322 The notation **do** P **while** b **od** has been used as a loop construct that is executed as follows. First, P is executed; then b is evaluated, and if its value is $\top$ then execution is repeated, and if its value is $\bot$ then execution is finished.

(a) Let x be an integer variable. Prove

$$mod\ x'\ 2 \ = \ mod\ x\ 2 \ \Leftarrow\ \textbf{do}\ x{:=}\ x{-}2\ \textbf{while}\ x{\ge}2\ \textbf{od}$$

(b) Let m and n be integer variables. Prove

$$m{:=}\ m{+}n{-}10.\ \ n{:=}\ 10 \ \Leftarrow\ \textbf{do}\ m{:=}\ m{-}1.\ \ n{:=}\ n{+}1\ \textbf{while}\ n{\ne}10\ \textbf{od}$$

(c) In parts (a) and (b), add a time variable, and charge time 1 for each loop iteration. Notice that for this loop, recursive time is not quite the same as charging time 1 for each iteration. Choose a time specification, and prove it.

After trying the question, scroll down to the solution.

(a) Let x be an integer variable. Prove

$$mod\ x'\ 2\ =\ mod\ x\ 2 \ \Leftarrow\ \textbf{do}\ x{:=}\ x-2\ \textbf{while}\ x\ge 2\ \textbf{od}$$

§ To prove S is refined by **do** P **while** b **od** , prove instead

$$S\ \Leftarrow\ P.\ \textbf{if}\ b\ \textbf{then}\ S\ \textbf{else}\ ok\ \textbf{fi}$$

So we prove

$(mod\ x'\ 2\ =\ mod\ x\ 2\ \ \Leftarrow\ \ x{:=}\ x-2.\ \textbf{if}\ x\ge 2\ \textbf{then}\ mod\ x'\ 2\ =\ mod\ x\ 2\ \textbf{else}\ ok\ \textbf{fi})$

replace ok

$=$ $(mod\ x'\ 2\ =\ mod\ x\ 2\ \ \Leftarrow\ \ x{:=}\ x-2.\ \textbf{if}\ x\ge 2\ \textbf{then}\ mod\ x'\ 2\ =\ mod\ x\ 2\ \textbf{else}\ x'{=}x\ \textbf{fi})$

substitution

$=$ $mod\ x'\ 2\ =\ mod\ x\ 2\ \ \Leftarrow\ \ \textbf{if}\ x-2\ge 2\ \textbf{then}\ mod\ x'\ 2\ =\ mod\ (x-2)\ 2\ \textbf{else}\ x'=x-2\ \textbf{fi}$

by cases

$=$ $(mod\ x'\ 2\ =\ mod\ x\ 2\ \Leftarrow\ x-2\ge 2\ \land\ mod\ x'\ 2\ =\ mod\ (x-2)\ 2)$ specialization and

$\land\ (mod\ x'\ 2\ =\ mod\ x\ 2\ \Leftarrow\ x-2<2\ \land\ x'=x-2)$ specialization again

$\Leftarrow$ $(mod\ x'\ 2\ =\ mod\ x\ 2\ \Leftarrow\ mod\ x'\ 2\ =\ mod\ (x-2)\ 2)$ context and

$\land\ (mod\ x'\ 2\ =\ mod\ x\ 2\ \Leftarrow\ x'=x-2)$ context again

$=$ $(mod\ (x-2)\ 2\ =\ mod\ x\ 2\ \Leftarrow\ mod\ x'\ 2\ =\ mod\ (x-2)\ 2)$

$\land\ (mod\ (x-2)\ 2\ =\ mod\ x\ 2\ \Leftarrow\ x'=x-2)$

$=$ $\top \land \top$

$=$ $\top$

(b) Let m and n be integer variables. Prove

$$m{:=}\ m+n-10.\ n{:=}\ 10\ \ \Leftarrow\ \ \textbf{do}\ m{:=}\ m-1.\ n{:=}\ n+1\ \textbf{while}\ n\ne 10\ \textbf{od}$$

§ Apparently, we are not talking about time in this question; we don't have variable t . So we can't talk about termination or nontermination, because those are timing issues.

I prove

$m{:=}\ m+n-10.\ n{:=}\ 10\ \ \Leftarrow$

$m{:=}\ m-1.\ n{:=}\ n+1.\ \textbf{if}\ n\ne 10\ \textbf{then}\ m{:=}\ m+n-10.\ n{:=}\ 10\ \textbf{else}\ ok\ \textbf{fi}$

starting with the right side.

$m{:=}\ m-1.\ n{:=}\ n+1.\ \textbf{if}\ n\ne 10\ \textbf{then}\ m{:=}\ m+n-10.\ n{:=}\ 10\ \textbf{else}\ ok\ \textbf{fi}$

replace $n{:=}\ 10$ and ok

$=$ $m{:=}\ m-1.\ n{:=}\ n+1.\ \textbf{if}\ n\ne 10\ \textbf{then}\ m{:=}\ m+n-10.\ m'{=}m\ \land\ n'{=}10\ \textbf{else}\ m'{=}m\ \land\ n'{=}n\ \textbf{fi}$

substitution law in **then** part

$=$ $m{:=}\ m-1.\ n{:=}\ n+1.\ \textbf{if}\ n\ne 10\ \textbf{then}\ m'{=}m+n-10\ \land\ n'{=}10\ \textbf{else}\ m'{=}m\ \land\ n'{=}n\ \textbf{fi}$

substitution law twice

$=$ $\textbf{if}\ n+1\ne 10\ \textbf{then}\ m'{=}m-1+n+1-10\ \land\ n'{=}10\ \textbf{else}\ m'{=}m-1\ \land\ n'{=}n+1\ \textbf{fi}$

in **if** and **then** parts arithmetic; in **else** part context: $n{=}9$

$=$ $\textbf{if}\ n\ne 9\ \textbf{then}\ m'{=}m+n-10\ \land\ n'{=}10\ \textbf{else}\ m'{=}m+n-10\ \land\ n'{=}10\ \textbf{fi}$ case idempotent

