CSC236 QUIZ 6, TUESDAY JULY 5

Name: Student number:

Consider the method `seventeenTicker`, below. Prove the following loop invariant holds given the precondition:

$P(i)$ "If there are i iterations of the loop, then $17q_i + r_i \leq t$ and $r_i \leq 16$. If there are $i+1$ iterations of the loop, then $17q_i + r_i < 17q_{i+1} + r_{i+1}$." Then $\forall i \in \mathbb{N}, P(i)$.

Explain how to use $P(i)$ to show that `seventeenTicker` correct with respect to its precondition/postcondition. You may assume that the java type `int` is the same as the integers.

PROOF (INDUCTION ON i): If $i = 0$, then $P(i)$ asserts that $17q_i + r_i = 17(0) + 0 \leq t$ (true, since by the precondition $t \geq 0$), that $r_i \leq 16$ (true, since $r_0 = 0$), and if there is an $(i+1)th$ loop iteration, then $17q_i + r_i = 0 < 17q_{i+1} + r_{i+1} = 17(0) + 1$, which is true, since $0 < 1$. Thus the base case holds.

INDUCTION STEP: Assume that $P(i)$ holds for some arbitrary $i \in \mathbb{N}$. I wish to show that this implies $P(i+1)$. If there is no $(i+1)th$th iteration of the loop, then $P(i+1)$ holds vacuously. Otherwise, by the IH, $17q_i + r_i \leq t$, and (since there is another iteration) $17q_i + r_i \neq t$, so $17q_i + r_i < t$. This means that $17q_i + r_i + 1 \leq t$. Consider two cases:

CASE 1, $r_i < 16$: In this case the "$(r < 16)$" branch is executed, so $r_{i+1} = r_i + 1$, $q_{i+1} = q_i$, so $17q_i + r_i < 17q_i + r_i + 1 = 17q_{i+1} + r_{i+1} \leq t$. Also, $r_{i+1} \leq 16$, since $r_i < 16$.

CASE 2, $r_i \geq 16$: By the IH, $r_i \leq 16$, so this implies $r_i = 16$. In this case the "$(r < 16)$ else" branch is executed, and $r_{i+1} = 0$, $q_{i+1} = q_i + 1$, so $17q_i + r_i < 17q_i + r_i + 1 = 17(q_i + 1) + r_i - 16 = 17q_{i+1} + r_{i+1} \leq t$. Also, $r_{i+1} = 0 \leq 16$.

In both cases $17q_{i+1} + r_{i+1} \leq t$ and $r_{i+1} \leq 16$, as claimed. Furthermore, if there is an $(i+2)$th iteration of the loop, then there are two cases to consider:

CASE 1, $r_{i+1} < 16$: In this case the "$(r < 16)$" branch is executed, so $q_{i+2} = q_{i+1}$ and $r_{i+2} = r_{i+1} + 1$. Thus $17q_{i+2} + r_{i+2} = 17q_{i+1} + r_{i+1} + 1 > 17q_{i+1} + r_{i+1}$, as wanted.

CASE 2, $r_{i+1} \geq 16$: In this case the "$(r < 16)$ else" branch is executed, so $q_{i+2} = q_{i+1} + 1$ and $r_{i+2} = 0$. Thus $17q_{i+2} + r_{i+2} = 17q_{i+1} + 17 + 0 = 17q_{i+1} + r_{i+1} + 1$ (since we showed above that $r_{i+1} \leq 16$, so in this case it must equal 16).

In all cases we have $P(i+1)$, so $P(i) \Rightarrow P(i+1)$, as wanted.

I concluded that $P(i)$ is true for all $i \in \mathbb{N}$.

Loop invariant $P(i)$ shows that the sequence $\langle t - (17q_i + r_i) \rangle$ is non-negative and strictly decreasing. Since the sequence involves sums, differences, and multiples of integers, each term is an integer. Thus it is a strictly decreasing sequence of natural numbers, hence finite (by PWO) — there is some last term k. Thus there is no $(k+1)$th iteration of the loop, and the loop terminates.