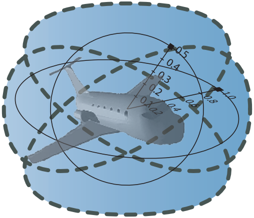
06: Truth & Proof

15-424: Foundations of Cyber-Physical Systems

André Platzer

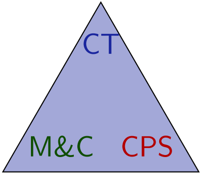
aplatzer@cs.cmu.edu
Computer Science Department
Carnegie Mellon University, Pittsburgh, PA



Outline

Outline

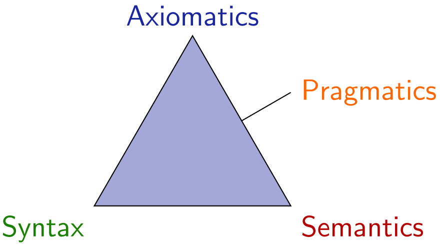
systematic reasoning for CPS
verifying CPS models at scale
pragmatics: how to use axiomatics to justify truth
structure of proofs and their arithmetic



discrete+continuous relation
with evolution domains

analytic skills for CPS

Logical Trinity with Extra Leg



Syntax	defines the notation What problems are we allowed to write down?
Semantics	what carries meaning. What real or mathematical objects does the syntax stand for?
Axiomatics	internalizes semantic relations into universal syntactic transformations.
Pragmatics	how to use axiomatics to justify syntactic rendition of semantical concepts. How to do a proof?

Outline

Sequent Calculus

Definition (Sequent)

$$\Gamma \vdash \Delta$$

has the same meaning as $\bigwedge_{P\in\Gamma} P \rightarrow \bigvee_{Q\in\Delta} Q$.
The *antecedent* Γ and *succedent* Δ are finite sets of dL formulas.

Definition (Soundness of sequent calculus proof rules)

$$\frac{\Gamma_1 \vdash \Delta_1 \quad \dots \quad \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta}$$

is *sound* iff validity of all premises implies validity of conclusion:

$$\text{If } \vDash (\Gamma_1 \vdash \Delta_1) \text{ and } \dots \text{ and } \vDash (\Gamma_n \vdash \Delta_n) \text{ then } \vDash (\Gamma \vdash \Delta)$$

Sequent Calculus

Definition (Sequent)

$$\Gamma \vdash \Delta$$

has the same meaning as $\bigwedge_{P \in \Gamma} P \rightarrow \bigvee_{Q \in \Delta} Q$.
The *antecedent* Γ and *succedent* Δ are finite sets of dL formulas.

Definition (Soundness of sequent calculus proof rules)

construct proofs ↑

$$\frac{\Gamma_1 \vdash \Delta_1 \quad \dots \quad \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta}$$

is *sound* iff validity of all premises implies validity of conclusion:

$$\text{If } \vDash (\Gamma_1 \vdash \Delta_1) \text{ and } \dots \text{ and } \vDash (\Gamma_n \vdash \Delta_n) \text{ then } \vDash (\Gamma \vdash \Delta)$$

Sequent Calculus

Definition (Sequent)

$$\Gamma \vdash \Delta$$

has the same meaning as $\bigwedge_{P\in\Gamma} P \rightarrow \bigvee_{Q\in\Delta} Q$.
The *antecedent* Γ and *succedent* Δ are finite sets of dL formulas.

Definition (Soundness of sequent calculus proof rules)

construct proofs ↑

$$\frac{\Gamma_1 \vdash \Delta_1 \quad \dots \quad \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta}$$

↓ validity transfers

is *sound* iff validity of all premises implies validity of conclusion:

$$\text{If } \vDash (\Gamma_1 \vdash \Delta_1) \text{ and } \dots \text{ and } \vDash (\Gamma_n \vdash \Delta_n) \text{ then } \vDash (\Gamma \vdash \Delta)$$

Developed on the board:

1. Proof rules for propositional logic
2. Proofs with dynamics
3. Contextual equivalence rewriting / congruence
4. Quantifier proof rules
5. Structural proof rules

See lecture notes for details [1].

Simple Propositional Example Proof in Sequent Calculus

$$\frac{}{\vdash v^2 \leq 10 \land b>0 \rightarrow b>0 \land (\neg(v \geq 0) \lor v^2 \leq 10)}$$

Simple Propositional Example Proof in Sequent Calculus

$$\to\text{R}\ \frac{v^2\leq 10 \land b>0 \vdash b>0 \land (\neg(v\geq 0) \lor v^2\leq 10)}{\vdash v^2\leq 10 \land b>0 \to b>0 \land (\neg(v\geq 0) \lor v^2\leq 10)}$$

Simple Propositional Example Proof in Sequent Calculus

$$\wedge R \frac{\overline{v^2 \le 10 \wedge b>0 \vdash b>0} \qquad \overline{v^2 \le 10 \wedge b>0 \vdash \neg(v \ge 0) \vee v^2 \le 10}}{v^2 \le 10 \wedge b>0 \vdash b>0 \wedge (\neg(v \ge 0) \vee v^2 \le 10)}$$

$$\to R \frac{v^2 \le 10 \wedge b>0 \vdash b>0 \wedge (\neg(v \ge 0) \vee v^2 \le 10)}{\vdash v^2 \le 10 \wedge b>0 \to b>0 \wedge (\neg(v \ge 0) \vee v^2 \le 10)}$$

