150 Let x be an integer variable. Let P be a specification refined as follows.

$P \Leftarrow$ **if** $x>0$ **then** $x:= x-2.\ P$
else **if** $x<0$ **then** $x:= x+1.\ P$
else ok **fi** **fi**

(a) Prove the refinement when $P = x'=0$.

(b) Add recursive time and find and prove an upper bound for the execution time.

After trying the question, scroll down to the solution.

(a) Prove the refinement when $P = x'=0$.

§ Using Refinement by Cases, I must prove three things:

$$x'=0 \Leftarrow x>0 \land (x{:=}\ x-2.\ \ x'=0)$$
$$x'=0 \Leftarrow x<0 \land (x{:=}\ x+1.\ \ x'=0)$$
$$x'=0 \Leftarrow x=0 \land ok$$

Let's start with the first.

$x>0 \land (x{:=}\ x-2.\ \ x'=0)$ — use substitution law

$= \ x>0 \land x'=0$ — specialization

$\Rightarrow \ x'=0$

Now the middle one.

$x<0 \land (x{:=}\ x+1.\ \ x'=0)$ — use substitution law

$= \ x<0 \land x'=0$ — specialization

$\Rightarrow \ x'=0$

And the last one.

$x=0 \land ok$ — replace ok

$= \ x=0 \land x'=x$ — transitivity

$\Rightarrow \ x'=0$

(b) Add recursive time and find and prove an upper bound for the execution time.

§ Adding recursive time,

$P \Leftarrow$ **if** $x>0$ **then** $x{:=}\ x-2.\ \ t{:=}\ t+1.\ \ P$
else if $x<0$ **then** $x{:=}\ x+1.\ \ t{:=}\ t+1.\ \ P$
else ok **fi fi**

The exact execution timing specification is

$P = t' = t +$ **if** $x>0$ **then** $ceil(x/2) + 2 - mod\ x\ 2$ **else** $-x$ **fi**

but $ceil$ and mod are awkward functions to deal with, so I'll prove

$P =$ **if** $x>0$ **then** $t' \le t + x/2 + 2$ **else** $t' \le t-x$ **fi**

(I tried re-expressing P as a conjunction

$$P = (x>0 \Rightarrow t' \le t + x/2 + 2) \land (x\le 0 \Rightarrow t' \le t-x)$$

so that I can use Refinement by Parts, but that didn't work. That's because the $x>0$ part may take x to 0 or below, and require the other part.)

Using Refinement by Cases, I must prove three things:

$$P \Leftarrow x>0 \land (x{:=}\ x-2.\ \ t{:=}\ t+1.\ \ P)$$
$$P \Leftarrow x<0 \land (x{:=}\ x+1.\ \ t{:=}\ t+1.\ \ P)$$
$$P \Leftarrow x=0 \land ok$$

Let's start with the first case.

$x>0 \land (x{:=}\ x-2.\ \ t{:=}\ t+1.\ \ P) \Rightarrow P$ — replace first P

$= \ x>0 \land (x{:=}\ x-2.\ \ t{:=}\ t+1.$ **if** $x>0$ **then** $t' \le t + x/2 + 2$ **else** $t' \le t-x$ **fi**$) \Rightarrow P$ — Substitution Law twice

$= \ x>0 \land$ **if** $x-2>0$ **then** $t' \le t + 1 + (x-2)/2 + 2$ **else** $t' \le t+1-(x-2)$ **fi** $\Rightarrow P$ — simplify

$= \ x>0 \land$ **if** $x>2$ **then** $t' \le t + x/2 + 2$ **else** $t' \le t-x+3$ **fi** $\Rightarrow P$ — note that $x>0 = x=1 \lor x=2 \lor x>2$ and then distribute

$= \ \ (x=1 \land$ **if** $x>2$ **then** $t' \le t + x/2 + 2$ **else** $t' \le t-x+3$ **fi** $\Rightarrow P)$ — context

$\land \ (x=2 \land$ **if** $x>2$ **then** $t' \le t + x/2 + 2$ **else** $t' \le t-x+3$ **fi** $\Rightarrow P)$ — context

