147 Let x be an integer variable, and let t be the time variable. Find the strongest implementable time specification P such that

$$P \Leftarrow \textbf{if } x=0 \textbf{ then } ok \textbf{ else } x:= x+1.\ t:= t+1.\ P \textbf{ fi}$$

and prove the refinement.

After trying the question, scroll down to the solution.

§ $$P \;=\; (x\le 0 \;\Rightarrow\; t' = t-x) \land (x>0 \Rightarrow t'=\infty)$$
$$=\; x\le 0 \;\land\; t' = t-x \;\lor\; x>0 \land t'=\infty$$
$$=\; \textbf{if } x\le 0 \textbf{ then } t' = t-x \textbf{ else } t'=\infty \textbf{ fi}$$

Proof, using the first form, using refinement by cases and parts:

$$\begin{array}{lll}
 & (x\le 0 \;\Rightarrow\; t' = t-x \;\;\Longleftarrow\;\; x=0 \land ok) & \text{expand } ok \\
= & (x\le 0 \;\Rightarrow\; t' = t-x \;\;\Longleftarrow\;\; x=0 \land x'=x \land t'=t) & \text{context} \\
= & (0\le 0 \;\Rightarrow\; t = t-0 \;\;\Longleftarrow\;\; x=0 \land x'=x \land t'=t) & \text{arithmetic, reflexivity, base} \\
= & \top &
\end{array}$$

$$\begin{array}{lll}
 & (x\le 0 \;\Rightarrow\; t' = t-x \;\;\Longleftarrow\;\; x\ne 0 \land (x:= x+1.\;\; t:= t+1.\;\; x\le 0 \;\Rightarrow\; t' = t-x)) & \text{substitution} \\
= & (x\le 0 \;\Rightarrow\; t' = t-x \;\;\Longleftarrow\;\; x\ne 0 \land (x+1\le 0 \;\Rightarrow\; t' = (t+1)-(x+1))) & \text{portation and arith} \\
= & x\ne 0 \land x\le 0 \land (x+1\le 0 \;\Rightarrow\; t' = t-x) \Rightarrow\; t' = t-x & x \text{ is integer} \\
= & x<0 \land (x<0 \;\Rightarrow\; t' = t-x) \Rightarrow\; t' = t-x & \text{discharge} \\
= & x<0 \land t' = t-x \;\Rightarrow\; t' = t-x & \text{specialize} \\
= & \top &
\end{array}$$

$$\begin{array}{lll}
 & (x>0 \Rightarrow t'=\infty \;\;\Longleftarrow\;\; x=0 \land ok) & \text{context} \\
= & (0>0 \Rightarrow t'=\infty \;\;\Longleftarrow\;\; x=0 \land ok) & \text{arithmetic, base, base} \\
= & \top &
\end{array}$$

$$\begin{array}{lll}
 & (x>0 \Rightarrow t'=\infty \;\;\Longleftarrow\;\; x\ne 0 \land (x:= x+1.\;\; t:= t+1.\;\; x>0 \Rightarrow t'=\infty)) & \text{substitution} \\
= & (x>0 \Rightarrow t'=\infty \;\;\Longleftarrow\;\; x\ne 0 \land (x+1>0 \Rightarrow t'=\infty)) & \text{portation} \\
= & x>0 \land x\ne 0 \land (x+1>0 \Rightarrow t'=\infty) \Rightarrow t'=\infty & x \text{ is integer} \\
= & x>0 \land (x\ge 0 \Rightarrow t'=\infty) \Rightarrow t'=\infty & \text{discharge} \\
= & x>0 \land t'=\infty \Rightarrow t'=\infty & \text{specialize} \\
= & \top &
\end{array}$$