Part A

Question 1.

1. $\{x = 5\}$
   $\{3 = 3\}$
   $x := 3$ — Assign
   $\{x = 3\}$
   $\{x = 3\}$ — Consequence
   $x = 5 \Rightarrow 3 = 3 \Rightarrow x = 3[x := 3]$

2. $\{even(x)\}$
   $\{odd(x+1)\}$
   $x := x+1$ — Assign
   $\{odd(x)\}$
   $\{odd(x)\}$ — Consequence
   $even(x) \Rightarrow odd(x+1)$

3. $\{x = 5\}$
   $\{x = 5\}$
   skip — skip
   $\{x = 5\}$
   $\{odd(x)\}$ — Consequence
   $x = 5 \Rightarrow odd(x)$

Question 2.

1. Loop invariant : true

Body verification

$\{true \wedge true\}$ skip $\{true\}$

Postcondition

$\underbrace{true}_{\text{loop invariant}} \wedge \underbrace{\neg true}_{\text{loop guard}} \Rightarrow \underbrace{false}_{\text{postcondition}}$

$\therefore$ $\{true\}$ while true do skip $\{false\}$

2. Loop invariant : $x = 5$

Body verification

$\{x = 5\}$
continue
$\{false\}$ — continue
$x := 3$
$\{false\}$ — Assign
$\{x = 5\}$

↓ As false implies anything

Post condition

$x = 5 \wedge \neg x = 5 \Rightarrow false$

as no value of x satisfies LHS.

$\therefore$ $\{x = 5\}$ while $(x = 5)$ do continue; $x := 3$ $\{\not\Rightarrow false\}$

Question 3

1.

$$\left.\begin{array}{l}\{a[x]=3\}\\ x := a[x]\\ \{x=3\}\end{array}\right] \text{assign} \qquad x=3[x:=a[x]] = a[x]=3$$

2.

$$\{\underbrace{a\{a[x]\leftarrow a[x]\}[x] = a[x]}_{P}\}$$

$$\{a\{a[x]\leftarrow a[x]\}[x] = a\{a[x]\leftarrow a[x]\}[a[x]]\}$$

$$y := a[x]$$

$$\{a\{y\leftarrow y\}[x] = a[y\leftarrow y]Ey]\}$$

$$a[y] := y$$

$$(a[x] = a[y])$$

We can always assume $R \vee \neg R$ holds.

$\therefore$ true $\Rightarrow$ $a[x]=x \vee a[x]\neq x$

If $a[x]=x \Rightarrow$

$$a\{\underline{a[x]}\leftarrow a[x]\}\underline{[x]} = a[x]$$

equal

by $x=y \Rightarrow a[x\leftarrow z][y] = z$

If $a[x] != x \Rightarrow$

$$a\{\underline{a[x]}\leftarrow a[x]\}\underline{[x]}$$

unequal

$$\Rightarrow = a[x]$$

by $x\neq y$ $a[y\leftarrow z][x] = a[x]$

$\therefore$ true $\Rightarrow$ $a\{a[x]\leftarrow a[x]\}[x] = a[x]$

As required

Replace ! by fact.

Question 4

We need to use recursive function definition rule.

Use specification

$\{x \geq 0\}\ f(x)\ \{x! = return\}$

Prove body

Assume $\{x \geq 0\}\ f(x)\ \{x! = return\}$

$return\ \{\}\ x! = return$

$\{x \geq 0\}$

if $x = 0$ then

$\{x = 0\}$ ⇓ — definition of factorial

$\{x! = 1\}$

$return\ 1$

$\{false\}$

} return as $x! = 1 = x! = return\ [return := 1]$

else local y in

$\{x > 0\}$

$\{x - 1 \geq 0\}$

$y := f(x-1);$

$\{y = (x-1)!\}$

} function call $(x \geq 0\ [x := x-1])$ $f(x-1)$ $\{x! = return\ (x := x-1)\ [y := return]\}$

$\{y * x = x!\}$

$return\ (y * x);$

} return

$\{false\}$

$\{false\}$

Question 4 (cont)

let $f(z) = \ldots$

in

$\{z \geq 0\}$ — true $\Rightarrow z \geq 0$

$z := f(z)$ — call.