Simple Propositional Example Proof in Sequent Calculus

$$
\dfrac{
\wedge L\ \dfrac{\dfrac{}{v^2\le 10, b>0 \vdash b>0}}{v^2\le 10 \wedge b>0 \vdash b>0}
\qquad
\dfrac{}{v^2\le 10 \wedge b>0 \vdash \neg(v\ge 0) \vee v^2\le 10}
}{
\wedge R\ \dfrac{v^2\le 10 \wedge b>0 \vdash b>0 \wedge (\neg(v\ge 0) \vee v^2\le 10)}{\to R\ \vdash v^2\le 10 \wedge b>0 \to b>0 \wedge (\neg(v\ge 0) \vee v^2\le 10)}
}
$$

$$
\dfrac{\dfrac{\dfrac{*}{v^2\leq 10, \color{red}{b>0} \vdash \color{red}{b>0}}\ \text{id}}{v^2\leq 10 \land b>0 \vdash b>0}\ \land\text{L} \qquad \dfrac{}{v^2\leq 10 \land b>0 \vdash \neg(v\geq 0) \lor v^2\leq 10}}{\dfrac{v^2\leq 10 \land b>0 \vdash b>0 \land (\neg(v\geq 0) \lor v^2\leq 10)}{\vdash v^2\leq 10 \land b>0 \rightarrow b>0 \land (\neg(v\geq 0) \lor v^2\leq 10)}\ \rightarrow\text{R}}\ \land\text{R}
$$

Simple Propositional Example Proof in Sequent Calculus

$$
\dfrac{
\dfrac{
\dfrac{*}{v^2\leq 10, b>0 \vdash b>0}\,\text{id}
}{v^2\leq 10 \land b>0 \vdash b>0}\,\land\text{L}
\qquad
\dfrac{
\dfrac{}{v^2\leq 10 \land b>0 \vdash \neg(v\geq 0), v^2\leq 10}
}{v^2\leq 10 \land b>0 \vdash \neg(v\geq 0) \lor v^2\leq 10}\,\lor\text{R}
}{
\dfrac{v^2\leq 10 \land b>0 \vdash b>0 \land (\neg(v\geq 0) \lor v^2\leq 10)}{\vdash v^2\leq 10 \land b>0 \to b>0 \land (\neg(v\geq 0) \lor v^2\leq 10)}\,\to\text{R}
}\,\land\text{R}
$$

Simple Propositional Example Proof in Sequent Calculus

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{*}{v^2{\le}10,\, b{>}0 \vdash\ b{>}0}\ \text{id}
    }{v^2{\le}10 \land b{>}0 \vdash\ b{>}0}\ \land\text{L}
    \qquad
    \dfrac{
      \dfrac{
        \overline{v^2{\le}10,\, b{>}0 \vdash \neg(v{\ge}0),\, v^2{\le}10}
      }{v^2{\le}10 \land b{>}0 \vdash \neg(v{\ge}0),\, v^2{\le}10}\ \land\text{L}
    }{v^2{\le}10 \land b{>}0 \vdash \neg(v{\ge}0) \lor v^2{\le}10}\ \lor\text{R}
  }{v^2{\le}10 \land b{>}0 \vdash\ b{>}0 \land (\neg(v{\ge}0) \lor v^2{\le}10)}\ \land\text{R}
}{\vdash\ v^2{\le}10 \land b{>}0 \to b{>}0 \land (\neg(v{\ge}0) \lor v^2{\le}10)}\ \to\text{R}
$$

Simple Propositional Example Proof in Sequent Calculus

$$
\dfrac{\dfrac{\dfrac{*}{v^2\le 10,\ b>0 \vdash b>0}\ \text{id}}{v^2\le 10 \land b>0 \vdash b>0}\ \land\text{L} \qquad \dfrac{\dfrac{\dfrac{*}{\color{red}{v^2\le 10}, b>0 \vdash \neg(v\ge 0), \color{red}{v^2\le 10}}\ \text{id}}{v^2\le 10 \land b>0 \vdash \neg(v\ge 0), v^2\le 10}\ \land\text{L}}{v^2\le 10 \land b>0 \vdash \neg(v\ge 0) \lor v^2\le 10}\ \lor\text{R}}{\dfrac{v^2\le 10 \land b>0 \vdash b>0 \land (\neg(v\ge 0) \lor v^2\le 10)}{\vdash v^2\le 10 \land b>0 \to b>0 \land (\neg(v\ge 0) \lor v^2\le 10)}\ \to\text{R}}\ \land\text{R}
$$

Developed on the board:

1. Proof rules for propositional logic
2. Proofs with dynamics
3. Contextual equivalence rewriting / congruence
4. Quantifier proof rules
5. Structural proof rules

See lecture notes for details [1].

Developed on the board:

1. Proof rules for propositional logic
2. Proofs with dynamics
3. Contextual equivalence rewriting / congruence
4. Quantifier proof rules
5. Structural proof rules

See lecture notes for details [1].

