E1

a)

$[skip_{SAM}]$ $\quad \langle skip : \gamma, s\rangle \Rightarrow \langle \gamma, s\rangle$

$[ass_{SAM}]$ $\quad \langle x := a : \gamma, s\rangle \Rightarrow \langle \gamma, s[x \mapsto \mathcal{A}[\![a]\!](s)]\rangle$

$[comp_{SAM}]$ $\quad \langle S_1; S_2 : \gamma, s\rangle \Rightarrow \langle S_1 : S_2 : \gamma, s\rangle$

$[if^{tt}_{SAM}]$ $\quad \langle \underline{if}\ b\ \underline{then}\ S_1\ \underline{else}\ S_2 : \gamma, s\rangle \Rightarrow \langle S_1 : \gamma, s\rangle$ if $\mathcal{B}[\![b]\!](s) = tt$

$[if^{ff}_{SAM}]$ $\quad \langle \underline{if}\ b\ \underline{then}\ S_1\ \underline{else}\ S_2 : \gamma, s\rangle \Rightarrow \langle S_2 : \gamma, s\rangle$ if $\mathcal{B}[\![b]\!](s) = ff$

$[while^{tt}_{SAM}]$ $\quad \langle \underline{while}\ b\ \underline{do}\ S : \gamma, s\rangle \Rightarrow \langle S : \underline{while}\ b\ \underline{do}\ S : \gamma\rangle$ if $\mathcal{B}[\![b]\!](s) = tt$

$[while^{ff}_{SAM}]$ $\quad \langle \underline{while}\ b\ \underline{do}\ S : \gamma, s\rangle \Rightarrow \langle \gamma, s\rangle$ if $\mathcal{B}[\![b]\!](s) = ff$

b)

$\langle z := 0;\ \underline{while}\ y \le x\ \underline{do}\ (z := z+1;\ x := x-y),\ s\rangle$

$\Rightarrow \langle z := 0 : \underline{while}\ y \le x\ \underline{do}\ (z := z+1;\ x := x-y),\ s\rangle$

$\Rightarrow \langle \underline{while}\ y \le x\ \underline{do}\ (z := z+1;\ x := x-y),\ s[z \mapsto 0]\rangle$

$\Rightarrow \langle (z := z+1;\ x := x-y) : \underline{while}\ y \le x\ \underline{do}\ (z := z+1;\ x := x-y),\ s[z \mapsto 0]\rangle$

$\Rightarrow \langle z := z+1 : x := x-y : \underline{while}\ y \le x\ \underline{do}\ (z := z+1;\ x := x-y),\ s[z \mapsto 0]\rangle$

$\Rightarrow \langle x := x-y : \underline{while}\ y \le x\ \underline{do}\ (z := z+1;\ x := x-y),\ s[z \mapsto 1]\rangle$

$\Rightarrow \langle \underline{while}\ y \le x\ \underline{do}\ (z := z+1;\ x := x-y),\ s[x \mapsto 12, z \mapsto 1]\rangle$

$\vdots$

$\Rightarrow \langle \underline{while}\ y \le x\ \underline{do}\ (z := z+1;\ x := x-y),\ s[x \mapsto 2, z \mapsto 3]\rangle$

$\Rightarrow s[x \mapsto 2, z \mapsto 3]$

E2

$Pre \stackrel{def}{=} x = x_0 \wedge x \geq 0$

$Post \stackrel{def}{=} y = x_0!$

C2 a) $Inv \stackrel{def}{=} y * x! = x_0! \wedge x \geq 0$

b) $vcg\,[\![y := 1; \{Inv\}\ \underline{while}\ \ldots]\!]\,(y = x_0!, true)$

$= vcg\,[\![y := 1]\!]\,(vcg\,[\![\{Inv\}\ \underline{while}\ \ldots]\!]\,(y = x_0!, true))$

$= vcg\,[\![y := 1]\!]\,(\underline{let}\ (P', Q') = vcg\,[\![y := y * x; x := x - 1]\!]\,(Inv, true)$

$\vdots \qquad \underline{in}\ (Inv, true \wedge Q' \wedge (Inv \wedge \neg(x = 0) \Rightarrow P') \wedge (Inv \wedge \neg\neg(x = 0) \Rightarrow y = x_0!))$

$= vcg\,[\![y := 1]\!]\,(y * x! = x_0! \wedge x \geq 0,$

$true \wedge true \wedge$

$y * x! = x_0! \wedge x \geq 0 \wedge \neg(x = 0) \Rightarrow (y * x) * (x-1)! = x_0! \wedge x - 1 \geq 0 \wedge$

$y * x! = x_0! \wedge x \geq 0 \wedge \neg\neg(x = 0) \Rightarrow y = x_0!\ )$

$= (1 * x! = x_0! \wedge x \geq 0, \ldots)$

Then $VCG(\{Pre\}\ y := 1; \{Inv\}\ \underline{while}\ \ldots \{Post\}) =$

$x = x_0 \wedge x \geq 0 \Rightarrow 1 * x! = x_0! \wedge x \geq 0$ ①

$\wedge\ true \wedge true$

$\wedge\ y * x! = x_0! \wedge x \geq 0 \wedge \neg(x = 0) \Rightarrow (y * x) * (x-1)! = x_0! \wedge x - 1 \geq 0$ ②

$\wedge\ y * x! = x_0! \wedge x \geq 0 \wedge \neg\neg(x = 0) \Rightarrow y = x_0!$ ③

c) We argue for validity of the individual conjuncts:

