CS 245 — Assignment #9
Spring 2006

Due Date: Tuesday, July 25 at 5pm.

Use `makeCover` to produce a cover page for your assignment and hand in your assignment in the CS 245 assignment box. Assignments are to be done individually.

1. (12 points) Prove that the following triple (pre-condition, program, post-condition) is satisfied under partial correctness. Use natural deduction or transformational proof techniques to prove any implied conditions. Clearly state your loop invariant.

$(\!|n \geq 1|\!)$
```
i = 1;
z = 1;
while (i != n) {
   i = i + 1;
   z = z + (2*i - 1);
}
```
$(\!|z = n^2|\!)$

Loop Invariant

$z = i^2$

Annotated Program

$(\| n \geq 1 \|)$	
$(\| 1 = 1^2 \|)$	`implied (algebra)`
`i = 1;`	
$(\| 1 = i^2 \|)$	`assignment`
`z = 1;`	
$(\| z = i^2 \|)$	`assignment`
`while (i != n) {`	
$(\| z = i^2 \ \wedge \ i \neq n \|)$	`partial-while`
$(\| z + (2(i+1) - 1) = (i+1)^2 \|)$	`implied (1)`
`i = i + 1;`	
$(\| z + (2i - 1) = i^2 \|)$	`assignment`
`z = z + (2*i - 1);`	
$(\| z = i^2 \|)$	`assignment`
`}`	
$(\| z = i^2 \ \wedge \ i = n \|)$	`partial-while`
$(\| z = n^2 \|)$	`implied ( =_E)`

Proof of implied condition (1):

$$\begin{array}{ll} & z = i^2 \wedge i \neq n \\ \Rightarrow & z + (2(i+1) - 1) = (i+1)^2 \end{array}$$

1.	$z = i^2 \wedge i \neq n$	assumption
2.	$z = i^2$	$1, \wedge\_E$
3.	$z + (2(i+1) - 1) = i^2 + (2(i+1) - 1)$	2, algebra
4.	$z + (2(i+1) - 1) = i^2 + 2i + 1$	3, algebra
5.	$z + (2(i+1) - 1) = (i+1)^2$	4, algebra
6.	(line 1) $\Rightarrow$ (line 5)	$1 - 5, \Rightarrow\_I$

2. (13 points) Prove that the following triple (pre-condition, program, post-condition) is satisfied under partial correctness. Use natural deduction or transformational proof techniques to prove any implied conditions. Clearly state your loop invariant.

$(\!| n \geq 1 |\!)$

```
max = A[1];
for i = 2 to n {
    if (max < A[i]) {
        max = A[i];
    }
}
```

$(\!| \forall k \bullet 1 \leq k \leq n \;\Rightarrow\; max \geq A[k] |\!)$

Notes

There are two cases: one where $n = 1$ and the for loop does nothing, and one where $n \geq 2$ and the for loop does do something. Thus, we need two separate proofs of correctness. In the first proof, the precondition is $(\!|n = 1|\!)$. Here, the triple:

$(\!|n = 1|\!)$
`max = A[1];`
$(\!|\forall k \bullet 1 \leq k \leq n \;\; \Rightarrow \;\; max \geq A[k]|\!)$

is obviously satisfied under partial correctness and we will omit the proof (you may also omit the proof in your submitted solution). In the second proof, the precondition is $(\!|n \geq 2|\!)$. Below is the proof for this second case.

Loop Invariant

$\forall k \bullet 1 \leq k \leq i - 1 \Rightarrow max \geq A[k]$

Annotated Program

$(\!|n \geq 2|\!)$	
$(\!|\forall k \bullet 1 \leq k \leq 1 \;\; \Rightarrow \;\; A[1] \geq A[k] \;\; \wedge \;\; n \geq 2|\!)$	`implied (1)`
`max = A[1];`	
$(\!|\forall k \bullet 1 \leq k \leq 1 \;\; \Rightarrow \;\; max \geq A[k] \;\; \wedge \;\; n \geq 2|\!)$	`assignment`
`for i = 2 to n {`	
$(\!|\forall k \bullet 1 \leq k \leq i - 1 \;\; \Rightarrow \;\; max \geq A[k] \;\; \wedge \;\; 2 \leq i \leq n|\!)$	`for-loop`
`if (max < A[i]) {`	
$(\!|(\forall k \bullet 1 \leq k \leq i - 1 \;\; \Rightarrow \;\; max \geq A[k]) \;\; \wedge \;\; (max < A[i])|\!)$	`if-then`
$(\!|\forall k \bullet 1 \leq k \leq i \;\; \Rightarrow \;\; A[i] \geq A[k]|\!)$	`implied (2)`
`max = A[i];`	
$(\!|\forall k \bullet 1 \leq k \leq i \;\; \Rightarrow \;\; max \geq A[k]|\!)$	`assignment`
`}`	
$(\!|\forall k \bullet 1 \leq k \leq i \;\; \Rightarrow \;\; max \geq A[k]|\!)$	`if-then (3)`
`}`	
$(\!|\forall k \bullet 1 \leq k \leq n \;\; \Rightarrow \;\; max \geq A[k]|\!)$	`for-loop`

Proof of implied condition (1):

$(n \geq 2) \Rightarrow (\forall k \bullet 1 \leq k \leq 1 \;\Rightarrow\; A[1] \geq A[k] \wedge n \geq 2)$

It is easy to see that $(\forall k \bullet 1 \leq k \leq 1 \Rightarrow A[1] \geq A[k])$ is a tautology: when $k \neq 1$, $1 \leq k \leq 1$ is false and therefore the implication is true; and when $k = 1$, $A[1] \geq A[k])$ is true and therefore the implication is true.