Simple Dynamics Example Proof in Sequent Calculus

$$\overline{\vdash [a := -b; c := 10]\big(v^2 \leq 10 \land -a > 0 \rightarrow b > 0 \land (\neg(v \geq 0) \lor v^2 \leq c)\big)}$$

Simple Dynamics Example Proof in Sequent Calculus

$$
[;]\ \frac{\vdash [a := -b][c := 10]\big(v^2 \le 10 \land -a > 0 \rightarrow b > 0 \land (\neg(v \ge 0) \lor v^2 \le c)\big)}{\vdash [a := -b;\ c := 10]\big(v^2 \le 10 \land -a > 0 \rightarrow b > 0 \land (\neg(v \ge 0) \lor v^2 \le c)\big)}
$$

Simple Dynamics Example Proof in Sequent Calculus

$$
\dfrac{\dfrac{\overline{\vdash [c := 10]\big(v^2 \leq 10 \land -(-b)>0 \rightarrow b>0 \land (\neg(v \geq 0) \lor v^2 \leq c)\big)}}{\vdash [a := -b][c := 10]\big(v^2 \leq 10 \land -a>0 \rightarrow b>0 \land (\neg(v \geq 0) \lor v^2 \leq c)\big)}[:=]}{\vdash [a := -b; c := 10]\big(v^2 \leq 10 \land -a>0 \rightarrow b>0 \land (\neg(v \geq 0) \lor v^2 \leq c)\big)}[;]
$$

Simple Dynamics Example Proof in Sequent Calculus

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash v^2\leq 10 \land -(-b)>0 \rightarrow b>0 \land (\neg(v\geq 0) \lor v^2\leq 10)}}{\vdash [c:=10]\big(v^2\leq 10 \land -(-b)>0 \rightarrow b>0 \land (\neg(v\geq 0) \lor v^2\leq c)\big)}\;[:=]}{\vdash [a:=-b][c:=10]\big(v^2\leq 10 \land -a>0 \rightarrow b>0 \land (\neg(v\geq 0) \lor v^2\leq c)\big)}\;[:=]}{\vdash [a:=-b;\, c:=10]\big(v^2\leq 10 \land -a>0 \rightarrow b>0 \land (\neg(v\geq 0) \lor v^2\leq c)\big)}\;[;]
$$

Simple Dynamics Example Proof in Sequent Calculus

$$
\wedge\text{R}\,\dfrac{\wedge\text{L}\,\dfrac{\text{id}\,\dfrac{*}{v^2\leq 10, b>0 \vdash b>0}}{v^2\leq 10 \wedge b>0 \vdash b>0} \qquad \vee\text{R}\,\dfrac{\wedge\text{L}\,\dfrac{\text{id}\,\dfrac{*}{v^2\leq 10, b>0 \vdash \neg(v\geq 0), v^2\leq 10}}{v^2\leq 10 \wedge b>0 \vdash \neg(v\geq 0), v^2\leq 10}}{v^2\leq 10 \wedge b>0 \vdash \neg(v\geq 0) \vee v^2\leq 10}}{\rightarrow\text{R}\,\dfrac{v^2\leq 10 \wedge b>0 \vdash b>0 \wedge (\neg(v\geq 0) \vee v^2\leq 10)}{\vdash v^2\leq 10 \wedge b>0 \rightarrow b>0 \wedge (\neg(v\geq 0) \vee v^2\leq 10)}}
$$

$$
[;]\,\dfrac{[:=]\,\dfrac{[:=]\,\dfrac{\dfrac{}{\vdash v^2\leq 10 \wedge -(-b)>0 \rightarrow b>0 \wedge (\neg(v\geq 0) \vee v^2\leq 10)}}{\vdash [c := 10]\big(v^2\leq 10 \wedge -(-b)>0 \rightarrow b>0 \wedge (\neg(v\geq 0) \vee v^2\leq c)\big)}}{\vdash [a := -b][c := 10]\big(v^2\leq 10 \wedge -a>0 \rightarrow b>0 \wedge (\neg(v\geq 0) \vee v^2\leq c)\big)}}{\vdash [a := -b; c := 10]\big(v^2\leq 10 \wedge -a>0 \rightarrow b>0 \wedge (\neg(v\geq 0) \vee v^2\leq c)\big)}
$$

Simple Dynamics Example Proof in Sequent Calculus

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{\dfrac{*}{v^2\le 10,\, b>0 \vdash b>0}\,\text{id}}{v^2\le 10 \land b>0 \vdash b>0}\,\land\text{L}
\qquad
\dfrac{\dfrac{\dfrac{*}{v^2\le 10,\, b>0 \vdash \neg(v\ge 0),\, v^2\le 10}\,\text{id}}{v^2\le 10 \land b>0 \vdash \neg(v\ge 0),\, v^2\le 10}\,\land\text{L}}{v^2\le 10 \land b>0 \vdash \neg(v\ge 0) \lor v^2\le 10}\,\lor\text{R}
}{v^2\le 10 \land b>0 \vdash b>0 \land (\neg(v\ge 0) \lor v^2\le 10)}\,\land\text{R}
}{\vdash v^2\le 10 \land {\color{red} b>0} \to b>0 \land (\neg(v\ge 0) \lor v^2\le 10)}\,\to\text{R}
}{}
$$

$$
\dfrac{\dfrac{\dfrac{\vdash v^2\le 10 \land {\color{red} -(-b)>0} \to b>0 \land (\neg(v\ge 0) \lor v^2\le 10)}{\vdash [c:=10]\big(v^2\le 10 \land -(-b)>0 \to b>0 \land (\neg(v\ge 0) \lor v^2\le c)\big)}\,[:=]}{\vdash [a:=-b][c:=10]\big(v^2\le 10 \land -a>0 \to b>0 \land (\neg(v\ge 0) \lor v^2\le c)\big)}\,[:=]}{\vdash [a:=-b;\, c:=10]\big(v^2\le 10 \land -a>0 \to b>0 \land (\neg(v\ge 0) \lor v^2\le c)\big)}\,[;]
$$

Need some real arithmetic
Here: to glue previous propositional proof with this dynamic proof

Developed on the board:

1. Proof rules for propositional logic
2. Proofs with dynamics
3. Contextual equivalence rewriting / congruence
4. Quantifier proof rules
5. Structural proof rules

See lecture notes for details [1].

