

Return

$$\overline{\Gamma; \nu; \{f_1\} \rightsquigarrow \{ \exists \vec{z}. (f_2 \wedge \text{res} = e) \} \mid \text{return } e;}$$

$$f_1 \vdash \exists \vec{z}. f_2, \\ \text{fv}(e) \subseteq \nu$$

$$\overline{\Gamma; \nu; [f_1] \rightsquigarrow [\text{ok}; \exists \vec{z}. (f_2 \wedge \text{res} = e)] \mid \text{return } e;}$$

$$? \quad f_1 \vdash \exists \vec{z}. f_2, \\ \text{fv}(e) \subseteq \nu$$

Read

$$\Gamma; \nu \cup \{v\}; \{ \Sigma, * u \mapsto (\text{fld} : t) \wedge \pi, \wedge v = t \} \\ \rightsquigarrow \{f_2\} \mid C$$

$$\Gamma; \nu; \{ \Sigma, * u \mapsto (\text{fld} : t) \} \wedge \pi, \rightsquigarrow \{f_2\} \mid \text{typ } v = \\ u \mapsto \text{fld} = t;$$

(fld \rightarrow field of
data)

(typ \rightarrow variable type)

$$\boxed{\begin{array}{l} u \in V \\ v \notin V \end{array}} \rightarrow$$

Call

$$\Gamma \cup \{ \{G_1\} \text{ frame } (\vec{u}) \{G_2\} \}; \nu \in \{w\} \cdot \{F_1 \\ \times G_2 \ominus [\nu / res] \} \rightsquigarrow \{F_2\} / C$$

$$\Gamma \cup \{ \{G_1\} \text{ frame } (\vec{u}) \{G_2\} \}; \nu; \{F_1 \neq F_2\} \rightsquigarrow \{F_2\} / \text{fp } \nu \\ = \text{frame } (\vec{u} \ominus); C$$

$$G_1 \ominus = F, \\ \text{fv}(\vec{u} \ominus) \in V$$

< same for
(sc) >

Examples (attempts)

from paper

$$(\exists L. n \vdash L \neq L \vdash \text{nil} \wedge X = \text{nil} \wedge L \neq \text{nil}) \\ \text{from } C \text{ (set}(n, g))$$

$$\text{ex: } (\exists L. n \vdash L \neq L \vdash \text{nil} \wedge X = \text{nil} \wedge L \neq \text{nil})$$

$$\text{ex: } [y \vdash Y \neq v \vdash V \neq (z \mapsto W) \neq Y \mapsto W \wedge Z = \text{nil} \wedge \\ \text{error} \leftarrow (w = \text{nil})]$$

(z) = y
write)

OK version?

$$\text{OK: } (z \mapsto Z \neq Z \mapsto V \neq y \mapsto Y) (Z) := y [z \mapsto X \neq X \mapsto Y \neq \\ y \mapsto Y]$$

1- replace error triple with exc version of the triple?

2- neg & k disjunct frame that forces errors?

1) $[y \mapsto Y * r \mapsto V * z \mapsto W * \gamma \mapsto W \wedge Z = \text{nil}]$
replace

Write

$$[y \mapsto Y * r \mapsto V * z \mapsto W * \gamma \mapsto W \wedge \underbrace{W \mapsto V}_{\wedge Z = \text{nil}}]$$

2) $[y \mapsto Y * r \mapsto V * z \mapsto W * \gamma \mapsto W \wedge Z = \text{nil} \wedge \underbrace{W \neq \text{nil}}]$
negate frame

Write

$$[y \mapsto Y * r \mapsto V * z \mapsto W * \gamma \mapsto W \wedge Z = \text{nil} \wedge \underbrace{W \mapsto V}]$$

- Can the above be used as VC's?

- Can they be directly used as pre & post?

