RustBelt 5 章
Invariants and modalities

K.Hirata

Contents

Invariant と mask に関して詳細に見ていく。

- 5.1 “timeless” の制約のない、一般の invariants に関する rule 準備
- 5.2 Cancellation mechanism (一度得た所有権が返却できるシステム) について調べる。 動機
- 5.3 view shift の概念の拡張 (5.2 からモチベーションを得る)
  問題(うまくいかない)
- 5.4-5 view shift が modality として見た方が良いという話
  解決
- 5.6 何を言ってるのかわからん

5.1 General invariants and the later modality

Timeless

VS-INV-TIMELESS

$$\frac{P * Q_1 \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}} P * Q_2 \qquad \mathcal{N} \subseteq \mathcal{E} \qquad \mathsf{timeless}(P)}{\boxed{P}^{\mathcal{N}} * Q_1 \Rrightarrow_{\mathcal{E}} \boxed{P}^{\mathcal{N}} * Q_2}$$

HOARE-INV-TIMELESS

$$\frac{\{P * Q_1\}\, e\, \{v.\, P * Q_2\}_{\mathcal{E}\setminus\mathcal{N}} \qquad \mathsf{atomic}(e) \qquad \mathsf{timeless}(P) \qquad \mathcal{N} \subseteq \mathcal{E}}{\left\{\boxed{P}^{\mathcal{N}} * Q_1\right\} e \left\{v.\, \boxed{P}^{\mathcal{N}} * Q_2\right\}_{\mathcal{E}}}$$

- Later modality は、ないとまずいらしい。
- Vs-timeless を使うと、timeless の場合の rule を導ける。
- Later modality を取り除くには、HOARE-STEP を使う。

一般

INV-ALLOC

$$\triangleright P \Rrightarrow_{\mathcal{E}} \boxed{P}^{\mathcal{N}}$$

VS-INV

$$\frac{\triangleright P * Q_1 \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}} \triangleright P * Q_2 \qquad \mathcal{N} \subseteq \mathcal{E}}{\boxed{P}^{\mathcal{N}} * Q_1 \Rrightarrow_{\mathcal{E}} \boxed{P}^{\mathcal{N}} * Q_2}$$

▷-INTRO

$$P \vdash \triangleright P$$

▷-MONO

$$\frac{P \vdash Q}{\triangleright P \vdash \triangleright Q}$$

VS-TIMELESS

$$\frac{\mathsf{timeless}(P)}{\triangleright P \Rrightarrow_{\mathcal{E}} P}$$

▷ commutes around □, ∨, ∧, ∗, ∀, and ∃ with non-empty domain

HOARE-INV

$$\frac{\{\triangleright P * Q_1\}\, e\, \{v.\, \triangleright P * Q_2\}_{\mathcal{E}\setminus\mathcal{N}} \qquad \mathsf{atomic}(e) \qquad \mathcal{N} \subseteq \mathcal{E}}{\left\{\boxed{P}^{\mathcal{N}} * Q_1\right\} e \left\{v.\, \boxed{P}^{\mathcal{N}} * Q_2\right\}_{\mathcal{E}}}$$

HOARE-STEP

$$\frac{\{P\}\, e\, \{v.\, Q\}_{\mathcal{E}} \qquad e \text{ is not a value}}{\{P * \triangleright R\}\, e\, \{v.\, Q * R\}_{\mathcal{E}}}$$

5.2 Cancellable invariants

- Cancellable invariants: 一時的に share される invariant で、のちに取り除かれるもの。

- (Fractional points-to と似たように、) この場合は、**fractional token** が invariant に equip できる。(考えられる、的な意味か？)

  - Access する権利は分割できるが、cancel するためには full ownership が必要。

. $\mathsf{CInv}^{\gamma,\mathcal{N}}(P)$: 命題 P に対しての cancellable invariant の存在を表現する。

  . $\mathcal{N}$: 名前空間 (なので、気にしなくていいと思われる)

