Malloc works. Proof

Assume lemma conditions and show

$(n, (reg, ms)) \in \mathcal{O}(W)$

Use anti red. lemma. let ms_f be given, then

$(reg, ms \uplus ms_f) \to^{i} (reg[pc \mapsto upp(c_{malloc}), r_0 \mapsto c_{ret}], ms \uplus ms_f)$

From $ms :_n W$ and $W \exists^{priv} [i \mapsto \iota_{malloc,0}]$ we get ms_{foot} and ms' s.t.

$ms_{foot} :_n [W(i)]$ and

$ms = ms_{foot} \uplus ms'$

$\to^{i'} (reg[pc \mapsto upp(c_{ret}), r_1 \mapsto ((rwx, global), b, e, a)], ms_{foot}' \uplus ms' \uplus ms_{alloc})$

$\begin{array}{l} reg(r_0) \\ [r_m \mapsto ms_{foot}(a)] \\ [r_0 \mapsto c_{ret}] \end{array}$

ms_{alloc} all 0.
(and so on)

$\to^{i''} (reg[pc \mapsto c_{next}][r \mapsto ((rwx, global), b, e, a)], ms_{foot}' \uplus ms' \uplus ms_{alloc})$

Show: $i'' \leq n-1$ ✓

- $\iota_{malloc} \sqsupseteq^{pub} W(i)$: malloc spec ✓
- $ms'_{foot} \uplus ms' :_{i''} W[i \mapsto \iota_{malloc}]$

Follows from

$ms_{foot} \uplus ms' :_n W$

use same partition.

regions respect pub fut. worlds

$(n, (ms_{foot}')) \in H_{malloc}$ — $[i \mapsto \iota_{malloc}]$

$\Rightarrow$ — — $W[i \mapsto \iota_{malloc}]$

- reg' ... ✓
- $end - base = k-1$: malloc spec ✓
- dom ... — " —
- $\forall a \in$ ... — " —

$(i'', (reg', ms' \uplus ms_{foot}' \uplus ms_{alloc})) \in \mathcal{O}(W)$

done.

Proof Cstcls works.

Make the assumptions of the lemma

And show

$(n, (reg, ms)) \in \mathcal{O}(W)$

~~Use anti-reduction lemma, so let ms_f be given, then~~

~~$((reg, ms \uplus ms_f)) \to$~~

At this point,

(reg, ms) points to malloc r_{t1} n w/ c_{next} next,

so use malloc correctness lemma

SFTS Hyp-Cont

assume $n' \leq n-1$

c_{malloc} $\supseteq \mathcal{W}f{:}?$

$ms_{footprint}' \uplus ms' :_{n'} W[i \mapsto c_{malloc}]$

$ms_{footprint}' :_{n'} [i \mapsto c_{malloc}]$

c_{next}' pc

$reg'(r') = ((rw+, global), base_{env}, end_{env}, base_{env})$ r_{t1}

$reg(r)$ $\notin \{pc, r_{t1}, r_1\}$

Le

Show

$(n', (reg, ms' \uplus ms_{footprint}' \uplus \tilde{ms_{env}})) \in \mathcal{O}(W[c_{malloc}]$

Use anti red lemma. Let ms_f be given, then

$(reg', ms' \uplus ms_{footprint}' \uplus \tilde{ms_{env}}) \longrightarrow$

$(reg'', ms'' \uplus ms_{footprint}' \uplus ms_{env})$

where ms_{env} "=" $reg(r_{env})$

and

$reg''(r_{t1}) = reg'(r_{t1})$ $= c_{env}$ w/ perm rw.

except for pc

$reg''(r) = reg'(r)$

and

$(reg'', ms' \uplus ms_{footprint}' \uplus ms_{env})$ is looking at malloc r_1 8 w/ c_{next}' next

Now SFTS show

$(n', (reg'', ms' \uplus ms_{footprint}' \uplus ms_{env})) \in \mathcal{O}(W[c_{malloc}]$

$[i_{sta}(tmp, ms_{env})]]$

To this end use malloc cor. lemma.

specifically:

$ms' \uplus ms_{footprint}' \uplus ms_{env} :_{n'} W[c_{malloc}, i_{sta}(tmp, ms_{env})]]$

because assumption + sta lemma + disj union mem sat lemma.

SFTS Hyp-Cont i.e.

assume

$n'' \leq n' - 1$

$\iota'_{malloc} \sqsupseteq^{pub} W(i)$

$ms''_{codeprint} \uplus ms' \uplus ms_{env} : n'' \; W[\iota'_{malloc}, \iota^{sta}(temp, ms_{env})]$

$ms''_{footprint} : [\iota'_{malloc}]$

$$reg'''(r') = \begin{cases} c_{next}'' & pc \\ ((rwx, global), b, e, b) & r_1 \\ reg''(r) & \notin pc, r_1 \end{cases}$$

$e - b = 7$

$dom(\tilde{ms}_{act}) = [b, e]$

all 0!

Show

$(n'', (reg'', ms' \uplus ms''_{footprint} \uplus ms_{env} \uplus \tilde{ms}_{act}))$

$\quad \in O(W[\iota'_{malloc}, \iota^{sta}(temp, ms_{env})]])$

Use anti-red lemma. Know:

$(reg''', ms' \uplus ms''_{footprint} \uplus ms_{env} \uplus \tilde{ms}_{act}) \to^{-}$

$\quad (reg^{(4)}, ms' \uplus ms''_{footprint} \uplus ms_{env} \uplus ms_{act})$

where

$ms_{act}(b, b+1) = reg(r_{code}), c_{env}$

$ms_{act}(b+2, \ldots, b+6) = i_1, \ldots, i_6$

$reg^{(4)}(pc) = c_{next}$, $reg^{(4)}(r_1) = ((e, global), b, e, b+2)$

$reg^{(4)}(r) = reg^{(3)}(r)$ o/w

Use the Hyp-Cond assumed in Catch's lemma.

To get

$(reg^{(4)}, ms' \uplus ms''_{footprint} \uplus ms_{env} \uplus ms_{act})$

$\quad \in O(W[\iota^{sta}(temp, ms_{env}), \iota'_{malloc}]])$

SFTS given .... let $k = 6$