Recitation 4: completed

Recitation 4

Announcements

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

Today

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

Quantifier rules and freshness

Rules for quantifiers

let's ignore these at first

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

$\forall R$: right rule

$(y \notin \{\Gamma, \Delta, \forall x P(x)\})$

Why $y \notin \Gamma$?

$$\dfrac{\dfrac{*}{x=0 \vdash x=0}\,id}{x=0 \vdash \forall x\,(x=0)}\,(\forall R) \text{ wrong}$$

Not valid

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

$$\dots \quad \frac{\dfrac{*}{\vdash y \cdot y \geq 0}\ \forall E}{\vdash \forall x\ (x \cdot y \geq 0)}\ \forall R \text{ (wrong)}$$

not valid

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

Existential quantifiers

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

($\exists$d axiom)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma \vdash P(e)}{\Gamma, \neg P(e) \vdash \cdot}\,\neg L}{\Gamma, \forall x \neg P(x) \vdash \cdot}\,\forall L \quad (e \text{ term})}{\Gamma \vdash \neg(\forall x \neg P(x))}\,\neg R}{\Gamma \vdash \exists x P(x)}\,\exists E$$

$\exists E$

$$\Downarrow$$

$$\Gamma \vdash P(e), \Delta \qquad (e \text{ term})$$

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

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

Example:

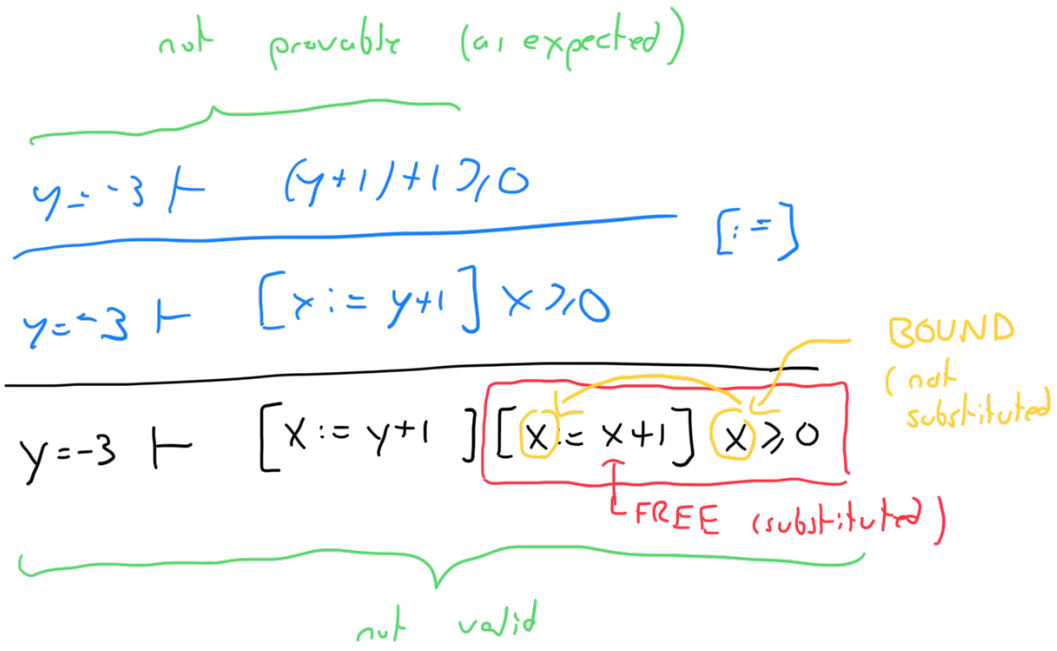
$$\dfrac{\dfrac{\dfrac{}{\vdash\ u + (-u) = 0}\ \mathbb{R}\ (QE)}{\vdash\ \exists y\ u + y = 0}\ \exists R\ \ y \leftarrow -u}{\vdash\ \forall x\ \exists y\ x + y = 0}\ \forall R\ (u \text{ fresh})$$

