CS 330 (Fall 2013), Professor: Carlotta Domeniconi

Quiz 5 Solutions

Student's name:

1. [100 points]

Consider the following pseudo-code. Assume n is an integer, and $n \geq 0$ at the beginning of its execution.

$i \leftarrow 0;$
$z \leftarrow 3;$
while $(i < n)$ do
    $i \leftarrow i + 1$
    $z \leftarrow z * z$

(1) State the loop invariant.

$$(z = 3^{2^i}) \wedge (i \leq n) \tag{1}$$

(2) Prove the loop invariant.

We need to show:

$$(z = 3^{2^i}) \wedge (i \leq n) \wedge (i < n)\{i \leftarrow i + 1; z \leftarrow z \times z\}(z = 3^{2^i}) \wedge (i \leq n) \tag{2}$$

We use the sequence rule:

$$(z = 3^{2^i}) \wedge (i \leq n) \wedge (i < n)\{i \leftarrow i + 1\}(z = 3^{2^{i-1}}) \wedge (i \leq n)$$

$$(z = 3^{2^{i-1}}) \wedge (i \leq n)\{z \leftarrow z \times z\}(z = 3^{2^{i-1}} \times 3^{2^{i-1}} = 3^{2^{i-1}+2^{i-1}} = 3^{2^i}) \wedge (i \leq n)$$

By the sequence rule, the invariant in (1) is proved.

(3) Apply the loop invariant.

By applying the while loop, from (2) we obtain:

$$(z = 3^{2^i}) \wedge (i \leq n)\{\text{while } (i < n) \text{ do } i \leftarrow i + 1; z \leftarrow z \times z\}(z = 3^{2^i}) \wedge (i \leq n) \wedge (i \geq n)$$

Thus, at the end of the execution of the given code, we have:

$(i \leq n) \wedge (i \geq n)$, which implies $i = n$. Combined with $z = 3^{2^i}$, this gives $z = 3^{2^n}$.