170 Let s and n be *nat* variables. Here is a refinement.

$$s' = s + 2^n - 1 \quad \Leftarrow \quad \mathbf{if}\ n{=}0\ \mathbf{then}\ ok\ \mathbf{else}\ n{:=}\ n{-}1.\ \ s{:=}\ s + 2^n.\ \ s' = s + 2^n - 1\ \mathbf{fi}$$

(a) Prove it.

(b) Insert appropriate time increments according to the recursive measure, and write appropriate timing specifications.

(c) Prove the timing refinement.

After trying the question, scroll down to the solution.

(a) Prove it.

§ By cases. First case:

$$(s' = s + 2^n - 1 \ \Leftarrow\ n{=}0 \wedge ok) \qquad \text{expand } ok$$
$$= \quad (s' = s + 2^n - 1 \ \Leftarrow\ n{=}0 \wedge s'{=}s \wedge n'{=}n) \qquad \text{context}$$
$$= \quad (s = s + 2^0 - 1 \ \Leftarrow\ n{=}0 \wedge s'{=}s \wedge n'{=}n) \qquad \text{simplify and specialize}$$
$$\Rightarrow \quad \top$$

Last case, right side:

$$n{\ne}0 \wedge (n{:=}\ n{-}1.\ \ s{:=}\ s + 2^n.\ \ s' = s + 2^n - 1) \qquad \text{substitution law twice}$$
$$= \quad n{\ne}0 \wedge s' = s + 2^{n-1} + 2^{n-1} - 1 \qquad \text{simplify and specialize}$$
$$\Rightarrow \quad s' = s + 2^n - 1$$

(b) Insert appropriate time increments according to the recursive measure, and write appropriate timing specifications.

§ $t' = t{+}n \ \Leftarrow\ \textbf{if } n{=}0 \textbf{ then } ok \textbf{ else } n{:=}\ n{-}1.\ \ s{:=}\ s + 2^n.\ \ t{:=}\ t{+}1.\ \ t' = t{+}n \textbf{ fi}$

(c) Prove the timing refinement.

§ By cases. First case:

$$(t' = t{+}n \ \Leftarrow\ n{=}0 \wedge ok) \qquad \text{expand } ok$$
$$= \quad (t' = t{+}n \ \Leftarrow\ n{=}0 \wedge s'{=}s \wedge n'{=}n \wedge t'{=}t) \qquad \text{context}$$
$$= \quad (t = t{+}0 \ \Leftarrow\ n{=}0 \wedge s'{=}s \wedge n'{=}n \wedge t'{=}t) \qquad \text{simplify and specialize}$$
$$\Rightarrow \quad \top$$

Last case, right side:

$$n{\ne}0 \wedge (n{:=}\ n{-}1.\ \ s{:=}\ s + 2^n.\ \ t{:=}\ t{+}1.\ \ t' = t{+}n) \qquad \text{substitution law 3 times}$$
$$= \quad n{\ne}0 \wedge t' = t{+}1 + n{-}1 \qquad \text{simplify and specialize}$$
$$\Rightarrow \quad t' = t{+}n$$