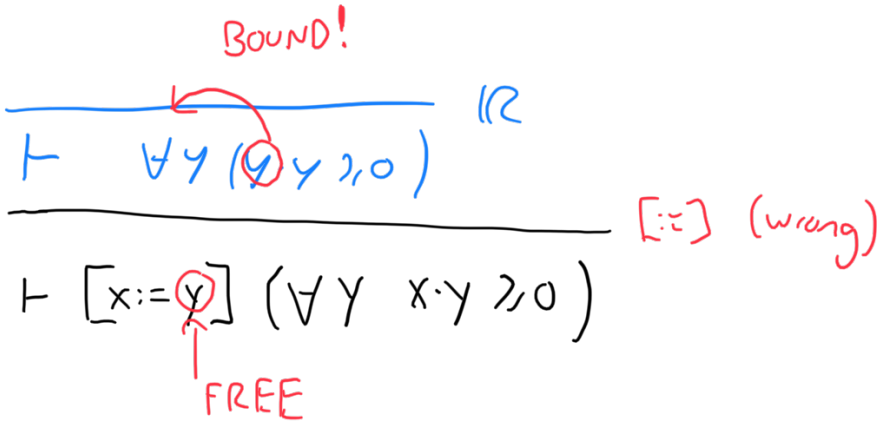
$[:=]$ axiom

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

⚠

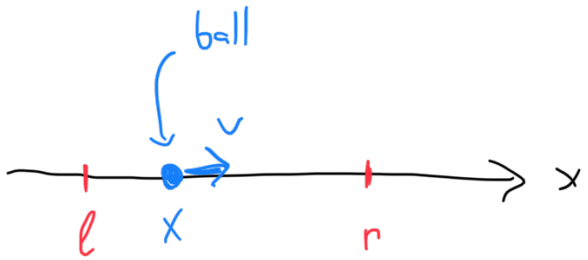
- Only replace free instances of x
- No free var in e should get bound in $p(e)$

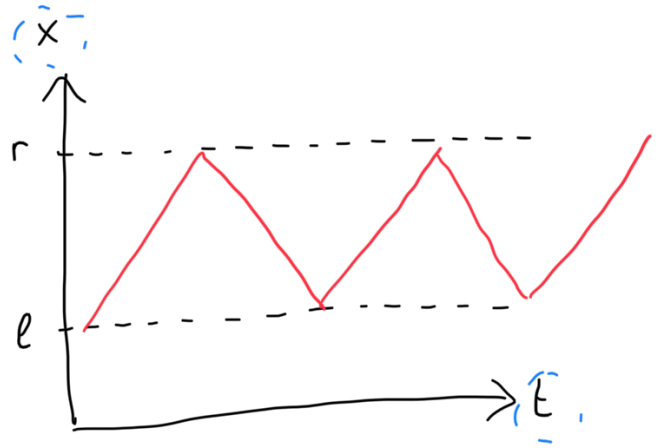




KeyMaera X Demo

An event-triggered, 1D ping pong controller





Highlight: V, G and GV

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

$$\dfrac{\dfrac{*}{x=0 \vdash x=0}\,id}{x=0 \vdash [y:=1]\,x=0}\,V$$

does not write x

$$\underline{G}\quad \dfrac{P}{\Gamma \vdash [\alpha]\,P}$$

$$\dfrac{\dfrac{*}{\vdash x^2 \geq 0}\,R}{x \geq 1 \vdash [x:=x+1]\,x^2 \geq 0}\,G$$

KeyMaeara X GV tactic:

what remains to be proved after calling GV

$$\dfrac{\dfrac{x=-1 \vdash \forall v\ x \leqslant v^2}{x=-1 \vdash [\{v'=5\}]\ \forall\ x \leqslant v^2}\,V \qquad \dfrac{*}{\vdash (\forall v\ x \leqslant v^2 \rightarrow x \leqslant v^2}\,R}{x=-1 \vdash [\{v'=5\}]\ x \leqslant v^2}\,M$$

Neither G nor V are applicable

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

Monotonicity rule

$$M\ \dfrac{\Gamma \vdash [a]P \qquad \vdash P \rightarrow Q}{\Gamma \vdash [a]Q}$$