Supplemental Document for Reading #3

A Useful Theorem about `while` Loops

The following theorem was stated, as "Loop Theorem #1", in the notes for Reading #3.

Theorem (First Loop Theorem): Consider an algorithm, for a given computational problem, with a `while` loop

```
while (t) {
  S
}
```

and an assertion $\mathcal{A}$. If

(a) an execution of the loop test `t` has no side-effects — that is, does not change the value of any inputs, variables, or global data,

(b) $\mathcal{A}$ is satisfied whenever the loop is reached, during an execution of the algorithm starting with the problem's precondition being satisfied, and

(c) if $\mathcal{A}$ is satisfied at the beginning of any execution of the loop body `S` (when the problem's precondition was satisfied when execution of the algorithm started) then $\mathcal{A}$ is satisfied, once again, when this execution of the loop body ends,

then $\mathcal{A}$ is a loop invariant for this `while` loop.

Proof: Consider an execution of the algorithm that begins with the problem's precondition initially being satisfied.

In order to show that $\mathcal{A}$ is a loop invariant for the `while` loop mentioned in the claim, it is necessary and sufficient to show that this assertion is satisfied

i. at the ***beginning*** of every execution of this loop,

ii. at the ***beginning*** of every execution of the body of this loop,

iii. at the ***end*** of every execution of the body of this loop, and

iv. at the ***end*** of every execution of this loop.

With that noted, consider an execution of this algorithm when its problem's precondition is initially satisfied.

It follows by property (b), in the claim, that the assertion $\mathcal{A}$ is satisfied at the beginning of every execution of the `while` loop that is part of this execution of the algorithm — that is, at time (i) as listed above.

In order to establish that $\mathcal{A}$ is also satisfied at times (ii) and (iii), above, consider the following

Subclaim: Consider the computational problem, algorithm, and assertion $\mathcal{A}$ mentioned in the claim of the "First Loop Theorem". Consider, as well, an execution of this algorithm when the problem's precondition is initially satisfied.

If ℓ is a positive integer such that the loop body is executed at least ℓ times, during an execution of this `while` loop, then $\mathcal{A}$ is satisfied at both the beginning and end of this ℓ^{th} execution of the loop body.

Proof of Subclaim: The subclaim will be proved by induction on ℓ. The standard form of mathematical induction will be used.

Basis ($\ell = 1$): Suppose that there is at least $\ell = 1$ execution of the body of the `while` loop that is part of execution of this `while` loop, during this execution of the algorithm.

As noted above, $\mathcal{A}$ is satisfied at the beginning of this execution of the `while` loop. Since an execution of the loop test `t` does not change the values of any inputs, variables or global data, the assertion $\mathcal{A}$ is also satisfied after `t` is checked — that is, at the beginning of the first execution of the loop body.

It now follows by property (c), given in the subclaim, that assertion $\mathcal{A}$ is also satisfied at the end of the first execution of the body of the `while` loop — as needed to establish the subclaim when $\ell = 1$.

Inductive Step: Let k be an integer such that $k \geq 1$. It is necessary and sufficient to use the following

> Inductive Hypothesis: Consider the algorithm and computational problem mentioned in the claim, and the `while` loop included in this algorithm. If the body of the `while` loop is executed at least k times, during some execution of the loop, then assertion $\mathcal{A}$ is satisfied at both the beginning and the end of the k^{th} execution of the loop body.

to prove the following

> Inductive Claim: Consider the algorithm and computational problem mentioned in the claim, and the `while` loop included in this algorithm. If the body of the `while` loop is executed at least $k + 1$ times, during some execution of the loop, then assertion $\mathcal{A}$ is satisfied at both the beginning and the end of the $k + 1^{\text{st}}$ execution of the loop body.

With that noted, suppose that the loop body is executed at least $k + 1$ times (during the conditions described in the subclaim): The Inductive Claim is trivially true otherwise.

Then it is certainly true that the loop body has been executed at least k times under the conditions described in the subclaim, and it follows by the Inductive Hypothesis that assertion $\mathcal{A}$ is satisfied at both the beginning and the end of the k^{th} execution of the body of the `while` loop.

Since the loop test `t` does not change any inputs, variables, or global data (by property (a)), it follows that assertion $\mathcal{A}$ is also satisfied at the beginning of the $k + 1^{\text{st}}$ execution of the body of the `while` loop.

It follows by property (c) that the assertion is also satisfied at the end of the $k + 1^{\text{st}}$ execution of the body of the `while` loop, as needed to establish the Inductive Claim — completing the inductive step, and the proof of the subclaim. □

Since every execution of the loop body is the k^{th} execution, for some positive integer k, it now follows that the assertion is satisfied at both the beginning and end of every execution of the body of the `while` loop, that is, at times (ii) and (iii) as listed in the claim.

Suppose, now, that the loop is reached, but the loop test `t` is checked and fails. As noted above, assertion $\mathcal{A}$ holds immediately before this and, since an execution of test `t` does not change the value of any inputs, variables or global data, assertion $\mathcal{A}$ is also satisfied afterwards, so that this assertion is satisfied at the end of the execution of the loop — at time (iv) — in this case.

On the other hand, if the loop test is passed when first checked, and this execution of the loop eventually ends, then it must do so after the k^{th} execution of the loop body for some positive integer k. It follows by the above subclaim that assertion $\mathcal{A}$ is satisfied immediately after this final execution of the loop body. Since an execution of the loop test `t` does not change the value of any inputs, variables or global data, assertion $\mathcal{A}$ is also satisfied at the end of the loop — that is, at time (iv) — as needed to complete the proof of the claim. □