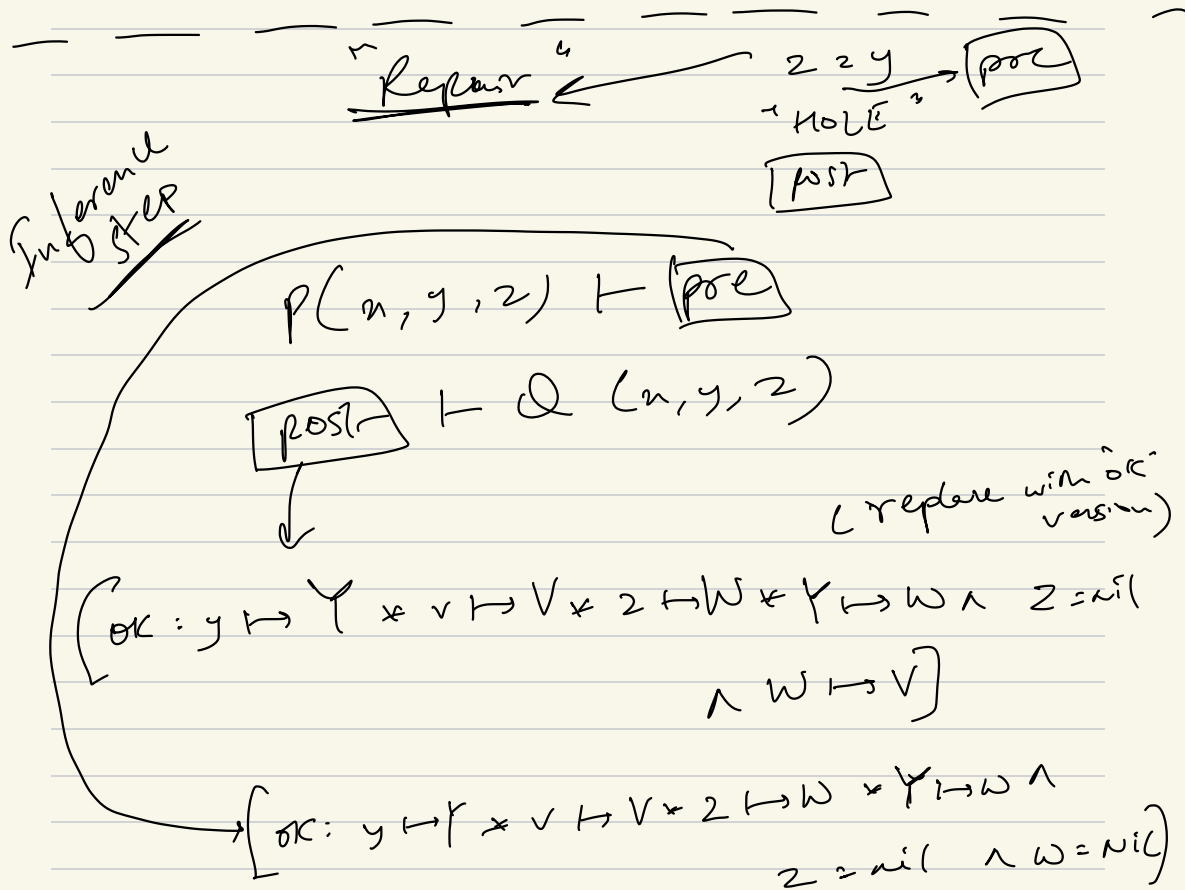
→ more rules? (early return, error out, assume false, remove param)

if (a) return; error();

no-op delete ??

skip() (if post condition still satisfied)

all of this possible because under-approximation



$$\boxed{\text{OK:}} \quad (y \vdash Y * v \vdash V * z \vdash W * Y \vdash W * w \vdash V \mid - \quad \textcircled{Q * K} \quad \dots \textcircled{1} \quad \text{unknown})$$

$$\wedge z = \text{nil}]$$

$$\textcircled{P * K} \vdash [y \vdash Y * v \vdash V * z \vdash W * Y \vdash W \wedge \dots \textcircled{2} \quad \text{OK:} \quad z = \text{nil} \wedge w = \text{nil}]$$

unknown

$$Q \stackrel{\text{def}}{=} (y \vdash Y * v \vdash V * z \vdash W * Y \vdash W * w \vdash V \mid - \quad \wedge z = \text{nil}) \quad \checkmark$$