  . γ : ghost identifier。token と invariant を結びつける。

. $[\mathsf{CInv}: \gamma]_q$: 有理数 q の分の token の所有権。[…] が token。

CINV-TIMELESS

$$\mathsf{timeless}([\mathsf{CInv} : \gamma]_q)$$

CINV-PERSISTENT

$$\mathsf{persistent}(\mathsf{CInv}^{\gamma,\mathcal{N}}(P))$$

CINV-SPLIT

$$[\mathsf{CInv} : \gamma]_{q_1+q_2} \Leftrightarrow [\mathsf{CInv} : \gamma]_{q_1} * [\mathsf{CInv} : \gamma]_{q_2}$$

CINV-VALID

$$[\mathsf{CInv} : \gamma]_q \Rightarrow q \leq 1$$

CINV-ALLOC

$$\triangleright P \Rrightarrow_{\mathcal{E}} \exists \gamma.\, [\mathsf{CInv} : \gamma]_1 * \mathsf{CInv}^{\gamma,\mathcal{N}}(P)$$

CINV-CANCEL

$$\frac{\mathcal{N} \subseteq \mathcal{E}}{\mathsf{CInv}^{\gamma,\mathcal{N}}(P) * [\mathsf{CInv} : \gamma]_1 \Rrightarrow_{\mathcal{E}} \triangleright P}$$

VS-CINV

$$\frac{\triangleright P * Q_1 \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}} \triangleright P * Q_2 \qquad \mathcal{N} \subseteq \mathcal{E}}{\mathsf{CInv}^{\gamma,\mathcal{N}}(P) * [\mathsf{CInv} : \gamma]_q * Q_1 \Rrightarrow_{\mathcal{E}} \mathsf{CInv}^{\gamma,\mathcal{N}}(P) * [\mathsf{CInv} : \gamma]_q * Q_2}$$

HOARE-CINV

$$\frac{\{\triangleright P * Q_1\}\, e\, \{\triangleright P * Q_2\}_{\mathcal{E}\setminus\mathcal{N}} \qquad \mathsf{atomic}(e) \qquad \mathcal{N} \subseteq \mathcal{E}}{\left\{\mathsf{CInv}^{\gamma,\mathcal{N}}(P) * [\mathsf{CInv} : \gamma]_q * Q_1\right\} e \left\{\mathsf{CInv}^{\gamma,\mathcal{N}}(P) * [\mathsf{CInv} : \gamma]_q * Q_2\right\}_{\mathcal{E}}}$$

- CINV-ALLOC (新しい cancellable invariant)
  - $\mathsf{CInv}^{\gamma,\mathcal{N}}(P)$: 命題 P に対しての cancellable invariant の存在。
  - $[\mathsf{CInv}: \gamma]_q$: 有理数 q の分の token の所有権。
- CINV-SPLIT (所有権の分割)
- CINV-VALID (1 を超えるな)

CINV-TIMELESS

$$\mathsf{timeless}([\mathsf{CInv} : \gamma]_q)$$

CINV-PERSISTENT

$$\mathsf{persistent}(\mathsf{CInv}^{\gamma,\mathcal{N}}(P))$$

CINV-SPLIT

$$[\mathsf{CInv} : \gamma]_{q_1+q_2} \Leftrightarrow [\mathsf{CInv} : \gamma]_{q_1} * [\mathsf{CInv} : \gamma]_{q_2}$$

CINV-VALID

$$[\mathsf{CInv} : \gamma]_q \Rightarrow q \leq 1$$

CINV-ALLOC

$$\triangleright P \Rrightarrow_{\mathcal{E}} \exists \gamma.\, [\mathsf{CInv} : \gamma]_1 * \mathsf{CInv}^{\gamma,\mathcal{N}}(P)$$

CINV-CANCEL

$$\frac{\mathcal{N} \subseteq \mathcal{E}}{\mathsf{CInv}^{\gamma,\mathcal{N}}(P) * [\mathsf{CInv} : \gamma]_1 \Rrightarrow_{\mathcal{E}} \triangleright P}$$

