

Recitation 4: completed

Recitation 4

Announcements

- New quiz deadlines: Sat 10pm + Mon 10pm

Today

- KeyMacra X demo
- Quantifier rules and Freshness
- When programs don't matter: V and G

Quantifier rules and freshness

Rules for quantifiers

$$\begin{array}{c} \forall R \\ \uparrow \\ \text{right rule} \end{array} \quad \frac{\Gamma \vdash P(y), \Delta}{\Gamma \vdash \forall x P(x), \Delta} \quad \begin{array}{l} \text{let's ignore these at first} \\ (y \text{ fresh}) \\ (y \notin \{\Gamma, \Delta, \forall x P(x)\}) \end{array}$$

Why $y \notin \Gamma$?

$$\begin{array}{c} * \\ \hline x=0 \vdash x=0 \\ \hline x=0 \vdash \forall x (x=0) \end{array} \quad \begin{array}{l} ;d \\ (yR) \text{ wrong} \end{array}$$

Not valid

Why $y \notin \forall x P(x)$?

$$\begin{array}{c}
 \frac{\frac{*}{\vdash y \cdot y \geq 0} \text{ qE}}{\vdash \forall x (x \cdot y \geq 0)} \text{ } \forall R \text{ (wrong)} \\
 \text{not valid}
 \end{array}$$

$$\forall L \quad \frac{\Gamma, P(e) \vdash \Delta}{\Gamma, \forall x P(x) \vdash \Delta} \text{ (e term)}$$

Existential quantifiers

We have $\exists x P \leftrightarrow \neg (\forall x \neg P)$
(\exists axiom)

$$\begin{array}{c}
 \frac{\Gamma \vdash P(e)}{\quad} \neg L \\
 \left. \begin{array}{c}
 \frac{\Gamma, \neg P(e) \vdash \cdot}{\quad} \forall L \quad \text{(e term)} \\
 \frac{\Gamma, \forall x \neg P(x) \vdash \cdot}{\quad} \neg R \\
 \frac{\Gamma \vdash \neg (\forall x \neg P(x))}{\quad} \exists I
 \end{array} \right\} \exists e \\
 \frac{\quad}{\Gamma \vdash \exists x P(x)}
 \end{array}$$



$$\vdash \Gamma \vdash P(e), \Delta \quad \text{... } \vdash$$

$$\exists K \quad \frac{}{\Gamma \vdash \exists x P(x), \Delta} \quad (x \text{ free})$$

$$\exists L \quad \frac{\Gamma, P(y) \vdash \Delta}{\Gamma, \exists x P(x) \vdash \Delta} \quad (y \text{ fresh})$$

Example:

$$\begin{array}{l} \frac{}{\vdash u + (-u) = 0} \quad \mathcal{R} \text{ (QE)} \\ \frac{}{\vdash \exists y \quad u + y = 0} \quad \mathcal{R} \quad y \text{ fresh} \\ \frac{}{\vdash \forall x \exists y \quad x + y = 0} \quad \mathcal{R} \quad (u \text{ fresh}) \end{array}$$

$[\cdot := \cdot]$ axiom

$$[\cdot := \cdot] \quad [x := e] \, p(x) \leftrightarrow p(e)$$



Only replace free instances of x

No free var in e should get bound in $p(e)$

not provable (as expected)

$$\frac{y = -3 \vdash (y+1) \geq 0}{y = -3 \vdash [x := y+1] x \geq 0} [i=]$$

$$y = -3 \vdash [x := y+1] x \geq 0$$

$$y = -3 \vdash [x := y+1] [\boxed{x = x+1} \boxed{x \geq 0}]$$

↑ FREE (substituted)

BOUND
(not substituted)

not valid

BOUND!

$$\frac{\vdash \forall y (y \geq 0)}{\vdash [x := y] (\forall y x \cdot y \geq 0)} [i=] \text{ (wrong)}$$

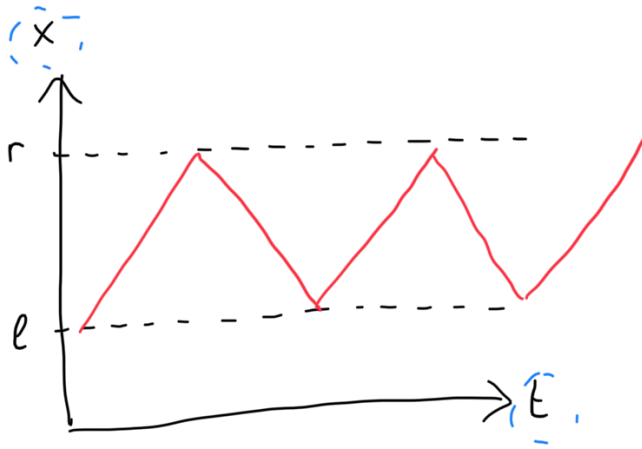
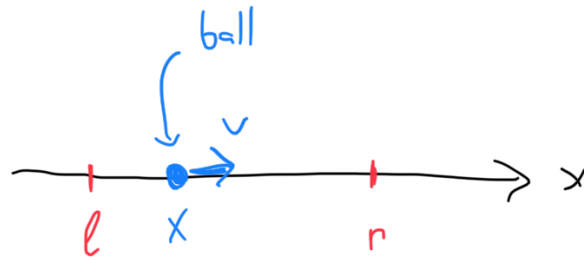
[i=] (wrong)

$$\vdash [x := y] (\forall y x \cdot y \geq 0)$$

↑ FREE

KeyMaera X Demo

An event-triggered, 1D ping pong controller



Highlight: V , G and GV

V $p \rightarrow [\alpha] p \quad (FV(p) \cap BV(\alpha) = \emptyset)$

$$\begin{array}{c}
 \frac{*}{x=0 \vdash x=0} \text{ id} \\
 \hline
 x=0 \vdash \underbrace{[y:=1]}_{\text{does not write } x} x=0 \quad \checkmark
 \end{array}$$

$$\underline{G} \quad \frac{P}{\Gamma \vdash [\varphi] P}$$

$$\begin{array}{c}
 \frac{\frac{*}{\vdash x^2 \geq 0} \text{ IR}}{x \geq 1 \vdash [x:=x+1] x^2 \geq 0} G
 \end{array}$$

KeyMaera X GV tactic:

what remains to be proved after calling GV

$$\begin{array}{c}
 \underbrace{x = -1 \vdash \forall v \ x \leq v^2} \\
 \hline
 x = -1 \vdash [\{v' = 5\}] \wedge x \leq v^2 \quad \quad \quad \frac{*}{\vdash (\forall v \ x \leq v^2) \rightarrow x \leq v^2} \quad R \\
 \hline
 \quad \quad \quad M \\
 \underbrace{x = -1 \vdash [\{v' = 5\}] \ x \leq v^2}
 \end{array}$$

Neither G nor V are applicable

Here is what KeyMaera X "GV" tactic would do.

$$\left(\text{Monotonicity rule} \right)$$

$$M \quad \frac{\Gamma \vdash [\phi] P \quad \vdash P \rightarrow Q}{\Gamma \vdash [\phi] Q}$$