Outline

Real Arithmetic

Lemma ($\mathbb{R}$ Real arithmetic)

$\text{FOL}_{\mathbb{R}}$ *decidable, so side condition implementable:*

$$\mathbb{R}\ \frac{}{\Gamma \vdash \Delta} \qquad (\text{if } \bigwedge_{P\in\Gamma} P \rightarrow \bigvee_{Q\in\Delta} Q \text{ is valid in } \text{FOL}_{\mathbb{R}})$$

$$\mathbb{R}\frac{}{a > 0, b > 0 \vdash y \geq 0 \rightarrow ax^2 + by \geq 0} \qquad \mathbb{R}\frac{}{x^2 > 0 \vdash x > 0}$$

Lemma ($\mathbb{R}$ Real arithmetic)

$\mathrm{FOL}_{\mathbb{R}}$ *decidable, so side condition implementable:*

$$\mathbb{R}\ \frac{}{\Gamma \vdash \Delta} \qquad (\textit{if } \bigwedge_{P\in\Gamma} P \rightarrow \bigvee_{Q\in\Delta} Q \textit{ is valid in } \mathrm{FOL}_{\mathbb{R}})$$

$$\mathbb{R}\frac{*}{a > 0, b > 0 \vdash y \geq 0 \rightarrow ax^2 + by \geq 0}$$

$$\mathbb{R}\frac{}{x^2 > 0 \vdash x > 0}$$

Real Arithmetic

Lemma ($\mathbb{R}$ Real arithmetic)

FOL$_{\mathbb{R}}$ *decidable, so side condition implementable:*

$$\mathbb{R}\ \frac{}{\Gamma \vdash \Delta} \qquad (\textit{if } \bigwedge_{P\in\Gamma} P \to \bigvee_{Q\in\Delta} Q \textit{ is valid in } \mathrm{FOL}_{\mathbb{R}})$$

$$\mathbb{R}\frac{*}{a>0, b>0 \vdash y\geq 0 \to ax^2+by\geq 0} \qquad \mathbb{R}\frac{\textit{false}}{x^2>0 \vdash x>0}$$

Real Arithmetic

Lemma (ℝ Real arithmetic)

$\text{FOL}_{\mathbb{R}}$ *decidable, so side condition implementable:*

$$\mathbb{R}\ \frac{}{\Gamma \vdash \Delta} \qquad (\textit{if } \bigwedge_{P\in\Gamma} P \rightarrow \bigvee_{Q\in\Delta} Q \textit{ is valid in } \text{FOL}_{\mathbb{R}})$$

$$\mathbb{R}\frac{*}{a > 0, b > 0 \vdash y \geq 0 \rightarrow ax^2 + by \geq 0} \qquad \mathbb{R}\frac{\textit{false}}{x^2 > 0 \vdash x > 0}$$

Theorem (Tarski's quantifier elimination)

$\text{FOL}_{\mathbb{R}}$ *admits quantifier elimination: with each first-order real arithmetic formula P, a quantifier-free formula* $\text{QE}(P)$ *can be associated effectively that is equivalent, i.e.* $P \leftrightarrow \text{QE}(P)$ *is valid.*

Lemma (ℝ Real arithmetic)

$\mathrm{FOL}_{\mathbb{R}}$ *decidable, so side condition implementable:*

$$\mathbb{R}\ \frac{}{\Gamma \vdash \Delta} \qquad \left(\textit{if } \bigwedge_{P\in\Gamma} P \rightarrow \bigvee_{Q\in\Delta} Q \textit{ is valid in } \mathrm{FOL}_{\mathbb{R}}\right)$$

$$\mathbb{R}\ \frac{*}{a > 0, b > 0 \vdash y \geq 0 \rightarrow ax^2 + by \geq 0} \qquad \mathbb{R}\ \frac{\textit{false}}{x^2 > 0 \vdash x > 0}$$

Theorem (Tarski's quantifier elimination)

$\mathrm{FOL}_{\mathbb{R}}$ *admits quantifier elimination: with each first-order real arithmetic formula P, a quantifier-free formula $\mathrm{QE}(P)$ can be associated effectively that is equivalent, i.e. $P \leftrightarrow \mathrm{QE}(P)$ is valid.*

What if there are no quantifiers?

Real Arithmetic

Lemma (ℝ Real arithmetic)

$\mathrm{FOL}_{\mathbb{R}}$ *decidable, so side condition implementable:*

$$\mathbb{R}\ \frac{}{\Gamma \vdash \Delta} \qquad \left(\textit{if } \bigwedge_{P\in\Gamma} P \to \bigvee_{Q\in\Delta} Q \textit{ is valid in } \mathrm{FOL}_{\mathbb{R}}\right)$$

$$\mathbb{R}\frac{*}{a>0, b>0 \vdash y \geq 0 \to ax^2+by \geq 0} \qquad \mathbb{R}\frac{\textit{false}}{x^2>0 \vdash x>0}$$

Theorem (Tarski's quantifier elimination)

$\mathrm{FOL}_{\mathbb{R}}$ *admits quantifier elimination: with each first-order real arithmetic formula* P*, a quantifier-free formula* $\mathrm{QE}(P)$ *can be associated effectively that is equivalent, i.e.* $P \leftrightarrow \mathrm{QE}(P)$ *is valid.*