VS-CINV

$$\frac{\triangleright P * Q_1 \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}} \triangleright P * Q_2 \qquad \mathcal{N} \subseteq \mathcal{E}}{\mathsf{CInv}^{\gamma,\mathcal{N}}(P) * [\mathsf{CInv} : \gamma]_q * Q_1 \Rrightarrow_{\mathcal{E}} \mathsf{CInv}^{\gamma,\mathcal{N}}(P) * [\mathsf{CInv} : \gamma]_q * Q_2}$$

HOARE-CINV

$$\frac{\{\triangleright P * Q_1\}\, e\, \{\triangleright P * Q_2\}_{\mathcal{E}\setminus\mathcal{N}} \qquad \mathsf{atomic}(e) \qquad \mathcal{N} \subseteq \mathcal{E}}{\left\{\boxed{P}^{\mathcal{N}} * Q_1\right\} e \left\{v.\, \boxed{P}^{\mathcal{N}} * Q_2\right\}_{\mathcal{E}}}$$

- CINV-CANCEL (cancel)
  - Full token を所有しているとき、invariant を cancel して、$\triangleright P$ の full ownership を取り返せる。その後は invariant には access できない。
- VS-CINV, HOARE-CINV (VS-INV と HOARE-INV と比較)

VS-INV

$$\frac{\triangleright P * Q_1 \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}} \triangleright P * Q_2 \qquad \mathcal{N} \subseteq \mathcal{E}}{\boxed{P}^{\mathcal{N}} * Q_1 \Rrightarrow_{\mathcal{E}} \boxed{P}^{\mathcal{N}} * Q_2}$$

HOARE-INV

$$\frac{\{\triangleright P * Q_1\}\, e\, \{v.\, \triangleright P * Q_2\}_{\mathcal{E}\setminus\mathcal{N}} \qquad \mathsf{atomic}(e) \qquad \mathcal{N} \subseteq \mathcal{E}}{\left\{\boxed{P}^{\mathcal{N}} * Q_1\right\} e \left\{v.\, \boxed{P}^{\mathcal{N}} * Q_2\right\}_{\mathcal{E}}}$$

Cancellable invariants の実装

先ほどの cancellable invariants は実装可能。Frac を使う。

$$[\mathsf{CInv} : \gamma]_q := \boxed{q : \mathit{Frac}}^{\gamma} \qquad \mathsf{CInv}^{\gamma,\mathcal{N}}(P) := \boxed{P \vee \boxed{1 : \mathit{Frac}}^{\gamma}}^{\mathcal{N}}$$

timeless($\boxed{q:Frac}^{\gamma}$)

CINV-TIMELESS

$$\mathsf{timeless}([\mathsf{CInv} : \gamma]_q)$$

persistent($\boxed{P}^{\mathcal{N}}$)

CINV-PERSISTENT

$$\mathsf{persistent}(\mathsf{CInv}^{\gamma,\mathcal{N}}(P))$$

Frac の性質

CINV-SPLIT $\boxed{q_1}^{\gamma} * \boxed{q_2}^{\gamma} \Leftrightarrow \boxed{q_1+q_2}^{\gamma}$

$$[\mathsf{CInv} : \gamma]_{q_1+q_2} \Leftrightarrow [\mathsf{CInv} : \gamma]_{q_1} * [\mathsf{CInv} : \gamma]_{q_2}$$

CINV-VALID

$$[\mathsf{CInv} : \gamma]_q \Rightarrow q \leq 1$$

$\boxed{a}^{\gamma} \Rightarrow \mathcal{V}(a)$

CINV-ALLOC $\exists\gamma.\ \boxed{1}^{\gamma} * \boxed{P \vee \boxed{1}^{\gamma}}^{\mathcal{N}}$

$$\triangleright P \Rrightarrow_{\mathcal{E}} \exists\gamma.\ [\mathsf{CInv} : \gamma]_1 * \mathsf{CInv}^{\gamma,\mathcal{N}}(P)$$

$\mathsf{True} \Rrightarrow_{\mathcal{E}} \exists\gamma.\ \boxed{1}^{\gamma}$ (VS-FRAME) と, $\triangleright P \Rightarrow \triangleright P \vee \boxed{1}^{\gamma} \Rightarrow \triangleright P \vee \triangleright \boxed{1}^{\gamma}$

