


Chapter 6 Paradoxes

contents

- § 6.1 Naive higher-order ghost state paradox
- § 6.2 Linear impredicative invariants paradox

abstract

§6.1 と §6.2 は共に Iris がどうして現在の形になっているかを説明する。

§6.1 は、later modality \triangleright が必要な理由を説明する。 \triangleright のない
ナイーヴな体系を考える。

True \Rightarrow False

が“證明” . ほぼ矛盾が示せたような事になる。

§6.2 は、なぜ線形非論理ではなく、affine な論理 ($P * Q \Rightarrow P$ が示せる)
を使うのかを説明する。線形非論理を使いたい motivation としては、
memory leak が起きづらいよう制御出来るから、というのが大きい。

しかし、実は Iris を例え線形而非論理で memory leak は防げない
ことが分かる。(これを paradox と呼んでいますが、矛盾ではない)
故に、affine にしない理由がありなし、

§ 6.1 Naive higher-order ghost state paradox

自己言及, はりこをして, 対角線論法, はく示す.

iProp (Iris の proposition 全体の集合) に依存した resource algebra を使った ghost state と, higher-order ghost state と呼ぶ.

higher-order ghost state は, core logic が 3 つ追加するのに便り.
しかし, 自己言及的故, 换かに注意が必要

$\text{Ag}_0(X)$ の X は iProp (iris の proposition 全体) を使う.

これは本当は Iris ではできない. (iProp は user がこの RA を使うが
(実際に決めるまで確定しないので, 循環定義))

Theorem 1 (Higher-order ghost state paradox)

$\text{Ag}_0(\text{iProp})$ のを使うが,

$$\text{True} \Rightarrow \text{False}$$

が証明可能.

idea.

X モリが無限にあることを利用して,

"あるアドレス r が存在して, r に allocate できる"

$$\frac{\text{True} \Rightarrow \exists r. \boxed{[\alpha]}}{\text{ghost-alloc}} \quad \text{or} \quad \text{一般化} \quad \frac{\forall r. \boxed{V(g(r))}}{\text{True} \Rightarrow \exists r. \boxed{[g(\beta)]}} \quad \text{ghost-alloc-dep}$$

を使うとして,

$$\text{True} \Rightarrow \exists r. \boxed{\text{Ag}_0(A(r))} \quad (*)$$

を示せる. また,

$$[\text{Ag}_0(P_1)] * [\text{Ag}_0(P_2)] \Rightarrow P_1 = P_2 \quad (**)$$

を使う矛盾.

証明.

$$A(r) := \exists p. \Box(p \Rightarrow \text{False}) * \boxed{\text{Ag}(p)}^r$$

$$Q(r) := \boxed{\text{Ag}(A(r))}^r$$

と定め。 $A(r)$ は、 r に、ある P が "allocate されていて、 P は矛盾している" ことを表す。
 $Q(r)$ は $\exists p. A(r) \wedge r = \text{allocate されている} = p$ を表す。

(*)より、 $\text{True} \Rightarrow \exists r. Q(r).$ (ある r に $A(r)$ が allocate されている)

$A(r)$ 成立

いま $A(r)$ が成立するなら、 $A(r)$ の定義から、 r が allocate されている 命題 P があり、
 P は矛盾する。 r が allocate されている のは $A(r)$ が "是"、 $A(r)$ は成立しない。

$A(r)$ 成立しない

逆もほぼ同様。 $A(r)$ が成立しない $\rightarrow r$ にある P は成り立た $\rightarrow A(r)$ は成り立たない。

$(*)$ は、 $r = A(r)$ と何とかか P が "allocate されている" なら、 その P は
 $A(r)$ である、 という形で使用する

□

Saved propositions soundly

$\text{Ag}(\text{iProp})$ は $\forall x \exists y$ が、 $\text{Ag}(\blacktriangleright \text{iProp})$ が $\forall x$ なも $(\blacktriangleright$ は未定義)
 $\exists \blacktriangleright$ で導入の paradox を避けて健全に構成される。

$$r \mapsto P := \boxed{\text{Ag}(\text{next}(P))}^r$$

と定め。

$$\text{True} \Rightarrow \exists r. r \mapsto P$$

$$r \mapsto P_1 * r \mapsto P_2 \Rightarrow \blacktriangleright(P_1 = P_2)$$

すなはち、 $\exists r. r \mapsto P$ と $\exists r. r \mapsto P'$ は $\blacktriangleright(P = P')$ となる。

$$P \Leftrightarrow \neg \blacktriangleright P$$

が示せば、 これは大丈夫らしい。

↑ = もの △ = 傷入の△ motivation と言って良いかは怪しい。
あくまでも ↑ の △ の 活躍の 具体例で、"△ がなければ This は 矛盾する" という 話
は今は しない ような。

