrow A\\
\Leftrightarrow & b \leftrightarrow B\ \wedge\ a \leftrightarrow A.
\end{array}
$$

2. Verify:

$$
\begin{array}{l}
|[\ \textbf{var}\ a, b : bool; \\
\quad \{true\} \\
\quad \textbf{if}\ \neg a \vee b \rightarrow a := \neg a \\
\quad\ \ [\!]\ a \vee \neg b \rightarrow b := \neg b \\
\quad \textbf{fi} \\
\quad \{a \vee b\} \\
]|
\end{array}
$$

Solution: Certainly $true \Rightarrow \neg a \vee b\ a \vee \neg b$. To verify the first branch:

$$
\begin{array}{ll}
 & (a \vee b)[\neg a/a] \\
\Leftrightarrow & \neg a \vee b.
\end{array}
$$

The other branch is similar.

Loop and Loop Invariants

3. Prove the correctness of the following program:

$$
\begin{array}{l}
|[\ \textbf{var}\ x, y, N : int\ \{N \geq 0\}; \\
\\
\quad x, y := 0, 1; \\
\quad \textbf{do}\ x \neq N \rightarrow x, y := x + 1, y + y\ \textbf{od} \\
\quad \{y = 2^N\} \\
]|
\end{array}
$$

Solution: Use the loop invariant

$$y = 2^x \ \wedge\ 0 \leq x \leq N$$

and bound $|N - x|$.

4. Prove the correctness of the following program:

$$
\begin{array}{l}
|[\ \textbf{var}\ x, y, N : int\ \{N \geq 0\}; \\
\\
\quad x, y := 0, 0; \\
\quad \textbf{do}\ x \neq 0 \rightarrow x := x - 1 \\
\quad\quad [\!]\ y \neq N \rightarrow x, y := N, y + 1 \\
\quad \textbf{od} \\
\quad \{x = 0\ \wedge\ y = N\} \\
]|
\end{array}
$$

Solution: Apparently the negation of the guards equivals $x = 0 \wedge y = N$. The difficult part is the proof of termination, for which we need this loop invariant:

$$P : 0 \leq x \leq N \wedge 0 \leq y \leq N,$$

and bound:

$$bnd : (N + 1) \times (N - y) + x.$$

It is immediate that $P \wedge (x \neq 0 \vee y \neq N)$ implies $bnd \geq 0$. For the second branch we reason:

$$\begin{array}{ll} & ((N+1) \times (N-y) + x < C)[N, y+1/x, y] \\ \Leftrightarrow & (N+1) \times (N-y-1) + N < C \\ \Leftrightarrow & (N+1) \times (N-y) - 1 < C \\ \Leftarrow & (N+1) \times (N-y) + x = C \ \wedge \ 0 \leq x. \end{array}$$

Note that the bound $N \times (N - y) + x$ fails for the second branch.

5. The following program non-deterministically computes x and y such that $x \times y = N$. Prove:

$$\begin{array}{l} |[\ \textbf{var}\ p, x, y, N : int; \{N \geq 1\} \\ \quad p, x, y := N - 1, 1, 1 \\ \quad \{N = x \times y + p\} \\ \ ;\textbf{do}\ p \neq 0 \rightarrow \\ \qquad \textbf{if}\ p\,\textbf{mod}\,x = 0 \rightarrow y, p := y + 1, p - x \\ \qquad \ \ [\!]\ p\,\textbf{mod}\,y = 0 \rightarrow x, p := x + 1, p - y \\ \qquad \textbf{fi} \\ \quad \textbf{od} \\ \quad \{x \times y = N\} \\ ]| \end{array}$$

Solution: If we try reasoning about the first branch:

$$\begin{array}{ll} & (N = x \times y + p)[y+1, p-x/y, p] \\ \Leftrightarrow & N = x \times (y+1) + p - x \\ \Leftrightarrow & N = x \times y + p, \end{array}$$

we notice that $N = x \times y + p$ does not need the guard $p\,\textbf{mod}\,x$ to hold. The guards, however, do play a role for the termination proof. We use the invariant

$$(N = x \times y + p) \ \wedge \ (0 \leq p) \ \wedge \ (0 < x) \ \wedge \ (0 < y) \ \wedge \ (p\,\textbf{mod}\,x = 0 \vee p\,\textbf{mod}\,y = 0)$$

and bound p.

The bound p decreases after the assignment $p := p - x$ because $0 < x$. For p to remain non-negative, notice that $p \neq 0$ and $p\,\textbf{mod}\,x = 0$ implies that $p \geq x$ (otherwise $p\,\textbf{mod}\,x$ would be p).