291 Let k be a natural constant, and let x and n be natural variables. Suppose one unit of space is allocated before each recursive call (for the return address), and freed after the call. Find and prove a maximum space bound for the refinement

$$P \Leftarrow \textbf{if } n=0 \textbf{ then } x:=0 \textbf{ else } n:=n-1.\ P.\ x:=x+k \textbf{ fi}$$

After trying the question, scroll down to the solution.

§ Adding space variable s and maximum space variable m ,

$$P \Leftarrow \textbf{if } n{=}0 \textbf{ then } x{:=}\ 0$$
$$\textbf{else } n{:=}\ n{-}1.\ \ s{:=}\ s{+}1.\ \ m{:=}\ m{\uparrow}s.\ \ P.\ \ s{:=}\ s{-}1.\ \ x{:=}\ x{+}k \textbf{ fi}$$

and define $P = s \le m \le s{+}n \Rightarrow m' = s{+}n$. Proof by cases. First case:

$$(s \le m \le s{+}n \Rightarrow m' = s{+}n \Leftarrow n{=}0 \wedge (x{:=}\ 0)) \qquad \text{portation}$$
$$= n{=}0 \wedge (x{:=}\ 0) \wedge s \le m \le s{+}n \Rightarrow m' = s{+}n \qquad \text{assignment}$$
$$= n{=}0 \wedge x'{=}0 \wedge n'{=}n \wedge s'{=}s \wedge m'{=}m \wedge s \le m \le s{+}n \Rightarrow m' = s{+}n$$
context $n{=}0$ in $s \le m \le s{+}n$
$$= n{=}0 \wedge x'{=}0 \wedge n'{=}n \wedge s'{=}s \wedge m'{=}m \wedge s{=}m \Rightarrow m' = s{+}n$$
context $n{=}0 \wedge m'{=}m \wedge s{=}m$ in $m' = s{+}n$
$$= n{=}0 \wedge x'{=}0 \wedge n'{=}n \wedge s'{=}s \wedge m'{=}m \wedge s{=}m \Rightarrow m{=}m \qquad \text{reflexivity}$$
$$= n{=}0 \wedge x'{=}0 \wedge n'{=}n \wedge s'{=}s \wedge m'{=}m \wedge s{=}m \Rightarrow \top \qquad \text{base}$$
$$= \top$$

Last case:

$$(\quad s \le m \le s{+}n \Rightarrow m' = s{+}n$$
$$\Leftarrow n{\ne}0 \wedge (n{:=}\ n{-}1.\ \ s{:=}\ s{+}1.\ \ m{:=}\ m{\uparrow}s.\ \ s \le m \le s{+}n \Rightarrow m' = s{+}n.$$
$$s{:=}\ s{-}1.\ \ x{:=}\ x{+}k)) \qquad \text{substitution 3 times}$$

$$= (\quad s \le m \le s{+}n \Rightarrow m' = s{+}n$$
$$\Leftarrow n{\ne}0 \wedge (s{+}1 \le m{\uparrow}(s{+}1) \le s{+}1{+}n{-}1 \Rightarrow m' = s{+}1{+}n{-}1.$$
$$s{:=}\ s{-}1.\ \ x{:=}\ x{+}k)) \qquad \text{arithmetic}$$

$$= (\quad s \le m \le s{+}n \Rightarrow m' = s{+}n$$
$$\Leftarrow n{\ne}0 \wedge (s{+}1 \le m{\uparrow}(s{+}1) \le s{+}n \Rightarrow m' = s{+}n.$$
$$s{:=}\ s{-}1.\ \ x{:=}\ x{+}k)) \qquad \text{sequential composition twice}$$

$$= (\quad s \le m \le s{+}n \Rightarrow m' = s{+}n$$
$$\Leftarrow n{\ne}0 \wedge (s{+}1 \le m{\uparrow}(s{+}1) \le s{+}n \Rightarrow m' = s{+}n)) \qquad \text{portation}$$

$$= s \le m \le s{+}n \wedge n{\ne}0 \wedge (s{+}1 \le m{\uparrow}(s{+}1) \le s{+}n \Rightarrow m' = s{+}n) \Rightarrow m' = s{+}n$$
$s{+}1 \le m{\uparrow}(s{+}1)$ and in context $n{\ne}0$ we have $s{+}1 \le s{+}n$
$$= s \le m \le s{+}n \wedge n{\ne}0 \wedge (m \le s{+}n \Rightarrow m' = s{+}n) \Rightarrow m' = s{+}n \qquad \text{context and identity}$$
$$= s \le m \le s{+}n \wedge n{\ne}0 \wedge m' = s{+}n \Rightarrow m' = s{+}n \qquad \text{specialize}$$
$$= \top$$