この 章で △ に 言及しているのは p.79 の Saved proposition, soundly と
直前で、それは ▲ 9 話の 前。

た"いい今 の 話は recursive な 定義が 危険 ので、それに
"later" の 種先を 保つ 制限を 謂う 必要が (3.1.3 出でますよな。
さて、今 話。

6.2 Linear impredicative invariants paradox.

$P * Q \Rightarrow P$ (the weakening rule) $\delta \vdash \exists x \in I \rightarrow \perp$

- 便利。"cleaning up" $\vdash \neg \top \wedge \neg \perp \vdash \perp$.

左に weakening を $\exists x \in I \rightarrow \perp$

- to verify the absence of memory leaks.
- the tricky concurrent algorithms we were verifying anyway assumed a GC. (\Rightarrow memory leak $\vdash \neg \top \wedge \neg \perp \vdash \perp$)

Even if Iris was linear, it could not be used to verify the absence of memory leaks. これは不可能。

Def.

[Emp : "resource を全くもたない" という命題]

$\{P\} \vdash \{v. \text{Emp}\}$ は、memory leak が無しとするべく表す、 \perp 。
impredicative Invariants を混ぜると、これは正しくない。

$P \Rightarrow \text{Emp}$ を weakening を使って Iris で説明する。
これは、linear separation logic では正確である。

$($ 緑線 \rightarrow Iris の $\{ \text{Emp} \}$ ref(0) $\{ \text{Emp} \}$ が示せてしまう $)$
青線の意味で自然な解釈ではない。

Impredicative invariants break linearity

Theorem 2 (Linear impredicative invariants paradox)

linear separation logic + impredicative cancellable invariants

cancellable invariant τ ,

token $[C_{Inv} : \tau]_g \vdash \perp \perp$ $[C_{Inv} : \tau]_g \not\vdash \text{Emp}$
これはなぜですか。

どう

$$P \Rightarrow_{\tau} \text{Emp}$$

どう証明可能。

特に

$$\triangleright P \Rightarrow_{\tau} \exists \gamma. [C_{Inv} : \gamma]_1 * C_{Inv}^{< N}(P)$$

$C_{Inv}\text{-Alloc}$

$$\frac{N \leq \varepsilon}{C_{Inv}^{< N}(P) \vdash [C_{Inv} : \tau]_g \rightarrow \stackrel{\varepsilon}{\not\Rightarrow} \text{Emp}}$$

$C_{Inv}\text{-Acc-Strong}$

$$(\triangleright P * [C_{Inv} : \tau]_g * (\triangleright P \rightarrow \stackrel{\varepsilon}{\not\Rightarrow} \text{Emp}))$$

なぜ。

次と $C_{Inv}\text{-Alloc}$ どう Theorem 2 は証明できません。 ($\triangleright \text{True} \Rightarrow \text{Emp}$ です)

Lemma 2. 次が証明可能

$$C_{Inv}^{< N}(\text{True}) * [C_{Inv} : \tau]_1 \Rightarrow_{\tau} \text{Emp}.$$

proof.

$C_{Inv}\text{-Acc-Strong}$ を使えば、左の式の view shift は

$$[C_{Inv} : \tau]_1 * \triangleright \text{True} * ((\triangleright \text{True}) \rightarrow \stackrel{< N}{\not\Rightarrow} \text{Emp})$$

が得られるので、これは Emp の view shift を得ることができます。左

右側の 2つを使えば Emp を得ることができます。 $[C_{Inv} : \tau]_1$ が残るまでは。

今、 $\forall Q, Q \rightarrow \text{True} \Leftarrow \text{True} \vdash \triangleright \text{True}$ を使えば、

$$[C_{Inv} : \tau]_1 * \triangleright \text{True} \rightarrow \triangleright \text{True}$$

が得られます。これと一番右の式を \wedge

$Q \rightarrow \text{True} \quad \text{True} \rightarrow \triangleright \text{True}$

$$Q = [C_{Inv} : \tau]_1 * \triangleright \text{True}$$

$[C_{Inv}: r], * \Delta \text{True} \xrightarrow{* \models}^{\tau^{Inv}} \top \text{Emp}$

心得是 R2, => C 左 + 中央 2" modus ponens 也是 Emp 的推导.

VST-frame work, Iron 什么,