$\land \ (x>2 \land$ **if** $x>2$ **then** $t' \le t + x/2 + 2$ **else** $t' \le t-x+3$ **fi** $\Rightarrow P)$ — context

$$
\begin{array}{lll}
= & \quad (x{=}1 \;\land\; t' \le t{+}2 \;\Rightarrow\; P) & \text{replace } P \\
& \land\; (x{=}2 \;\land\; t' \le t{+}1 \;\Rightarrow\; P) & \text{replace } P \\
& \land\; (x{>}2 \;\land\; t' \le t + x/2 + 2 \;\Rightarrow\; P) & \text{replace } P \\
= & \quad (x{=}1 \;\land\; t' \le t{+}2 \;\Rightarrow\; \textbf{if } x{>}0 \textbf{ then } t' \le t + x/2 + 2 \textbf{ else } t' \le t{-}x \textbf{ fi}) & \text{context} \\
& \land\; (x{=}2 \;\land\; t' \le t{+}1 \;\Rightarrow\; \textbf{if } x{>}0 \textbf{ then } t' \le t + x/2 + 2 \textbf{ else } t' \le t{-}x \textbf{ fi}) & \text{context} \\
& \land\; (x{>}2 \;\land\; t' \le t + x/2 + 2 \;\Rightarrow\; \textbf{if } x{>}0 \textbf{ then } t' \le t + x/2 + 2 \textbf{ else } t' \le t{-}x \textbf{ fi}) & \text{context} \\
= & \quad (x{=}1 \;\land\; t' \le t{+}2 \;\Rightarrow\; t' \le t + 1/2 + 2) & \text{arithmetic, connection} \\
& \land\; (x{=}2 \;\land\; t' \le t{+}1 \;\Rightarrow\; t' \le t + 2/2 + 2) & \text{arithmetic, connection} \\
& \land\; (x{>}2 \;\land\; t' \le t + x/2 + 2 \;\Rightarrow\; t' \le t + x/2 + 2) & \text{specialization} \\
= & \top &
\end{array}
$$

Now the middle case.

$$
\begin{array}{lll}
& x{<}0 \land (x{:=}\, x{+}1.\;\; t{:=}\, t{+}1.\;\; P) \;\Rightarrow\; P & \text{replace first } P \\
= & x{<}0 \land (x{:=}\, x{+}1.\;\; t{:=}\, t{+}1.\;\; \textbf{if } x{>}0 \textbf{ then } t' \le t + x/2 + 2 \textbf{ else } t' \le t{-}x \textbf{ fi}) \;\Rightarrow\; P & \\
& & \text{Substitution Law twice} \\
= & x{<}0 \land \textbf{if } x{+}1{>}0 \textbf{ then } t' \le t + 1 + (x{+}1)/2 + 2 \textbf{ else } t' \le t{+}1{-}(x{+}1) \textbf{ fi} \;\Rightarrow\; P & \text{simplify} \\
= & x{<}0 \land \textbf{if } x{\ge}0 \textbf{ then } t' \le t + (x{+}1)/2 + 3 \textbf{ else } t' \le t{-}x \textbf{ fi} \;\Rightarrow\; P & \text{context} \\
= & x{<}0 \land t' \le t{-}x \;\Rightarrow\; P & \text{replace } P \\
= & x{<}0 \land t' \le t{-}x \;\Rightarrow\; \textbf{if } x{>}0 \textbf{ then } t' \le t + x/2 + 2 \textbf{ else } t' \le t{-}x \textbf{ fi} & \text{context} \\
= & x{<}0 \land t' \le t{-}x \;\Rightarrow\; t' \le t{-}x & \text{specialization} \\
= & \top &
\end{array}
$$

Now the last case.

$$
\begin{array}{lll}
& x{=}0 \land ok \;\Rightarrow\; P & \text{replace } ok \text{ and } P \\
= & x{=}0 \land x'{=}x \land t'{\le}t \;\Rightarrow\; \textbf{if } x{>}0 \textbf{ then } t' \le t + x/2 + 2 \textbf{ else } t' \le t{-}x \textbf{ fi} & \text{context} \\
= & x{=}0 \land x'{=}x \land t'{\le}t \;\Rightarrow\; t \le t{-}0 & \text{arithmetic, reflexive, base} \\
= & \top &
\end{array}
$$