$\{z = !z\}$

Question 6

$\{ list(x) \}$

$\{ \exists t, v.\ x \mapsto t, v * (list(t) \vee (t = 0 \wedge emp)) \}$

$t := [x]$

$\{ \exists v.\ x \mapsto t, v * (list(t) \vee (t = 0 \wedge emp)) \}$

heap read

$\{ \exists t.\ x \mapsto t * P \}$

$t := [x]$

$\{ x \mapsto t * P \}$

$\{ x \mapsto t, v \}$

dispose x

dispose

$\{ emp \}$

Frame

$list(t) \vee (t = 0 \wedge emp)$

$\{ list(t) \vee t = 0 \wedge emp \}$

if $t \neq 0$ then

$\{ list(t) \}$

disposelist(t)

$\{ emp \}$

else

$\{ t = 0 \wedge (list(t) \vee t = 0 \wedge emp) \}$

$\{ emp \}$

skip

$\{ emp \}$

$\{ emp \}$.

This is harder than I expected

Question 7

We can prove for each thread

$$\{(f \neq 1 \wedge \text{empty}) \vee (f = 1 \wedge x \mapsto \_)\}$$
$$\text{if } f = 1 \text{ then } [x] := 5$$
$$[(f \neq 1 \wedge \text{empty}) \vee (f = 1 \wedge x \mapsto \_)]$$

$$\{(f \neq 1 \wedge x \mapsto \_) \vee (f = 1 \wedge f \neq y \wedge \text{empty})\}$$
$$\text{if } y = 1 \text{ then } [x] := 5$$
$$[(f \neq 1 \wedge x \mapsto \_) \vee (f = 1 \wedge f \neq y \wedge \text{empty})]$$

We can also prove

$$f \neq y \wedge x \mapsto \_$$
$$\Leftrightarrow (f \neq 1 \wedge^{f \neq y} x \mapsto \_) \vee (f = 1 \wedge y \neq f \wedge x \mapsto \_)$$
$$\Rightarrow \Big[(f \neq 1 \wedge^{f \neq y} \text{empty}) * (f \neq 1 \wedge^{f \neq y} x \mapsto \_) \vee (f = 1 \wedge^{f \neq y} x \mapsto \_) * (f = 1 \wedge y \neq f \wedge \text{empty})\Big] \vdash P$$
$$\Leftrightarrow P \vee (f = 1 \wedge^{f \neq y} x \mapsto 1) * (f \neq 1 \wedge x \mapsto \_) \vee (f \neq 1 \wedge^{f \neq y} \text{empty}) * (f = 1 \wedge \text{empty})$$
$$\Leftrightarrow (f \neq 1 \wedge^{f \neq y} \text{empty}) \vee (f = 1 \wedge x \mapsto \_) * ((f \neq 1 \wedge^{f \neq y} x \mapsto \_) \vee (f = 1 \wedge f \neq y \wedge \text{empty}))$$

So from pre-condition of parallel we can establish pre-conditions of each thread in a $*$ conjunction. Similar for post-condition

Question 8

$\{x=0\}$

1 $\{x=0 \vee x=5\}$	$\{x=0 \vee x=3\}$ 3
$x := x+3$	$x := 5$
$\{x=3 \vee x=8\}$	$\{x=5\}$
2 $\{x=3 \vee x=8 \vee x=5\}$	$\{x=5 \vee x=8\}$ 4

$\{x=8 \vee x=5\}$

Check interference freedom

1) $\{(x=0 \vee x=5) \wedge (x=0 \vee x=3)\}$ $x := 5$ $\{x=0 \vee x=5\}$

Simplify precondition

$\{x=0\}$ $x := 5$ $\{x=5\}$ $\Rightarrow$ $\{x=0 \vee x=5\}$

2) $\{(x=3 \vee x=8 \vee x=5) \wedge (x=0 \vee x=3)\}$ $x := 5$ $\{x=5\}$

And $x=5 \Rightarrow x=3 \vee x=8 \vee x=5$

3) $\{(x=0 \vee x=3) \wedge (x=0 \vee x=5)\}$

$\{x=0\}$

$x := x+3$

$\{x=3\}$

$\{x=0 \vee x=3\}$

4/ $\{ (x=5 \vee x=8) \wedge (x=0 \vee x=5) \}$

$\{ x=5 \}$

$x := x+3$

$\{ x=8 \}$

$\{ x=5 \vee x=8 \}$

assign

Conséquence.