$\Leftrightarrow \triangleright(P \vee \boxed{1}^{\gamma}) \Rrightarrow \boxed{P \vee \boxed{1}^{\gamma}}^{\mathcal{N}}$

CINV-CANCEL

$$\frac{\mathcal{N} \subseteq \mathcal{E}}{\mathsf{CInv}^{\gamma,\mathcal{N}}(P) * [\mathsf{CInv} : \gamma]_1 \Rrightarrow_{\mathcal{E}} \triangleright P}$$

$\boxed{P \vee \boxed{1}^{\gamma}}^{\mathcal{N}} * \boxed{1}^{\gamma} \Rrightarrow \triangleright P$

VS-CINV

$$\frac{\triangleright P * Q_1 \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}} \triangleright P * Q_2 \qquad \mathcal{N} \subseteq \mathcal{E}}{\mathsf{CInv}^{\gamma,\mathcal{N}}(P) * [\mathsf{CInv} : \gamma]_q * Q_1 \Rrightarrow_{\mathcal{E}} \mathsf{CInv}^{\gamma,\mathcal{N}}(P) * [\mathsf{CInv} : \gamma]_q * Q_2}$$

$(\triangleright P \vee \triangleright \boxed{1}^{\gamma}) * \boxed{1}^{\gamma}$

$\Leftrightarrow (\triangleright P * \boxed{1}^{\gamma}) \vee (\triangleright \boxed{1}^{\gamma} * \boxed{1}^{\gamma})$

$\Leftrightarrow \triangleright P * \boxed{1}^{\gamma}$

$\Rightarrow (\triangleright P \vee \triangleright \boxed{1}^{\gamma}) * \triangleright P$

$\boxed{P \vee \boxed{1}^{\gamma}}^{\mathcal{N}} * \boxed{1}^{\gamma} \Rrightarrow \boxed{P \vee \boxed{1}^{\gamma}}^{\mathcal{N}} * \triangleright P$

$\boxed{P \vee \boxed{1}^{\gamma}}^{\mathcal{N}} \vdash \boxed{1}^{\gamma} \Rrightarrow \boxed{P \vee \boxed{1}^{\gamma}}^{\mathcal{N}} * \triangleright P$

+

$\boxed{P \vee \boxed{1}^{\gamma}}^{\mathcal{N}} \vdash \boxed{P \vee \boxed{1}^{\gamma}}^{\mathcal{N}} * \triangleright P \Rrightarrow \triangleright P$

↳ 分岐 OK

HOARE-CINV

$$\frac{\{\triangleright P * Q_1\}\ e\ \{\triangleright P * Q_2\}_{\mathcal{E}\setminus\mathcal{N}} \qquad \mathsf{atomic}(e) \qquad \mathcal{N} \subseteq \mathcal{E}}{\left\{\mathsf{CInv}^{\gamma,\mathcal{N}}(P) * [\mathsf{CInv} : \gamma]_q * Q_1\right\} e \left\{\mathsf{CInv}^{\gamma,\mathcal{N}}(P) * [\mathsf{CInv} : \gamma]_q * Q_2\right\}_{\mathcal{E}}}$$

- より複雑な Rust style の cancellable invariant => §11 へ

But for now, we will focus on something else: one dissatisfying aspect of the specification above is that we had to *separately* prove VS-CINV and HOARE-CINV, and we were doing basically the same reasoning both times. It would be much more satisfying to be able to provide a single proof rule that can be used *both* to open cancellable invariants around view shifts, and around Hoare triples (and around anything else that might support opening invariants around it, like logically atomic triples[7]). For this purpose, Iris provides support for *mask-changing view shifts*.

-

5.3 Mask changing view shifts

- Hoare triple の invariant の展開の rule

$$\frac{\{\triangleright P * Q_1\}\, e\, \{v.\triangleright P * Q_2\}_{\mathcal{E}\setminus\mathcal{N}} \qquad \mathsf{atomic}(e) \qquad \mathcal{N} \subseteq \mathcal{E}}{\left\{\boxed{P}^{\mathcal{N}} * Q_1\right\} e \left\{v.\boxed{P}^{\mathcal{N}} * Q_2\right\}_{\mathcal{E}}}$$

- つまり、次の 3 ステップを使って、invariant から取り出す。

1. Open the invariant, obtaining $\triangleright P$ in the process.
2. Verify e (with a smaller mask).
3. Close the invariant, consuming $\triangleright P$ in the process.

