Program Logics Hand-in 4

Zijun Yu 202203581

Octobor 2023

Exercise 1

We introduce m and apply Ht-inv-open and E-$\triangleright$, since $l \leftarrow (m+1)$ is an atomic expression (assuming that $m+1$ is a value), SFTS

$$\boxed{I\ n}^{\iota} \vdash \{\exists m'. \triangleright(m' \geq n \land l \hookrightarrow m') * (m \geq n)\} l \leftarrow (m+1) \{\_. \triangleright(\exists m. m \geq n \land l \hookrightarrow m) * \mathrm{True}\}_{\mathcal{E}\setminus\iota} \quad (1)$$

We then use Ht-exist and introduce m', SFTS

$$\boxed{I\ n}^{\iota} \vdash \{\triangleright(m' \geq n \land l \hookrightarrow m') * (m \geq n)\} l \leftarrow (m+1) \{\_. \triangleright(\exists m. m \geq n \land l \hookrightarrow m) * \mathrm{True}\}_{\mathcal{E}\setminus\iota} \quad (2)$$

Using Ht-frame-atmoic with Ht-store and other structure rules we have

$$\boxed{I\ n}^{\iota} \vdash \{\triangleright(l \hookrightarrow m' \land m \geq n)\} l \leftarrow (m+1) \{v. v = () \land l \hookrightarrow (m+1) \land m \geq n\}_{\mathcal{E}\setminus\iota} \quad (3)$$

Because the precondition in (2) implies the precondition in (3), we apply Ht-csq, and we are left to show

$$v = () \land l \hookrightarrow (m+1) \land m \geq n \vdash \triangleright(\exists m. m \geq n \land l \hookrightarrow m) * \mathrm{True}$$

This holds as we can take $\exists m$ to be $m+1$ and apply E-$\triangleright$ and Later-weak.

Exercise 2

$$\dfrac{\dfrac{P_2 \vdash \mid\!\Rrightarrow Q}{P_1 * P_2 \vdash P_1 * \mid\!\Rrightarrow Q \vdash \mid\!\Rrightarrow (P_1 * Q)} \qquad \dfrac{P_1 * Q \vdash \mid\!\Rrightarrow R}{\mid\!\Rrightarrow (P_1 * Q) \vdash \mid\!\Rrightarrow \mid\!\Rrightarrow R \vdash \mid\!\Rrightarrow R}}{P_1 * P_2 \vdash \mid\!\Rrightarrow R}$$

Exercise 3

HT-TOKEN-ALLOC

By Ht-csq-vs, it suffices to show $S \vdash P \Rrightarrow \exists \gamma. \boxed{\mathrm{T}}^{\gamma} * P$, which is equivalent to

$$S \vdash \Box(P \Rightarrow \mid\!\Rrightarrow(\exists \gamma. \boxed{\mathrm{T}}^{\gamma} * P))$$

Because $S \vdash True \vdash \Box True$, by Trans, it suffices to show

$$\Box True \vdash \Box(P \Rightarrow \mid\!\Rrightarrow(\exists \gamma. \boxed{\mathrm{T}}^{\gamma} * P))$$

Then by Persistently-intro, it suffices to show

$$\Box True \vdash P \Rightarrow \mid\!\Rrightarrow(\exists \gamma. \boxed{\mathrm{T}}^{\gamma} * P)$$

which simplifies to

$$P \vdash \mathrel{|\!\!\!\Rrightarrow}(\exists \gamma. \boxed{\mathrm{T}}^{\gamma} * P)$$

which can be derived from Ghost-alloc, $*$I, and Upd-frame.

HT-TOKEN-UPDATE-PRE

By Ht-csq-vs, it suffices to show

$$S \vdash \boxed{\mathrm{S}}^{\gamma} * P \Rrightarrow \boxed{\mathrm{F}}^{\gamma} * P$$

By applying the same trick as in Ht-token-alloc, it suffices to show

$$\boxed{\mathrm{S}}^{\gamma} * P \vdash \mathrel{|\!\!\!\Rrightarrow} \left(\boxed{\mathrm{F}}^{\gamma} * P\right)$$

which follows from Ghost-update, $*$I, and Upd-frame.

HT-TOKEN-UPDATE-POST

By Ht-csq-vs, what we are left to show is exactly the same as in Ht-token-update-pre.

Exercise 4

By Ht-load, we know that

$$\{\triangleright\, l \hookrightarrow n\} !l \,\{v. v = n * l \hookrightarrow n\}$$

By Ht-csq, we further have

$$\{\triangleright\, l \hookrightarrow n\} !l \left\{v. \left(v = n \vee v = n + 1 * \boxed{\mathrm{F}}^{\gamma_1}\right) * l \hookrightarrow n\right\}$$

Then by Ht-frame-atomic and $*$I, we know that

$$\left\{\triangleright \left(l \hookrightarrow n * \boxed{\mathrm{S}}^{\gamma_1}\right) * \boxed{\tfrac{1}{2}}^{\gamma_2}\right\} !l \left\{v. \left(v = n \vee v = n + 1 * \boxed{\mathrm{F}}^{\gamma_1}\right) * l \hookrightarrow n * \boxed{\mathrm{S}}^{\gamma_1} * \boxed{\tfrac{1}{2}}^{\gamma_2}\right\}$$

Because $l \hookrightarrow n * \boxed{\mathrm{S}}^{\gamma_1} \vdash \triangleright \left(l \mapsto n * \boxed{\mathrm{S}}^{\gamma_1}\right) \vdash \triangleright I(\gamma_1, \gamma_2, n)$, by Ht-csq, we have that

$$\left\{\triangleright \left(l \hookrightarrow n * \boxed{\mathrm{S}}^{\gamma_1}\right) * \boxed{\tfrac{1}{2}}^{\gamma_2}\right\} !l \left\{v. \left(v = n \vee v = n + 1 * \boxed{\mathrm{F}}^{\gamma_1}\right) * \triangleright I(\gamma_1, \gamma_2, n) * \boxed{\tfrac{1}{2}}^{\gamma_2}\right\}$$

which is what we need to show.