252 (McCarthy's 91 problem) Let i be an integer variable. Let

$$M \;=\; \textbf{if } i>100 \textbf{ then } i:= i-10 \textbf{ else } i:= 91 \textbf{ fi}$$

(a) Prove $M \Leftarrow \textbf{if } i>100 \textbf{ then } i:= i-10 \textbf{ else } i:= i+11.\ M.\ M \textbf{ fi}$.

(b) Find the execution time of M as refined in part (a).

After trying the question, scroll down to the solution.

(a) Prove $M \Leftarrow \textbf{if } i>100 \textbf{ then } i:= i-10 \textbf{ else } i:= i+11.\ M.\ M \textbf{ fi}$.

§ by cases. First case:

$i>100 \land (i:= i-10)$ generalization

$\Rightarrow\ i>100 \land (i:= i-10)\ \lor\ i\le 100 \land (i:= 91)$ case analysis

$=\ M$

Last case:

$i\le 100 \land (i:= i+11.\ M.\ M)$ expand first M

$=\ i\le 100 \land (i:= i+11.\ \textbf{if } i>100 \textbf{ then } i:= i-10 \textbf{ else } i:= 91 \textbf{ fi}.\ M)$ distribute M

$=\ i\le 100 \land (i:= i+11.\ \textbf{if } i>100 \textbf{ then } i:= i-10.\ M \textbf{ else } i:= 91.\ M \textbf{ fi})$

expand M twice, expand the assignments within each M

$=\ i\le 100 \land (i:= i+11.\ \textbf{if } i>100 \textbf{ then } i:= i-10.\ \textbf{if } i>100 \textbf{ then } i' = i-10 \textbf{ else } i'=91 \textbf{ fi}$
$\textbf{else } i:= 91.\ \textbf{if } i>100 \textbf{ then } i' = i-10 \textbf{ else } i'=91 \textbf{ fi fi})$

substitution law twice

$=\ i\le 100 \land (i:= i+11.\ \textbf{if } i>100 \textbf{ then if } i>110 \textbf{ then } i' = i-20 \textbf{ else } i'=91 \textbf{ fi}$
$\textbf{else if } \bot \textbf{ then } i'=81 \textbf{ else } i'=91 \textbf{ fi fi})$ simplify **if**s

$=\ i\le 100 \land (i:= i+11.\ \textbf{if } i>110 \textbf{ then } i' = i-20 \textbf{ else } i'=91 \textbf{ fi})$ substitution law

$=\ i\le 100 \land \textbf{if } i>99 \textbf{ then } i' = i-9 \textbf{ else } i'=91 \textbf{ fi}$ use context

$=\ i\le 100 \land \textbf{if } i=100 \textbf{ then } i'=91 \textbf{ else } i'=91 \textbf{ fi}$ case idempotent

$=\ i\le 100 \land i'=91$ generalization

$\Rightarrow\ i>100 \land (i:= i-10)\ \lor\ i\le 100 \land (i:= 91)$ case analysis

$=\ M$

(b) Find the execution time of M as refined in part (a).

§ It is enough to add a single time increment before the first call, although it would not be wrong to add another before the last call.

$T \Leftarrow \textbf{if } i>100 \textbf{ then } i:= i-10 \textbf{ else } i:= i+11.\ t:= t+1.\ T.\ T \textbf{ fi}$

It isn't obvious to me what the timing specification T should be, so I executed the program and found $\textbf{if } i>100 \textbf{ then } t'=t \textbf{ else } t'=t+101-i \textbf{ fi}$. I also found that, although the case $i>100$ can be easily proven by itself,

$i>100 \land (i:= i-10)$ generalization

$\Rightarrow\ i>100 \land (i:= i-10)\ \lor\ i\le 100 \land t'=t+101-i$ expand assignment and drop a conjunct

$\Rightarrow\ i>100 \land t'=t\ \lor\ i\le 100 \land t'=t+101-i$ case analysis

$=\ \textbf{if } i>100 \textbf{ then } t'=t \textbf{ else } t'=t+101-i \textbf{ fi}$

the last case $i\le 100$ cannot, and requires the $i>100$ case. I start with the right side of the refinement.