Proof of implied condition (2):

$$
\begin{array}{ll}
 & (\forall k \bullet 1 \leq k \leq i-1 \Rightarrow max \geq A[k]) \wedge (A[i] > max) \\
\Rightarrow & (\forall k \bullet 1 \leq k \leq i \Rightarrow A[i] \geq A[k])
\end{array}
$$

1.	$(\forall k \bullet 1 \leq k \leq i-1 \Rightarrow max \geq A[k]) \wedge (A[i] > max)$	assumption
2.	$\forall k \bullet 1 \leq k \leq i-1 \Rightarrow max \geq A[k]$	$1, \wedge\_\mathrm{E}$
3.	$A[i] > max$	$1, \wedge\_\mathrm{E}$
4.	k_g	
5.	$1 \leq k_g \leq i$	assumption
6.	$1 \leq k_g \leq i-1 \vee k_g = i$	algebra
7.	$1 \leq k_g \leq i-1$	assumption
8.	$1 \leq k_g \leq i-1 \Rightarrow max \geq A[k_g]$	$2, \forall\_\mathrm{E}$
9.	$max \geq A[k_g]$	$7, 8, \Rightarrow\_\mathrm{E}$
10.	$A[i] \geq A[k_g]$	$3, 9,$ algebra
11.	$1 \leq k_g \leq i-1 \Rightarrow A[i] \geq A[k_g]$	$7-10, \Rightarrow\_\mathrm{I}$
12.	$k_g = i$	assumption
13.	$A[i] = A[i]$	$=\_\mathrm{I}$
14.	$A[i] = A[k_g]$	$12, 13, =\_\mathrm{E}$
15.	$A[i] \geq A[k_g]$	$14,$ algebra
16.	$k_g = i \Rightarrow A[i] \geq A[k_g]$	$12-15, \Rightarrow\_\mathrm{I}$
17.	$\neg(A[i] \geq A[k_g])$	assumption
18.	$\neg(1 \leq k_g \leq i-1)$	$11, 17, \Rightarrow\_\mathrm{I}$
19.	$\neg(k_g = i)$	$16, 17, \Rightarrow\_\mathrm{I}$
20.	$k_g = i$	$6, 18, \vee\_\mathrm{E}$
21.	**false**	$19, 20, \neg\_\mathrm{E}$
22.	$\neg\neg(A[i] \geq A[k_g])$	$17-21, \neg\_\mathrm{I}$
23.	$A[i] \geq A[k_g]$	$22, \neg\_\mathrm{E}$
24.	$1 \leq k_g \leq i \Rightarrow A[i] \geq A[k_g]$	$5-23, \Rightarrow\_\mathrm{I}$
25.	$(\forall k \bullet 1 \leq k \leq i \Rightarrow A[i] \geq A[k])$	$4-24, \forall\_\mathrm{I}$
26.	(line 1) $\Rightarrow$ (line 25)	$1-25, \Rightarrow\_\mathrm{I}$

Proof of implied condition (3):

$$\begin{array}{ll} & (\forall k \bullet 1 \leq k \leq i-1 \Rightarrow max \geq A[k]) \land \neg(A[i] > max) \\ \Rightarrow & \forall k \bullet 1 \leq k \leq i \Rightarrow max \geq A[k] \end{array}$$

1.	$(\forall k \bullet 1 \leq k \leq i-1 \Rightarrow max \geq A[k]) \land \neg(A[i] > max)$	assumption
2.	$\forall k \bullet 1 \leq k \leq i-1 \Rightarrow max \geq A[k]$	$1, \land$_E
3.	$\neg(A[i] > max)$	$1, \land$_E
4.	k_g	
5.	$1 \leq k_g \leq i$	assumption
6.	$1 \leq k_g \leq i-1 \lor k_g = i$	algebra
7.	$1 \leq k_g \leq i-1 \Rightarrow max \geq A[k_g]$	$2, \forall$_E
8.	$k_g = i$	assumption
9.	$A[i] = A[i]$	$=$_I
10.	$A[i] = A[k_g]$	$8, 9, =$_E
11.	$A[i] \geq A[k_g]$	10, algebra
12.	$max \geq A[i]$	3, algebra
13.	$max \geq A[k_g]$	11, 12, algebra
14.	$k_g = i \Rightarrow max \geq A[k_g]$	$8-13, \Rightarrow$_I
15.	$\neg(max \geq A[k_g])$	assumption
16.	$\neg(1 \leq k_g \leq i-1)$	$7, 15, \Rightarrow$_I
17.	$\neg(k_g = i)$	$14, 15, \Rightarrow$_I
18.	$k_g = i$	$6, 16, \lor$_E
19.	**false**	$17, 18, \neg$_E
20.	$\neg\neg(A[i] \geq A[k_g])$	$15-19, \neg$_I
21.	$A[i] \geq A[k_g]$	$20, \neg$_E
22.	$1 \leq k_g \leq i \Rightarrow max \geq A[k_g]$	$5-21, \Rightarrow$_I
23.	$(\forall k \bullet 1 \leq k \leq i \Rightarrow max \geq A[k])$	$4-22, \forall$_I
24.	(line 1) $\Rightarrow$ (line 23)	$1-23, \Rightarrow$_I