$$\textcircled{K} \stackrel{\text{def}}{=} [\text{emp} \wedge z = \text{nil}]$$

→ substituting K in (2) →

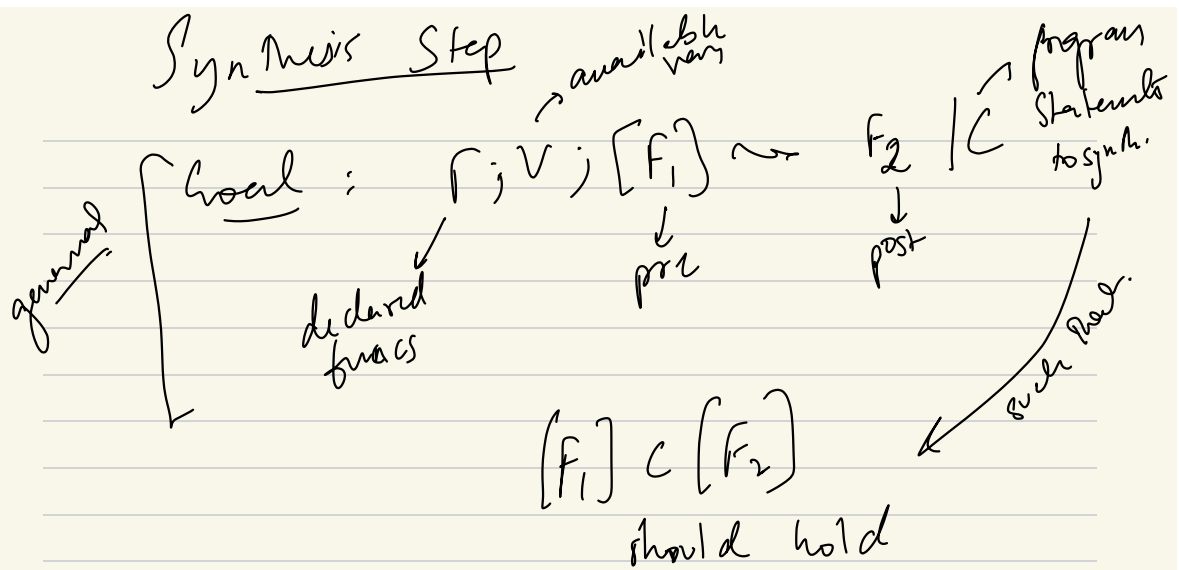
$$P \wedge \underline{z = \text{nil}} \vdash [y \vdash Y * v \vdash V * z \vdash W * Y \vdash W \wedge z = \text{nil} \wedge w = \text{nil}]$$

$$\downarrow$$

$$z = \text{nil} \not\vdash z = \text{nil} \wedge w = \text{nil} \quad ?$$

$$\downarrow \quad \textcircled{U_2} \quad ?$$

$$P \stackrel{\text{def}}{=} [y \vdash Y * v \vdash V * z \vdash W * Y \vdash W \wedge z = \text{nil} \wedge w = \text{nil}]$$

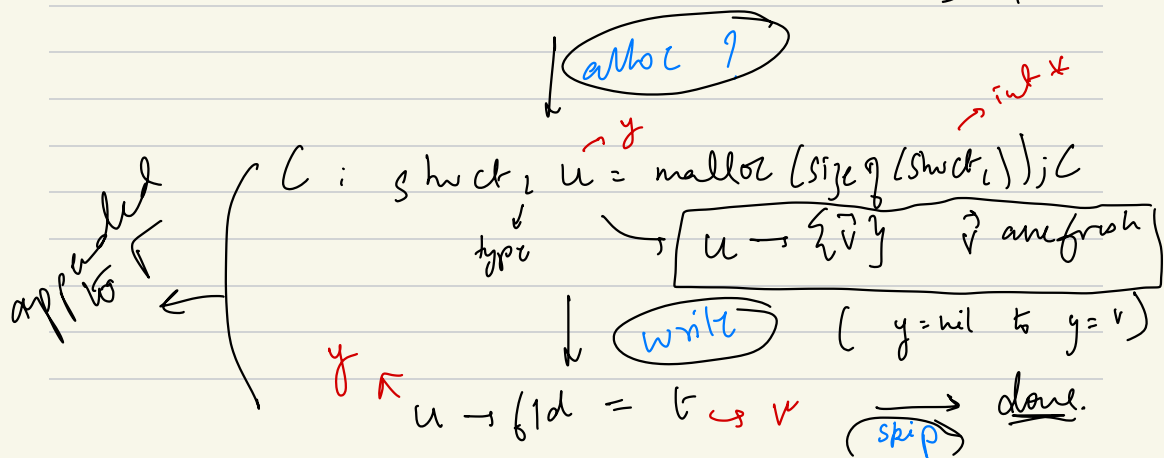


from previous page.

Sketchy point

$\Gamma; V; [y \vdash Y * v \vdash V * z \vdash W * Y \vdash W \wedge z = \text{nil} \wedge W = \text{nil}]$

$\rightsquigarrow [y \vdash Y * v \vdash V * z \vdash W * Y \vdash W * W \vdash V \wedge z = \text{nil}] \mid C$



Candidate for

$\text{int } x; y = \text{malloc}(\text{sizeof}(\text{int } x));$ } in
 $y = &v; \quad (\text{with } V)$ } scope)
→ to be satisfied?

↳ verify with Infer.

→ technically
correct

Question

- what if NPE is expected?
- Do early-return files work?