# Exercise 1.

We are to show

$$\{\boxed{K}^{\gamma} * P\}\ \mathrm{ref}(\mathrm{false})\ \{v.\ \exists \gamma.\ \exists l\, \exists \iota.\, v = l \land \boxed{l \mapsto \mathrm{false} * \boxed{K}^{\gamma} * P \lor l \mapsto \mathrm{true}}^{\iota}\}$$

By HT-Bind, SFTS 2 goals

① $\{\boxed{K}^{\gamma} * P\}\ \mathrm{ref}(\mathrm{false})\ \{v.\ \exists l.\ v = l \land \triangleright(l \mapsto \mathrm{false} * \boxed{K}^{\gamma} * P \lor l \mapsto \mathrm{true})\}$

② $\{v = l \land \triangleright(l \mapsto \mathrm{false} * \boxed{K}^{\gamma} * P)\}\ v\ \{v.\ \exists \gamma, l, \iota.\, v = l \land \boxed{l \mapsto \mathrm{false} * \boxed{K}^{\gamma} * P \lor l \mapsto \mathrm{true}}^{\iota}\}$

For ①. By forward reasoning. We have

$$\{\mathrm{True}\}\ \mathrm{ref}(\mathrm{false})\ \{v.\ \exists l.\ v = l \land l \mapsto \mathrm{false}\}$$

By LATER-WEAK, HT-CSQ, and some other structrual rules, we have

$$\{\boxed{K}^{\gamma} * P\}\ \mathrm{ref}(\mathrm{false})\ \{v.\ \exists l.\ v = l \land \triangleright(l \mapsto \mathrm{false} * \boxed{K}^{\gamma} * P)\}$$

By VI and HT-CSQ, we have

$$\{\boxed{K}^{\gamma} * P\}\ \mathrm{ref}(\mathrm{false})\ \{v.\ \exists l.\ v = l \land \triangleright(l \mapsto \mathrm{false} * \boxed{K}^{\gamma} * P \lor l \mapsto \mathrm{true})\}$$

This concludes ①

For ②. Because we have

$$\{v = l\}\ v\ \{v.\ \exists l.\ v = l\}$$

Then By HT-INV-ALLOC-POST. We have ②

Exercise 2.

For clarity, let $P \triangleq \exists xs.\ l \mapsto xs * \cancel{bg}\ bagList(\emptyset, xs)$

After some simplification, we want to show

$\{\emptyset(u) * isLock(v, P, \gamma)\}$ acquire $v$; $l \leftarrow some(u, !l)$; release $v$ $\{\_.\ True\}$

Because $isLock(v, P, \gamma)$ is duplicable, we can move it to the context

We then use HT-BIND, for the first statement, we want to show

① $\{\emptyset(u) * isLock(v, P, \gamma)\}$ acquire $v$ $\{w.\ \emptyset(u) * P * locked(\gamma)\}$

which is trival by the spec of lock and some structrual rules.

~~Then we are left show~~

We continue to use the Bind rule, for the second statement, we want to show

$\{\emptyset(u) * locked(\gamma) * P\}$ $l \leftarrow some(u, !l)$ $\{w.\ P * Locked(\gamma)\}$

We expand $P$ and use the bind rule and load rule to simplify the goal

② $\{\emptyset(u) * locked(\gamma) * l \mapsto xs * bagList(\emptyset, xs)\}$ $l \leftarrow some(u, xs)$ $\{w.\ Locked(\gamma) * \exists xs'.\ l \mapsto xs' * bagList(\emptyset, xs')\}$

Using forward reasoning, we have

$\{l \mapsto xs\}$ $l \leftarrow some(u, xs)$ $\{w.\ \exists xs'.\ l \mapsto xs' * xs' = some(u, xs)\}$

Thus we further have

$\{l \mapsto xs * \emptyset(u) * locked(\gamma) * bagList(\emptyset, xs)\}$ $l \leftarrow some(u, xs)$ $\{w.\ \exists xs'.\ l \mapsto xs' * xs' = some(u, xs) * locked(\gamma) * \emptyset(u) * bagList(\emptyset, xs)\}$

By LATER-WEAK and other structrual rules, we know the post condition

$xs' = some(u, xs) * \emptyset(u) * bagList(\emptyset, xs)$ implies $bagList(\emptyset, xs')$

