323 Let P: $nat \rightarrow bin$.

(a) Define quantifier $\Downarrow$ so that $\Downarrow m$: $nat \cdot P\ m$ is the smallest natural m such that $P\ m$, and ∞ if there is none.

(b) Prove $n := \Downarrow m$: $nat \cdot P\ m \ \Leftarrow\ n := 0.$ **while** $\neg\ P\ n$ **do** $n := n+1$ **od** .

After trying the question, scroll down to the solution.

(a) Define quantifier ⤋ so that $\text{⤋}m\text{: }nat\cdot\ P\ m$ is the smallest natural m such that $P\ m$, and ∞ if there is none.

§
$$\text{⤋}m\text{: }nat\cdot\ P\ m \;=\; \Downarrow n\text{: }(\S m\text{: }nat\cdot\ P\ m)\cdot\ n$$
$$=\; \Downarrow n\text{: }nat\cdot\ \mathbf{if}\ P\ n\ \mathbf{then}\ n\ \mathbf{else}\ \infty\ \mathbf{fi}$$

(b) Prove $n\text{:= }\text{⤋}m\text{: }nat\cdot\ P\ m \;\Leftarrow\; n\text{:= }0.\ \ \mathbf{while}\ \neg\ P\ n\ \mathbf{do}\ n\text{:= }n{+}1\ \mathbf{od}$.

§ I suppose n is the only variable, and I prove two refinements:

$$n\text{:= }\text{⤋}m\text{: }nat\cdot\ P\ m \;\Leftarrow\; n\text{:= }0.\ \ n\text{:= }\text{⤋}m\text{: }nat{+}n\cdot\ P\ m$$
$$n\text{:= }\text{⤋}m\text{: }nat{+}n\cdot\ P\ m \;\Leftarrow$$
$$\mathbf{if}\ \neg\ P\ n\ \mathbf{then}\ n\text{:= }n{+}1.\ \ n\text{:= }\text{⤋}m\text{: }nat{+}n\cdot\ P\ m\ \mathbf{else}\ ok\ \mathbf{fi}$$

Proof of first refinement is substitution law. Proof of last refinement, in two cases. First case:

$\quad \neg\ P\ n \wedge (n\text{:= }n{+}1.\ \ n\text{:= }\text{⤋}m\text{: }nat{+}n\cdot\ P\ m)$ — expand assignment and substitution

$=\quad \neg\ P\ n\ \wedge\ n' = \text{⤋}m\text{: }nat{+}n{+}1\cdot\ P\ m$ — Since $\neg\ P\ n$ we can increase the domain of ⤋

$=\quad \neg\ P\ n\ \wedge\ n' = \text{⤋}m\text{: }nat{+}n\cdot\ P\ m$ — use assignment form, and specialize

$\Longrightarrow\quad n\text{:= }\text{⤋}m\text{: }nat{+}n\cdot\ P\ m$

Last refinement last case:

$\quad P\ n\ \wedge\ ok$ — expand ok

$=\quad P\ n\ \wedge\ n'{=}n$ — $P\ n\ \Rightarrow\ (\text{⤋}m\text{: }nat{+}n\cdot\ P\ m){=}n$

$=\quad P\ n\ \wedge\ n' = \text{⤋}m\text{: }nat{+}n\cdot\ P\ m$ — use assignment form, and specialize

$\Longrightarrow\quad n\text{:= }\text{⤋}m\text{: }nat{+}n\cdot\ P\ m$

Although the question didn't ask for execution time, the recursive time is

$$t' = t + \text{⤋}m\text{: }nat\cdot\ P\ m$$