What if there are no quantifiers? Universal closure with $\mathrm{i}\forall\ \dfrac{\Gamma \vdash \forall x\, P, \Delta}{\Gamma \vdash P, \Delta}$

Quantifier Elimination After Universal Closure

$$\forall R \; \overline{\vdash \forall d \left(d \geq -x \rightarrow [x := 0 \cup x := x + d]\, x \geq 0\right)}$$

Quantifier Elimination After Universal Closure

$$\dfrac{\dfrac{}{\vdash d \geq -x \rightarrow [x := 0 \cup x := x + d]\, x \geq 0}\ [\cup]}{\vdash \forall d\, \big(d \geq -x \rightarrow [x := 0 \cup x := x + d]\, x \geq 0\big)}\ \forall R$$

Quantifier Elimination After Universal Closure

$$\dfrac{\dfrac{\dfrac{}{\vdash d \geq -x \rightarrow [x := 0]\, x \geq 0 \land [x := x + d]\, x \geq 0}[:=]}{\vdash d \geq -x \rightarrow [x := 0 \cup x := x + d]\, x \geq 0}[\cup]}{\vdash \forall d\, \big(d \geq -x \rightarrow [x := 0 \cup x := x + d]\, x \geq 0\big)}\forall R$$

Quantifier Elimination After Universal Closure

$$
\cfrac{\cfrac{\cfrac{\cfrac{}{\vdash d \geq -x \rightarrow 0 \geq 0 \land [x := x + d]\, x \geq 0}\,[:=]}{\vdash d \geq -x \rightarrow [x := 0]\, x \geq 0 \land [x := x + d]\, x \geq 0}\,[:=]}{\vdash d \geq -x \rightarrow [x := 0 \cup x := x + d]\, x \geq 0}\,[\cup]}{\vdash \forall d\, \big(d \geq -x \rightarrow [x := 0 \cup x := x + d]\, x \geq 0\big)}\,\forall R
$$

Quantifier Elimination After Universal Closure

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash d \geq -x \rightarrow 0 \geq 0 \land x + d \geq 0}\text{i}\forall}{\vdash d \geq -x \rightarrow 0 \geq 0 \land [x := x + d]\, x \geq 0}[:=]}{\vdash d \geq -x \rightarrow [x := 0]\, x \geq 0 \land [x := x + d]\, x \geq 0}[:=]}{\vdash d \geq -x \rightarrow [x := 0 \cup x := x + d]\, x \geq 0}[\cup]}{\vdash \forall d\, \big(d \geq -x \rightarrow [x := 0 \cup x := x + d]\, x \geq 0\big)}\forall\text{R}
$$

Quantifier Elimination After Universal Closure

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \forall d\,(d \geq -x \rightarrow 0 \geq 0 \land x + d \geq 0)}\,\text{i}\forall}{\vdash d \geq -x \rightarrow 0 \geq 0 \land x + d \geq 0}\,\text{i}\forall}{\vdash d \geq -x \rightarrow 0 \geq 0 \land [x := x + d]\,x \geq 0}\,[:=]}{\vdash d \geq -x \rightarrow [x := 0]\,x \geq 0 \land [x := x + d]\,x \geq 0}\,[:=]}{\vdash d \geq -x \rightarrow [x := 0 \cup x := x + d]\,x \geq 0}\,[\cup]}{\vdash \forall d\,(d \geq -x \rightarrow [x := 0 \cup x := x + d]\,x \geq 0)}\,\forall\text{R}
$$

Quantifier Elimination After Universal Closure

$$\mathbb{R}\ \dfrac{}{\vdash \forall x\, \forall d\, \big(d \geq -x \rightarrow 0 \geq 0 \land x + d \geq 0\big)}$$

$$\text{i}\forall\ \dfrac{}{\vdash \forall d\, \big(d \geq -x \rightarrow 0 \geq 0 \land x + d \geq 0\big)}$$

$$\text{i}\forall\ \dfrac{}{\vdash d \geq -x \rightarrow 0 \geq 0 \land x + d \geq 0}$$

$$[:=]\ \dfrac{}{\vdash d \geq -x \rightarrow 0 \geq 0 \land [x := x + d]\, x \geq 0}$$

$$[:=]\ \dfrac{}{\vdash d \geq -x \rightarrow [x := 0]\, x \geq 0 \land [x := x + d]\, x \geq 0}$$

$$[\cup]\ \dfrac{}{\vdash d \geq -x \rightarrow [x := 0 \cup x := x + d]\, x \geq 0}$$

$$\forall\text{R}\ \dfrac{}{\vdash \forall d\, \big(d \geq -x \rightarrow [x := 0 \cup x := x + d]\, x \geq 0\big)}$$

Quantifier Elimination After Universal Closure

$$
\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{*}{\vdash \forall x\, \forall d\, \big(d \geq -x \to 0 \geq 0 \land x + d \geq 0\big)}\,\mathbb{R}}{\vdash \forall d\, \big(d \geq -x \to 0 \geq 0 \land x + d \geq 0\big)}\,\text{i}\forall}{\vdash d \geq -x \to 0 \geq 0 \land x + d \geq 0}\,\text{i}\forall}{\vdash d \geq -x \to 0 \geq 0 \land [x := x + d]\, x \geq 0}\,[:=]}{\vdash d \geq -x \to [x := 0]\, x \geq 0 \land [x := x + d]\, x \geq 0}\,[:=]}{\vdash d \geq -x \to [x := 0 \cup x := x + d]\, x \geq 0}\,[\cup]}{\vdash \forall d\, \big(d \geq -x \to [x := 0 \cup x := x + d]\, x \geq 0\big)}\,\forall\text{R}
$$