So by the consequence rule, we know

$\{l \mapsto xs * \emptyset(u) * locked(\gamma) * bagList(\emptyset, xs)\}$ $l \leftarrow some(u, xs)$ $\{w.\ \exists xs'.\ l \mapsto xs' * bagList(\emptyset, xs') * locked(\gamma)\}$

which is our goal ②

Finally, for the last statement, we have to show

③ $\{P * locked(\gamma)\}$ release $v$ $\{\_.\ True\}$ where in the context we have $isLock(v, P, \gamma)$

which immediately follows from the spec of lock

# Exercise 3.

By the recursion rule, we need to show

$$\{isCounter(v,n,\gamma)\}\ let\ n:=!v\ in \dots \{u.\ u\ge n * isCounter(v, n+1, \gamma)\}$$

under the induction hypothesis

$$\forall \gamma, v, n.\ \{isCounter(v,n,\gamma)\}\ incr\ v\ \{u.\ u\ge n * isCounter(v,n+1,\gamma)\}$$

Let us expand isCounter in the pre-condition and move the invariant into context, SFTS

$$\boxed{\exists m.\ v\mapsto m * \boxed{\bullet m}^{\gamma}}^{\iota} \vdash \{\boxed{\circ n}^{\gamma}\}\ let\ n:=!v\ in \dots \{u.\ u\ge n * isCounter(v,n+1,\gamma)\}$$

By the bind rule, we show the intermediate goal

$$\boxed{\quad}^{\iota} \vdash \{\boxed{\circ n}^{\gamma}\}\ !v\ \{u.\ \exists m.\ u=m * m\ge n * \boxed{\circ n}^{\gamma}\}$$

We open the invariant and we need to show

① $$\{\boxed{\circ n}^{\gamma} * \triangleright(v\mapsto m * \boxed{\bullet m}^{\gamma})\}\ !v\ \{u.\ u=m * m\ge n * \boxed{\circ n}^{\gamma} * \triangleright(\exists m.\ v\mapsto m * \boxed{\bullet m}^{\gamma})\}$$

By forward reasoning, we have

$$\{\triangleright(v\mapsto m)\}\ !v\ \{u.\ u=m * v\mapsto m\}$$

~~By LATER-WEAK and some structural rules, we further have~~

$$\cancel{\{\dots * \triangleright(v\mapsto m) * \bullet m\}}$$

~~By the framing rule, we put a $\triangleright\boxed{\circ n}^{\gamma}$ in the pre and post condition. By Frame-Atomic, we put a $\triangleright\boxed{\circ n}^{\gamma}$ in the pre-condition and a $\boxed{\circ n}^{\gamma}$ in the post-condition so we have~~ By HT-Frame-Atomic, we have

$$\{\triangleright(v\mapsto m) * \triangleright(\boxed{\bullet m}^{\gamma} * \boxed{\circ n}^{\gamma})\}\ !v\ \{u.\ u=m * v\mapsto m * \boxed{\bullet m}^{\gamma} * \boxed{\circ n}^{\gamma}\}$$

Because $\boxed{\bullet m}^{\gamma} * \boxed{\circ n}^{\gamma} \Rightarrow \boxed{\bullet m \cdot \circ n}^{\gamma} \Rightarrow \bullet m \cdot \circ n \in \mathcal{V} \Rightarrow m\ge n$, By the consequence rule and LATER-WEAK, we have

$$\{\boxed{\circ n}^{\gamma} * \triangleright(v\mapsto m) * \triangleright\boxed{\bullet m}^{\gamma}\}\ !v\ \{u.\ u=m * m\ge n * \triangleright(v\mapsto m) * \triangleright\boxed{\bullet m}^{\gamma} * \boxed{\circ n}^{\gamma}\}$$

which is ①

Continue the rest of the bind rule, after some simplification, we need to show

$$\boxed{\quad}^{\iota} \vdash \{u\ge n * \boxed{\circ n}^{\gamma}\}\ if\ CAS(v,u,u+1)\ then\ u\ else\ incr\ v\ \{u.\ u\ge n * isCounter(v,n+1,\gamma)\}$$

We use the bind rule to show the intermediate goal: (we put $u\ge n$ in the context)

$$\boxed{\quad}^{\iota} \vdash \{\boxed{\circ n}^{\gamma}\}\ CAS(v,u,u+1)\ \{w.\ w=true * \boxed{\circ n+1}^{\gamma} \lor w=false * \boxed{\circ n}^{\gamma}\}$$

We open the invariant, TS.

$$\{\boxed{\circ n}^{\gamma} * \triangleright(v\mapsto m * \boxed{\bullet m}^{\gamma})\}\ CAS(v,u,u+1)\ \{w.\ (w=true * \boxed{\circ n+1}^{\gamma} \lor w=false * \boxed{\circ n}^{\gamma}) * \triangleright(\exists m\ v\mapsto m * \boxed{\bullet m}^{\gamma})\}$$

we do case analysis on whether $m=u$

If $m=u$, we need to show

② $$\{\boxed{\circ n}^{\gamma} * \triangleright(v\mapsto u * \boxed{\bullet u}^{\gamma})\}\ CAS(v,u,u+1)\ \{\dots\}$$

