130 (rolling)

(a) Can we always unroll a loop? If $S \Leftarrow A.\,S.\,Z$, can we conclude $S \Leftarrow A.\,A.\,S.\,Z.\,Z$?

(b) Can we always roll up a loop? If $S \Leftarrow A.\,A.\,S.\,Z.\,Z$, can we conclude $S \Leftarrow A.\,S.\,Z$?

After trying the question, scroll down to the solution.

(a) Can we always unroll a loop? If $S \Leftarrow A.\,S.\,Z$, can we conclude $S \Leftarrow A.\,A.\,S.\,Z.\,Z$?

§ Yes, by Stepwise Refinement, and transitivity. Here is a proof.

$(S \Leftarrow A.\,S.\,Z)$ idempotence

$=\ (S \Leftarrow A.\,S.\,Z) \wedge (S \Leftarrow A.\,S.\,Z)$ context, monotonicity of .

$\Rightarrow\ (S \Leftarrow A.\,(A.\,S.\,Z).\,Z) \wedge (S \Leftarrow A.\,S.\,Z)$ specialize

$\Rightarrow\ (S \Leftarrow A.\,A.\,S.\,Z.\,Z)$

There are many more kinds of loops than the one in this question. As long as the recursion(s) occur(s) in monotonic context(s), the answer is yes. In programs, all calls are in monotonic contexts.

(b) Can we always roll up a loop? If $S \Leftarrow A.\,A.\,S.\,Z.\,Z$, can we conclude $S \Leftarrow A.\,S.\,Z$?

§ No. Let x be an integer variable, let $A = ok$, let $S = even\ x'$, and let $Z = x{:=}\ x{+}1$. Then

$(S \Leftarrow A.\,A.\,S.\,Z.\,Z)$

$=\ (even\ x' \Leftarrow ok.\ ok.\ even\ x'.\ x{:=}\ x{+}1.\ x{:=}\ x{+}1)$

$=\ \top$

But

$(S \Leftarrow A.\,S.\,Z)$

$=\ (even\ x' \Leftarrow ok.\ even\ x'.\ x{:=}\ x{+}1)$

$=\ \bot$