$\textbf{if } i>100 \textbf{ then } i:= i-10$
$\textbf{else}\quad i:= i+11.\ t:= t+1.$
$\quad \textbf{if } i>100 \textbf{ then } t'=t \textbf{ else } t'=t+101-i \textbf{ fi}.$
$\quad \textbf{if } i>100 \textbf{ then } t'=t \textbf{ else } t'=t+101-i \textbf{ fi fi}$

Now I see that the timing specification isn't strong enough because the first call forgets the value of i which is still needed for the second call. So I strengthen it, and define T as

$T = \textbf{if } i>100 \textbf{ then } i:= i-10 \textbf{ else } t:= t+101-i.\ i:= 91 \textbf{ fi}$

and now prove the refinement. Starting with the right side

$\textbf{if } i>100 \textbf{ then } i:= i-10$
$\textbf{else}\quad i:= i+11.\ t:= t+1.$
$\quad \textbf{if } i>100 \textbf{ then } i:= i-10 \textbf{ else } t:= t+101-i.\ i:= 91 \textbf{ fi}.$
$\quad \textbf{if } i>100 \textbf{ then } i:= i-10 \textbf{ else } t:= t+101-i.\ i:= 91 \textbf{ fi fi}$

expand the assignments of the final **if** ,
and distribute the final **if** into the preceding **if**

$=\ \textbf{if } i>100 \textbf{ then } i:= i-10$
$\textbf{else}\quad i:= i+11.\ t:= t+1.$

$$
\begin{array}{lll}
& & \textbf{if } i{>}100 \\
& & \textbf{then } i{:=}\ i{-}10.\ \ \textbf{if } i{>}100 \textbf{ then } i'{=}i{-}10 \land t'{=}t \textbf{ else } i'{=}91 \land t'{=}t{+}101{-}i \textbf{ fi} \\
& & \textbf{else } t{:=}\ t{+}101{-}i.\ \ i{:=}\ 91.\quad \textbf{if } i{>}100 \textbf{ then } i'{=}i{-}10 \land t'{=}t \\
& & \qquad\qquad\qquad\qquad\quad \textbf{else } i'{=}91 \land t'{=}t{+}101{-}i \textbf{ fi fi} \qquad \text{subst law 3 times} \\
= & \textbf{if } i{>}100 \textbf{ then } i{:=}\ i{-}10 & \\
& \textbf{else} & i{:=}\ i{+}11.\ \ t{:=}\ t{+}1. \\
& & \textbf{if } i{>}100 \\
& & \textbf{then if } i{>}110 \textbf{ then } i'{=}i{-}20 \land t'{=}t \textbf{ else } i'{=}91 \land t'{=}t{+}111{-}i \textbf{ fi} \\
& & \textbf{else if } \bot \textbf{ then } i'{=}81 \land t'{=}t{+}101{-}i \textbf{ else } i'{=}91 \land t'{=}t{+}111{-}i \textbf{ fi fi} \quad \text{simplify } \textbf{if}\text{s} \\
= & \textbf{if } i{>}100 \textbf{ then } i{:=}\ i{-}10 & \\
& \textbf{else} & i{:=}\ i{+}11.\ \ t{:=}\ t{+}1. \\
& & \textbf{if } i{>}110 \textbf{ then } i'{=}i{-}20 \land t'{=}t \textbf{ else } i'{=}91 \land t'{=}t{+}111{-}i \textbf{ fi fi} \qquad \text{subst law 2 times} \\
= & \textbf{if } i{>}100 \textbf{ then } i{:=}\ i{-}10 & \\
& \multicolumn{2}{l}{\textbf{else if } i{>}99 \textbf{ then } i'{=}i{-}9 \land t'{=}t{+}1 \textbf{ else } i'{=}91 \land t'{=}t{+}101{-}i \textbf{ fi fi} \qquad \text{use context}} \\
= & \textbf{if } i{>}100 \textbf{ then } i{:=}\ i{-}10 & \\
& \multicolumn{2}{l}{\textbf{else if } i{=}100 \textbf{ then } i'{=}91 \land t'{=}t{+}101{-}i \textbf{ else } i'{=}91 \land t'{=}t{+}101{-}i \textbf{ fi fi} \quad \text{case idempotent}} \\
= & T &
\end{array}
$$