By forward reasoning, we have

$$\{\triangleright(v \mapsto u)\}\ CAS(v, u, u+1)\ \{w.\ w = true * v \mapsto u+1\}$$

By HT-Frame-Atomic, we have

$$\{\triangleright(v \mapsto u) * \triangleright\boxed{\circ n}^{\gamma} * \triangleright\boxed{\bullet u}^{\gamma}\}\ CAS(v, u, u+1)\ \{w.\ w = true * v \mapsto u+1 * \boxed{\circ n}^{\gamma} * \boxed{\bullet u}^{\gamma}\}$$

Since $\bullet u \cdot \circ n \rightsquigarrow \bullet(u+1) \cdot \circ(n+1)$, we have $\boxed{\circ n}^{\gamma} * \boxed{\bullet u}^{\gamma} \Rrightarrow \boxed{\circ n+1}^{\gamma} * \boxed{\bullet u+1}^{\gamma}$, so we have

$$\{\triangleright(v \mapsto u) * \boxed{\circ n}^{\gamma} * \triangleright\boxed{\bullet u}^{\gamma}\}\ CAS(v, u, u+1)\ \{w.\ w = true * \triangleright(v \mapsto u+1) * \boxed{\circ n+1}^{\gamma} * \triangleright\boxed{\bullet u+1}^{\gamma}\}$$

which concludes ② if we take $m$ in ② to be $u+1$

In the case where $m \neq u$, we need to show

③ $\{\boxed{\circ n}^{\gamma} * \triangleright(u \mapsto m * \boxed{\bullet m}^{\gamma}) * u \neq m\}\ CAS(v, u, u+1)\ \{w. \cdots\}$

This can be shown similarly as ②, where here we will apply HT-CAS-FAIL and take $m$ in the post-cond to be $m$

Then we are left to show

$$\boxed{\phantom{I}}^{\iota} \vdash \left\{\begin{pmatrix} w = true * \boxed{\circ n+1}^{\gamma} \lor \\ w = false * \boxed{\circ n}^{\gamma} \end{pmatrix}\right\}\ \text{if } w \text{ then } u \text{ else incr } v\ \{u.\ u \geq n * isCounter(v, n+1, \gamma)\}$$

We consider the two case in the pre-condition seperately by HT-DISJ.

In the first case, we need to show

$$\boxed{\phantom{I}}^{\iota} \vdash \{\boxed{\circ n+1}^{\gamma}\}\ u\ \{u.\ u \geq n * \boxed{\circ n+1}^{\gamma} * \exists l. \boxed{\phantom{I}}^{\iota}\}$$

which is true as we have $u \geq n$ and the invariant in the context

In the second case, we need to show

$$\boxed{\phantom{I}}^{\iota} \vdash \{\boxed{\circ n}^{\gamma}\}\ incr\ v\ \{u.\ u \geq n * isCounter(v, n+1, \gamma)\}$$

which follows from the induction hypothesis as we can move the invariant into the pre-condition and have $isCounter(v, n, \gamma)$.

# Exercise 4

For the first spec,. we need to show

$$\boxed{\phantom{xxxxxx}}^{\iota} \vdash \{ \lceil \circ(1,n) \rceil^{\gamma} \} \; !v \; \{u.\, u = n\}$$

We open the invariant and we need to show

$$① \quad \{ \lceil \circ(1,n) \rceil^{\gamma} * \triangleright(v \mapsto m * \lceil \bullet(1,m) \rceil^{\gamma}) \} \; !v \; \{u.\, u = n * \triangleright(\exists m.\, v \mapsto m * \lceil \bullet(1,m) \rceil^{\gamma})\}$$

By forward reasoning, we know

$$\{ \triangleright(v \mapsto m) \} \; !v \; \{u.\, u = m * v \mapsto m\}$$

By HTFrame-Atomic, we know

$$\{ \triangleright(v \mapsto m) * \triangleright(\lceil \circ(1,n) \rceil^{\gamma} * \lceil \bullet(1,m) \rceil^{\gamma}) \} \; !v \; \{u.\, u = m * v \mapsto m * \lceil \circ(1,n) \rceil^{\gamma} * \lceil \bullet(1,m) \rceil^{\gamma}\}$$

By def of the resource algebra and OWN-Valid, we have $m = n$, hence we have

$$\{ \triangleright(v \mapsto m) * \triangleright\lceil \circ(1,n) \rceil^{\gamma} * \triangleright\lceil \bullet(1,m) \rceil^{\gamma} \} \; !v \; \{u.\, u = n * v \mapsto n * \lceil \circ(1,n) \rceil^{\gamma} * \lceil \bullet(1,n) \rceil^{\gamma}\}$$

which implies ① by the consequence rule and taking $\exists m$ to be $n$

The second spec follows the exact same reasoning, except that we will have $m \geq n$ and will take $\exists m$ to be $m$.