Quantifier Elimination After Universal Closure

$$
\begin{array}{ll}
 & * \\
\hline
\mathbb{R} & \vdash \forall x\,\forall d\,\big(d \geq -x \rightarrow 0 \geq 0 \land x+d \geq 0\big) \\
\hline
\text{i}\forall & \vdash \forall d\,\big(d \geq -x \rightarrow 0 \geq 0 \land x+d \geq 0\big) \\
\hline
\text{i}\forall & \vdash d \geq -x \rightarrow 0 \geq 0 \land x+d \geq 0 \\
\hline
[:=] & \vdash d \geq -x \rightarrow 0 \geq 0 \land [x:=x+d]\,x \geq 0 \\
\hline
[:=] & \vdash d \geq -x \rightarrow [x:=0]\,x \geq 0 \land [x:=x+d]\,x \geq 0 \\
\hline
[\cup] & \vdash d \geq -x \rightarrow [x:=0 \cup x:=x+d]\,x \geq 0 \\
\hline
\forall\text{R} & \vdash \forall d\,\big(d \geq -x \rightarrow [x:=0 \cup x:=x+d]\,x \geq 0\big)
\end{array}
$$

Here we could leave $\forall d$ alone and use axioms in the middle of the formula.

Outline

Taming Arithmetic: Extreme Instantiation

$$\forall R \quad \frac{\Gamma \vdash p(y), \Delta}{\Gamma \vdash \forall x\, p(x), \Delta} (y \notin \Gamma, \Delta, \forall x p(x)) \qquad \exists R \quad \frac{\Gamma \vdash p(e), \Delta}{\Gamma \vdash \exists x\, p(x), \Delta}$$

$$\forall L \quad \frac{\Gamma, p(e) \vdash \Delta}{\Gamma, \forall x\, p(x) \vdash \Delta} \qquad \exists L \quad \frac{\Gamma, p(y) \vdash \Delta}{\Gamma, \exists x\, p(x) \vdash \Delta} (y \notin \Gamma, \Delta, \exists x p(x))$$

$$\frac{}{\Gamma \vdash [x' = f(x) \,\&\, Q]P}$$

Taming Arithmetic: Extreme Instantiation

$$\forall R \ \frac{\Gamma \vdash p(y), \Delta}{\Gamma \vdash \forall x\, p(x), \Delta}(y \notin \Gamma, \Delta, \forall x p(x)) \qquad \exists R \ \frac{\Gamma \vdash p(e), \Delta}{\Gamma \vdash \exists x\, p(x), \Delta}$$

$$\forall L \ \frac{\Gamma, p(e) \vdash \Delta}{\Gamma, \forall x\, p(x) \vdash \Delta} \qquad \exists L \ \frac{\Gamma, p(y) \vdash \Delta}{\Gamma, \exists x\, p(x) \vdash \Delta}(y \notin \Gamma, \Delta, \exists x p(x))$$

$$[']\ \frac{\overline{\Gamma \vdash \forall t{\geq}0\, \big((\forall 0{\leq}s{\leq}t\, [x := y(s)]Q) \rightarrow [x := y(t)]P\big)}}{\Gamma \vdash [x' = f(x)\,\&\, Q]P}$$

Taming Arithmetic: Extreme Instantiation

$$\forall R\ \frac{\Gamma \vdash p(y), \Delta}{\Gamma \vdash \forall x\, p(x), \Delta}(y \not\in \Gamma, \Delta, \forall x p(x)) \qquad \exists R\ \frac{\Gamma \vdash p(e), \Delta}{\Gamma \vdash \exists x\, p(x), \Delta}$$

$$\forall L\ \frac{\Gamma, p(e) \vdash \Delta}{\Gamma, \forall x\, p(x) \vdash \Delta} \qquad \exists L\ \frac{\Gamma, p(y) \vdash \Delta}{\Gamma, \exists x\, p(x) \vdash \Delta}(y \not\in \Gamma, \Delta, \exists x p(x))$$

$$\cfrac{\cfrac{\overline{\Gamma \vdash t \geq 0 \to \big((\forall 0 \leq s \leq t\, [x := y(s)]Q) \to [x := y(t)]P\big)}}{\Gamma \vdash \forall t \geq 0\, \big((\forall 0 \leq s \leq t\, [x := y(s)]Q) \to [x := y(t)]P\big)}\ \forall R}{\Gamma \vdash [x' = f(x)\, \&\, Q]P}\ [']$$

Taming Arithmetic: Extreme Instantiation

$$\forall R \quad \frac{\Gamma \vdash p(y), \Delta}{\Gamma \vdash \forall x\, p(x), \Delta} (y \notin \Gamma, \Delta, \forall x p(x)) \qquad \exists R \quad \frac{\Gamma \vdash p(e), \Delta}{\Gamma \vdash \exists x\, p(x), \Delta}$$

$$\forall L \quad \frac{\Gamma, p(e) \vdash \Delta}{\Gamma, \forall x\, p(x) \vdash \Delta} \qquad \exists L \quad \frac{\Gamma, p(y) \vdash \Delta}{\Gamma, \exists x\, p(x) \vdash \Delta} (y \notin \Gamma, \Delta, \exists x p(x))$$

$$\cfrac{\cfrac{\cfrac{\cfrac{}{\Gamma, t \geq 0 \vdash (\forall 0 \leq s \leq t\, [x := y(s)]Q) \rightarrow [x := y(t)]P}}{\Gamma \vdash t \geq 0 \rightarrow \big((\forall 0 \leq s \leq t\, [x := y(s)]Q) \rightarrow [x := y(t)]P\big)} \to R}{\Gamma \vdash \forall t \geq 0\, \big((\forall 0 \leq s \leq t\, [x := y(s)]Q) \rightarrow [x := y(t)]P\big)} \forall R}{\Gamma \vdash [x' = f(x) \,\&\, Q]P} [']$$