① obvious

② valid since $(y * x) * (x-1)! = y * x!$ when $x \geq 1$

③ valid since $x! = 1$ when $x = 0$

C1

$S_{ds}[\![\text{skip}]\!] \stackrel{def}{=} id'$ where $id'(s) \stackrel{def}{=} \{s\}$

$S_{ds}[\![x := a]\!](s) \stackrel{def}{=} \{s[x \mapsto \mathcal{A}[\![a]\!](s)]\}$

$S_{ds}[\![S_1 ; S_2]\!] \stackrel{def}{=} S_{ds}[\![S_2]\!] \circ' S_{ds}[\![S_1]\!]$ where $(g_2 \circ' g_1)(s) \stackrel{def}{=} \bigcup_{s' \in g_1(s)} g_2(s')$

$S_{ds}[\![S_1 \text{ or } S_2]\!](s) \stackrel{def}{=} S_{ds}[\![S_1]\!](s) \cup S_{ds}[\![S_2]\!](s)$

$S_{ds}[\![\text{if } b \text{ then } S_1 \text{ else } S_2]\!] \stackrel{def}{=} cond'(\mathcal{B}[\![b]\!], S_{ds}[\![S_1]\!], S_{ds}[\![S_2]\!])$

$S_{ds}[\![\text{while } b \text{ do } S]\!] \stackrel{def}{=} FIX\ F_{b,S}$

where $cond'(p, g_1, g_2)$ is defined as $cond$, but has now co-domain $P(State)$ instead of $State$

and $F_{b,S} : (State \to P(State)) \to (State \to P(State))$
$F_{b,S}(g) \stackrel{def}{=} cond'(\mathcal{B}[\![b]\!], g \circ' S_{ds}[\![S]\!], id')$

Here $g : State \to P(State)$

and $\perp' \in State \to P(State)$
$\perp'(s) \stackrel{def}{=} \emptyset$ for all $s \in State$

A1 a) $F(g)(s) = \underline{\text{cond}}'(B[\![(0 \le x) \wedge (x \le 1)]\!], g \circ' S_{ds}[\![x := x-1 \text{ or } x := x+1]\!], id')(s)$

$$= \begin{cases} g(s[x \mapsto s(x)-1]) \cup g(s[x \mapsto s(x)+1]) & \text{if } 0 \le s(x) \le 1 \\ \{s\} & \text{otherwise} \end{cases}$$

b) $F^1(\bot)(s) = F(F^0(\bot))(s) = F(\bot)(s) =$

$$\vdots = \begin{cases} \emptyset & \text{if } 0 \le s(x) \le 1 \\ \{s\} & \text{otherwise} \end{cases}$$

$F^2(\bot)(s) = F(F^1(\bot))(s) =$

$$\vdots = \begin{cases} \{s[x \mapsto -1]\} & \text{if } s(x) = 0 \\ \{s[x \mapsto 2]\} & \text{if } s(x) = 1 \\ \{s\} & \text{otherwise} \end{cases}$$

$F^3(\bot)(s) = F(F^2(\bot))(s) =$

$$\vdots = \begin{cases} \{s[x \mapsto -1], s[x \mapsto 2]\} & \text{if } 0 \le s(x) \le 1 \\ \{s\} & \text{otherwise} \end{cases}$$

$F^4(\bot)(s) = F(F^3(\bot))(s) = \ldots = F^3(\bot)(s)$ fixed point!

Hence $FIX\ F = F^3(\bot)$ and

$$S_{ds}[\![\underline{\text{while}}\ (0 \le x) \wedge (x \le 1)\ \underline{\text{do}}\ (x := x-1 \text{ or } x := x+1)]\!](s) = \begin{cases} \{s[x \mapsto -1], s[x \mapsto 2]\} & \text{if } 0 \le s(x) \le 1 \\ \{s\} & \text{otherwise} \end{cases}$$

c) If $0 \le s(x) \le 1$ then executing the program from s can terminate in either $s[x \mapsto -1]$ or $s[x \mapsto 2]$, or may not terminate at all.
If $s(x) < 0$ or $s(x) > 1$ then executing the program from s can terminate in s itself, or may not terminate at all (!).

A2

We show $\forall S \in Stm.\ \forall P \in Assn.\ \vdash_{par} \{P\}\ S\ \{true\}$ by structural induction on statements.

[$S \equiv x := a$] Assume $P \in Assn$. The derivation

$$\dfrac{\dfrac{}{\{true\}\ x := a\ \{true\}}\ ass_P}{\{P\}\ x := a\ \{true\}}\ cons_P : P \Rightarrow true \text{ is valid}$$

establishes derivability of $\{P\}\ x := a\ \{true\}$, i.e. $\vdash_{par} \{P\}\ x := a\ \{true\}$

[$S \equiv$ while b do S'] Assume $\forall Q \in Assn.\ \vdash \{Q\}\ S'\ \{true\}$ (ind. hyp.)
Assume $P \in Assn$. The derivation

$$\dfrac{\dfrac{\dfrac{\text{(ind. hyp.)}}{\{true \wedge b\}\ S'\ \{true\}}}{\{true\}\ \text{while } b \text{ do } S'\ \{true \wedge \neg b\}}\ while_P}{\{P\}\ \text{while } b \text{ do } S'\ \{true\}}\ cons_P : \begin{array}{l} P \Rightarrow true \\ true \wedge \neg b \Rightarrow true \end{array} \text{ are valid}$$

establishes $\vdash_{par} \{P\}$ while b do S' $\{true\}$

etc