$=$ $m'{=}m+n-10\ \land\ n'{=}10$ definition of assignment and sequential composition

$=$ $m{:=}\ m+n-10.\ n{:=}\ 10$

(c) In parts (a) and (b), add a time variable, and charge time 1 for each loop iteration. Notice that for this loop, recursive time is not quite the same as charging time 1 for each iteration. Choose a time specification, and prove it.

§ In part (a), to count iterations, put the time increment as follows:

$$\textbf{do}\ t{:=}\ t+1.\ x{:=}\ x-2\ \textbf{while}\ x\ge 2\ \textbf{od}$$

My time specification is

$$\textbf{if}\ x\ge 2\ \textbf{then}\ t'=t+floor\ (x/2)\ \textbf{else}\ t'=t+1\ \textbf{fi}$$

But *floor* is an awkward function to deal with, so I weaken my specification slightly to

$$\textbf{if}\ x\ge 2\ \textbf{then}\ t'\le t+x/2\ \textbf{else}\ t'=t+1\ \textbf{fi}$$

So I prove

if $x \ge 2$ **then** $t' \le t + x/2$ **else** $t' = t+1$ **fi**

$\Leftarrow$ $t := t+1.\ x := x-2.$ **if** $x \ge 2$ **then if** $x \ge 2$ **then** $t' \le t + x/2$ **else** $t' = t+1$ **fi else** ok **fi**

starting with the right (bottom) side:

$t := t+1.\ x := x-2.$ **if** $x \ge 2$ **then if** $x \ge 2$ **then** $t' \le t + x/2$ **else** $t' = t+1$ **fi else** ok **fi**

context $x \ge 2$

$=$ $t := t+1.\ x := x-2.$ **if** $x \ge 2$ **then** $t' \le t + x/2$ **else** ok **fi** — replace ok

$=$ $t := t+1.\ x := x-2.$ **if** $x \ge 2$ **then** $t' \le t + x/2$ **else** $x'=x \wedge t'=t$ **fi**

monotonicity to get rid of unneeded part of ok

$\Rightarrow$ $t := t+1.\ x := x-2.$ **if** $x \ge 2$ **then** $t' \le t + x/2$ **else** $t'=t$ **fi** — substitution law twice

$=$ **if** $x-2 \ge 2$ **then** $t' \le t + 1 + (x-2)/2$ **else** $t' = t+1$ **fi** — arithmetic simplification

$=$ **if** $x \ge 4$ **then** $t' \le t + x/2$ **else** $t' = t+1$ **fi** — when x is 2 or 3, $t' = t+1$, and so $t' \le t + x/2$

$\Rightarrow$ **if** $x \ge 2$ **then** $t' \le t + x/2$ **else** $t' = t+1$ **fi**

In part (b), to count iterations, put the time increment as follows:

do $t := t+1.\ m := m-1.\ n := n+1$ **while** $n \ne 10$ **od**

My time specification is **if** $n<10$ **then** $t' = t+10-n$ **else** $t'=\infty$ **fi**

So I prove

if $n<10$ **then** $t' = t+10-n$ **else** $t'=\infty$ **fi**

$\Leftarrow$ $t := t+1.\ m := m-1.\ n := n+1.$

if $n \ne 10$ **then if** $n<10$ **then** $t' = t+10-n$ **else** $t'=\infty$ **fi else** ok **fi**

starting with the right (bottom) side.

$t := t+1.\ m := m-1.\ n := n+1.$

if $n \ne 10$ **then if** $n<10$ **then** $t' = t+10-n$ **else** $t'=\infty$ **fi else** ok **fi** — replace ok

$=$ $t := t+1.\ m := m-1.\ n := n+1.$

if $n \ne 10$ **then if** $n<10$ **then** $t' = t+10-n$ **else** $t'=\infty$ **fi else** $m'=m \wedge n'=n \wedge t'=t$ **fi**

monotonicity to get rid of unneeded parts of ok

$\Rightarrow$ $t := t+1.\ m := m-1.\ n := n+1.$

if $n \ne 10$ **then if** $n<10$ **then** $t' = t+10-n$ **else** $t'=\infty$ **fi else** $t'=t$ **fi**

substitution law three times

$=$ **if** $n+1 \ne 10$ **then if** $n+1<10$ **then** $t' = t+1+10-(n+1)$ **else** $t'=\infty$ **fi else** $t'=t+1$ **fi**

arithmetic

$=$ **if** $n \ne 9$ **then if** $n<9$ **then** $t' = t+10-n$ **else** $t'=\infty$ **fi else** $t'=t+1$ **fi**

context: in final **else** part, $n=9$

$=$ **if** $n \ne 9$ **then if** $n<9$ **then** $t' = t+10-n$ **else** $t'=\infty$ **fi else** $t'=t+10-n$ **fi** — SOMEHOW

$=$ **if** $n \le 9$ **then** $t' = t+10-n$ **else** $t'=\infty$ **fi**

$=$ **if** $n<10$ **then** $t' = t+10-n$ **else** $t'=\infty$ **fi**