Taming Arithmetic: Extreme Instantiation

$$\forall R\ \frac{\Gamma \vdash p(y), \Delta}{\Gamma \vdash \forall x\, p(x), \Delta}(y \notin \Gamma, \Delta, \forall x p(x)) \qquad \exists R\ \frac{\Gamma \vdash p(e), \Delta}{\Gamma \vdash \exists x\, p(x), \Delta}$$

$$\forall L\ \frac{\Gamma, p(e) \vdash \Delta}{\Gamma, \forall x\, p(x) \vdash \Delta} \qquad \exists L\ \frac{\Gamma, p(y) \vdash \Delta}{\Gamma, \exists x\, p(x) \vdash \Delta}(y \notin \Gamma, \Delta, \exists x p(x))$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\overline{\Gamma, t\geq 0, \forall 0\leq s\leq t\, [x := y(s)]Q \vdash [x := y(t)]P}}{\Gamma, t\geq 0 \vdash (\forall 0\leq s\leq t\, [x := y(s)]Q)\rightarrow[x := y(t)]P}\rightarrow R}{\Gamma \vdash t\geq 0\rightarrow\big((\forall 0\leq s\leq t\, [x := y(s)]Q)\rightarrow[x := y(t)]P\big)}\rightarrow R}{\Gamma \vdash \forall t\geq 0\, \big((\forall 0\leq s\leq t\, [x := y(s)]Q)\rightarrow[x := y(t)]P\big)}\forall R}{\Gamma \vdash [x' = f(x)\,\&\, Q]P}[']$$

Taming Arithmetic: Extreme Instantiation

$$\forall R\ \frac{\Gamma \vdash p(y), \Delta}{\Gamma \vdash \forall x\, p(x), \Delta}(y \notin \Gamma, \Delta, \forall x p(x)) \qquad \exists R\ \frac{\Gamma \vdash p(e), \Delta}{\Gamma \vdash \exists x\, p(x), \Delta}$$

$$\forall L\ \frac{\Gamma, p(e) \vdash \Delta}{\Gamma, \forall x\, p(x) \vdash \Delta} \qquad \exists L\ \frac{\Gamma, p(y) \vdash \Delta}{\Gamma, \exists x\, p(x) \vdash \Delta}(y \notin \Gamma, \Delta, \exists x p(x))$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{\Gamma, t \geq 0, 0 \leq t \leq t \to [x := y(t)]Q \vdash [x := y(t)]P}}{\Gamma, t \geq 0, \forall 0 \leq s \leq t\, [x := y(s)]Q \vdash [x := y(t)]P}\forall L}{\Gamma, t \geq 0 \vdash (\forall 0 \leq s \leq t\, [x := y(s)]Q) \to [x := y(t)]P}\to R}{\Gamma \vdash t \geq 0 \to \big((\forall 0 \leq s \leq t\, [x := y(s)]Q) \to [x := y(t)]P\big)}\to R}{\Gamma \vdash \forall t \geq 0\, \big((\forall 0 \leq s \leq t\, [x := y(s)]Q) \to [x := y(t)]P\big)}\forall R}{\Gamma \vdash [x' = f(x)\, \&\, Q]P}[']$$

Taming Arithmetic: Extreme Instantiation

$$\forall R\ \frac{\Gamma \vdash p(y), \Delta}{\Gamma \vdash \forall x\, p(x), \Delta}(y \notin \Gamma, \Delta, \forall x p(x)) \qquad \exists R\ \frac{\Gamma \vdash p(e), \Delta}{\Gamma \vdash \exists x\, p(x), \Delta}$$

$$\forall L\ \frac{\Gamma, p(e) \vdash \Delta}{\Gamma, \forall x\, p(x) \vdash \Delta} \qquad \exists L\ \frac{\Gamma, p(y) \vdash \Delta}{\Gamma, \exists x\, p(x) \vdash \Delta}(y \notin \Gamma, \Delta, \exists x p(x))$$

$$
\begin{array}{r c}
 & \overline{t \geq 0 \vdash 0 \leq t \leq t, [x := y(t)]P} \quad \overline{\Gamma, t \geq 0, [x := y(t)]Q \vdash [x := y(t)]P} \\
\rightarrow L & \overline{\Gamma, t \geq 0, 0 \leq \color{red}{t} \leq t \rightarrow [x := y(\color{red}{t})]Q \vdash [x := y(t)]P} \\
\forall L & \overline{\Gamma, t \geq 0, \forall 0 \leq \color{red}{s} \leq t\, [x := y(\color{red}{s})]Q \vdash [x := y(t)]P} \\
\rightarrow R & \overline{\Gamma, t \geq 0 \vdash (\forall 0 \leq s \leq t\, [x := y(s)]Q) \rightarrow [x := y(t)]P} \\
\rightarrow R & \overline{\Gamma \vdash t \geq 0 \rightarrow \big((\forall 0 \leq s \leq t\, [x := y(s)]Q) \rightarrow [x := y(t)]P\big)} \\
\forall R & \overline{\Gamma \vdash \forall t \geq 0\, \big((\forall 0 \leq s \leq t\, [x := y(s)]Q) \rightarrow [x := y(t)]P\big)} \\
['] & \Gamma \vdash [x' = f(x)\, \&\, Q]P
\end{array}
$$