- The core idea is that they can be viewed as a *view-shift that changes the current mask*.

1. Open the invariant, obtaining $\triangleright P$ in the process: $\mathsf{True} \;{}^{\mathcal{E}}\!\Rrightarrow^{\mathcal{E}\setminus\mathcal{N}} \triangleright P$.
2. Verify e (with a smaller mask): $\{\triangleright P * Q_1\}\, e\, \{v.\triangleright P * Q_2\}_{\mathcal{E}\setminus\mathcal{N}}$.
3. Close the invariant, consuming $\triangleright P$ in the process: $\triangleright P \;{}^{\mathcal{E}\setminus\mathcal{N}}\!\Rrightarrow^{\mathcal{E}} \mathsf{True}$.

- このモチベーションの元、次のようなルールを作りたい

INV-OPEN-FLAWED

$$\frac{\mathcal{N} \subseteq \mathcal{E}}{\boxed{P}^{\mathcal{N}} \;\; \mathcal{E} \Rrightarrow \mathcal{E} \setminus \mathcal{N} \;\; \triangleright P}$$

INV-CLOSE-FLAWED

$$\frac{\mathcal{N} \subseteq \mathcal{E}}{\boxed{P}^{\mathcal{N}} \;\; * \triangleright P \;\; \mathcal{E} \setminus \mathcal{N} \Rrightarrow \mathcal{E} \;\; \mathsf{True}}$$

-

HOARE-VS-ATOMIC

$$\frac{P \;\; \mathcal{E}_1 \Rrightarrow \mathcal{E}_2 \;\; P' \qquad \{P'\}\, e\, \{v.\, Q'\}_{\mathcal{E}_2} \qquad \forall v.\, Q' \;\; \mathcal{E}_2 \Rrightarrow \mathcal{E}_1 \;\; Q \qquad \mathsf{atomic}(e)}{\{P\}\, e_1\, \{v.\, Q\}_{\mathcal{E}_1}}$$

VS-REFL

$$P \;\; \mathcal{E} \Rrightarrow \mathcal{E} \;\; P$$

VS-TRANS

$$\frac{P \;\; \mathcal{E}_1 \Rrightarrow \mathcal{E}_2 \;\; Q \qquad Q \;\; \mathcal{E}_2 \Rrightarrow \mathcal{E}_3 \;\; R}{P \;\; \mathcal{E}_1 \Rrightarrow \mathcal{E}_3 \;\; R}$$

VS-FRAME

$$\frac{P \;\; \mathcal{E}_1 \Rrightarrow \mathcal{E}_2 \;\; Q}{P * R \;\; \mathcal{E}_1 \Rrightarrow \mathcal{E}_2 \;\; Q * R}$$

- しかし、(まだ読めていないので来週話しますが、)これは失敗する。
  - INV-OPEN-FLAWED と INV-CLOSE-FLOWED は素直には別々のルールとして採用できない。

- 別々のルールに分けて問題が発生したので、とりあえず別々のルールにすることを諦めればいい。

$$\frac{\mathcal{N} \subseteq \mathcal{E}}{\boxed{P}^{\mathcal{N}} \;\; \mathcal{E} \Rrightarrow^{\mathcal{E} \setminus \mathcal{N}} \left(\triangleright P * \exists R.\, R * \left(R * \triangleright P \;\; \mathcal{E} \setminus \mathcal{N} \Rrightarrow^{\mathcal{E}} \mathsf{True} \right) \right)}$$

- まあ、一応これで矛盾なくできるんだけど、複雑だし、やりたかったことではない。
- View-shift を modality としてみることで、うまくできる。

  => 5.5 でそれを観察するんだけど、5.4 で Hoare triple と modality の関係を先に考察しておく。