Deductive Program Verification: Solutions to Exercise #2

Yu-Fang Chen
Dept. of Information Management, National Taiwan University

FLOLAC 2007: July 2–13, 2007

Note

We assume the binding powers of the various operators decrease in this order: $(\cdot)^n$ (exponentiation), $\{+, -\}$, $\neg$, $\{=, \geq, \leq\}$, $\{\forall, \exists\}$, $\{\wedge, \vee\}$, $\rightarrow$, $\leftrightarrow$, $\equiv$.

Solutions

1. Prove the total correctness of the following annotated program segment; please present your correctness proof as a proof outline, supplying all intermediate assertions.

$\{m > 0 \wedge n > 0\}$
$x, y := m, n;$
while $x \neq 0 \wedge y \neq 0$ **do**
    if $x < y$ **then** $x, y := y, x$ **fi**;
    $x := x - y$
od
$\{(x = 0 \wedge y = gcd(m, n)) \vee (y = 0 \wedge x = gcd(m, n))\}$

(50 points)

Solution.

$\{m > 0 \wedge n > 0\}$
$\{m = m \wedge n = n \wedge m \geq 0 \wedge n > 0\}$
$x, y := m, n;$
$\{x = m \wedge y = n \wedge x \geq 0 \wedge y > 0\}$
$\{invariant : gcd(x, y) = gcd(m, n) \wedge x \geq 0 \wedge y > 0\}\{rank\ function : x + y\}$
while $x \neq 0 \wedge y \neq 0$ **do**
$\{gcd(x, y) = gcd(m, n) \wedge x \geq 0 \wedge y > 0 \wedge x \neq 0 \wedge y \neq 0\}$
$\{gcd(x, y) = gcd(m, n) \wedge x > 0 \wedge y > 0\}$
    if $x < y$ **then**
    $\{gcd(x, y) = gcd(m, n) \wedge x > 0 \wedge y > 0 \wedge x < y\}$

$x, y := y, x$

$\{gcd(y, x) = gcd(m, n) \wedge y > 0 \wedge x > 0 \wedge y < x\}$

$\{gcd(x, y) = gcd(m, n) \wedge x > 0 \wedge y > 0 \wedge x \geq y\}$

fi;

$\{gcd(x, y) = gcd(m, n) \wedge x > 0 \wedge y > 0 \wedge x \geq y\}$

$\{gcd(x - y, y) = gcd(m, n) \wedge x - y \geq 0 \wedge y > 0\}$

$x := x - y$

$\{gcd(x, y) = gcd(m, n) \wedge x \geq 0 \wedge y > 0\}$

od

$\{gcd(x, y) = gcd(m, n) \wedge x \geq 0 \wedge y > 0 \wedge \neg(x \neq 0 \wedge y \neq 0)\}$

$\{(x = 0 \wedge y = gcd(m, n)) \vee (y = 0 \wedge x = gcd(m, n))\}$

□

2. Annotate the following program segments (of Peterson's two-process mutual exclusion algorithm) such that it is clear mutual exclusion is satisfied. The annotation must be *interference free*. You may need to introduce auxiliary variables.

// P_0	// P_1
// $Q[0]$ is *false* initially	// $Q[1]$ is *false* initially
...	...
$Q[0] := true$;	$Q[1] := true$;
$TURN := 0$;	$TURN := 1$;
await $\neg Q[1] \vee TURN \neq 0$;	**await** $\neg Q[0] \vee TURN \neq 1$;
// critical section;	// critical section;
$Q[0] := false$;	$Q[1] := false$;
...	...

(50 points)

Solution.

...	...
$\{\neg Q[0]\}$	$\{\neg Q[1]\}$
$Q[0] := true$;	$Q[1] := true$;
$\{Q[0]\}$	$\{Q[1]\}$
$\langle TURN := 0; X[0] := true; \rangle$	$\langle TURN := 1; X[1] := true; \rangle$
$\{Q[0] \wedge X[0]\}$	$\{Q[1] \wedge X[1]\}$
$\langle$**await** $\neg Q[1] \vee TURN \neq 0; X[0] := false; \rangle$	$\langle$**await** $\neg Q[0] \vee TURN \neq 1; X[1] := false; \rangle$
$\{Q[0] \wedge \neg X[0] \wedge (\neg Q[1] \vee$	$\{Q[1] \wedge \neg X[1] \wedge (\neg Q[0] \vee$
$TURN \neq 0 \vee X[1])\}$	$TURN \neq 1 \vee X[0])\}$
// critical section;	// critical section;
$Q[0] := false$;	$Q[1] := false$;
$\{\neg Q[0]\}$	$\{\neg Q[1]\}$
...	...

Because the conjunction of $Q[1] \wedge \neg X[1] \wedge (\neg Q[0] \vee TURN \neq 1 \vee X[0])$ and $Q[0] \wedge \neg X[0] \wedge (\neg Q[1] \vee TURN \neq 0 \vee X[1])$ is *false*. Mutual exclusion is satisfied between these two processes.

To check *interference free*, you have to proof all possible combinations of atomic region R and every assertion r in P_0 and P_1. Here we only list a few of them:

(a) Let $r = Q[0] \wedge \neg X[0] \wedge (\neg Q[1] \vee TURN \neq 0 \vee X[1])$,
$R = Q[1] := true$, $pre(R) = \neg Q[1]$.

$$\dfrac{\dfrac{\text{pred. calculus + algebra}}{r \rightarrow r[true/Q[1]]} \qquad \dfrac{}{\{r[true/Q[1]]\}\ S_1\ \{r\}}\ \text{(Assign.)}}{\{r \wedge pre(R)\}\ R\ \{r\}}\ \text{(S. Pre.)}$$

(b) Let $r = Q[0] \wedge \neg X[0] \wedge (\neg Q[1] \vee TURN \neq 0 \vee X[1])$,
$R = \langle TURN{:=}1; X[1] := true\rangle$, $pre(R) = Q[1]$.

$$\dfrac{\pi \qquad \dfrac{}{\{r[true/X[1]]\}\ X[1] := true\ \{r\}}\ \text{(Assign.)}}{\{r \wedge pre(R)\}\ R\ \{r\}}\ \text{(Sequence)}$$

π:

$$\dfrac{\dfrac{\text{pred. calculus + algebra}}{r \rightarrow r[true/X[1]][1/TURN]} \qquad \dfrac{}{\{r[true/X[1]][1/TURN]\}\ TURN := 1\ \{r[true/X[1]]\}}\ \text{(Assign.)}}{\{r \wedge pre(R)\}\ TURN := 1\ \{r[true/X[1]]\}}\ \text{(S. Pre.)}$$

□