Taming Arithmetic: Extreme Instantiation

$$\forall R\ \frac{\Gamma \vdash p(y), \Delta}{\Gamma \vdash \forall x\, p(x), \Delta}(y \notin \Gamma, \Delta, \forall x p(x)) \qquad \exists R\ \frac{\Gamma \vdash p(e), \Delta}{\Gamma \vdash \exists x\, p(x), \Delta}$$

$$\forall L\ \frac{\Gamma, p(e) \vdash \Delta}{\Gamma, \forall x\, p(x) \vdash \Delta} \qquad \exists L\ \frac{\Gamma, p(y) \vdash \Delta}{\Gamma, \exists x\, p(x) \vdash \Delta}(y \notin \Gamma, \Delta, \exists x p(x))$$

$$[']\dfrac{\forall R\dfrac{\to R\dfrac{\to R\dfrac{\forall L\dfrac{\to L\dfrac{\mathbb{R}\dfrac{*}{t{\geq}0 \vdash 0{\leq}t{\leq}t, [x := y(t)]P} \qquad \Gamma, t{\geq}0, [x := y(t)]Q \vdash [x := y(t)]P}{\Gamma, t{\geq}0, 0{\leq}{\color{red}t}{\leq}t{\to}[x := y({\color{red}t})]Q \vdash [x := y(t)]P}}{\Gamma, t{\geq}0, \forall 0{\leq}{\color{red}s}{\leq}t\, [x := y({\color{red}s})]Q \vdash [x := y(t)]P}}{\Gamma, t{\geq}0 \vdash (\forall 0{\leq}s{\leq}t\, [x := y(s)]Q) \to [x := y(t)]P}}{\Gamma \vdash t{\geq}0 \to \big((\forall 0{\leq}s{\leq}t\, [x := y(s)]Q) \to [x := y(t)]P\big)}}{\Gamma \vdash \forall t{\geq}0\, \big((\forall 0{\leq}s{\leq}t\, [x := y(s)]Q) \to [x := y(t)]P\big)}}{\Gamma \vdash [x' = f(x)\,\&\, Q]P}$$

Taming Arithmetic: Extreme Instantiation

$$\forall R\ \frac{\Gamma \vdash p(y), \Delta}{\Gamma \vdash \forall x\, p(x), \Delta}(y \notin \Gamma, \Delta, \forall x p(x)) \qquad \exists R\ \frac{\Gamma \vdash p(e), \Delta}{\Gamma \vdash \exists x\, p(x), \Delta}$$

$$\forall L\ \frac{\Gamma, p(e) \vdash \Delta}{\Gamma, \forall x\, p(x) \vdash \Delta} \qquad \exists L\ \frac{\Gamma, p(y) \vdash \Delta}{\Gamma, \exists x\, p(x) \vdash \Delta}(y \notin \Gamma, \Delta, \exists x p(x))$$

$$
{[']}\ \dfrac{
\forall R\ \dfrac{
\to R\ \dfrac{
\to R\ \dfrac{
\forall L\ \dfrac{
\to L\ \dfrac{
\mathbb{R}\ \dfrac{*}{t{\geq}0 \vdash 0{\leq}t{\leq}t, [x := y(t)]P}
\quad
\dfrac{\ldots}{\Gamma, t{\geq}0, [x := y(t)]Q \vdash [x := y(t)]P}
}{\Gamma, t{\geq}0, 0{\leq}{\color{red}t}{\leq}t \to [x := y({\color{red}t})]Q \vdash [x := y(t)]P}
}{\Gamma, t{\geq}0, \forall 0{\leq}{\color{red}s}{\leq}t\, [x := y({\color{red}s})]Q \vdash [x := y(t)]P}
}{\Gamma, t{\geq}0 \vdash (\forall 0{\leq}s{\leq}t\, [x := y(s)]Q) \to [x := y(t)]P}
}{\Gamma \vdash t{\geq}0 \to \big((\forall 0{\leq}s{\leq}t\, [x := y(s)]Q) \to [x := y(t)]P\big)}
}{\Gamma \vdash \forall t{\geq}0\, \big((\forall 0{\leq}s{\leq}t\, [x := y(s)]Q) \to [x := y(t)]P\big)}
}{\Gamma \vdash [x' = f(x)\ \&\ Q]P}
$$

Taming Arithmetic: Weakening

$$\text{WR}\ \frac{\Gamma \vdash \Delta}{\Gamma \vdash P, \Delta}$$

$$\text{WL}\ \frac{\Gamma \vdash \Delta}{\Gamma, P \vdash \Delta}$$

$$\text{WL}\frac{r{\geq}0 \vdash 0{\leq}r{\leq}r}{A, r{\geq}0 \vdash 0{\leq}r{\leq}r}$$

Throw arithmetic distraction A away by weakening since proof is independent of A.

Occam's assumption razor

Think how hard it would be to prove a theorem with all the facts in all books of mathematics as assumptions.
Compared to a proof from just the two facts that matter.

Taming Arithmetic: Creative Cuts & Substitute Equations

$$=\!\mathrm{R}\ \frac{\Gamma, x = e \vdash p(e), \Delta}{\Gamma, x = e \vdash p(x), \Delta}$$

$$=\!\mathrm{L}\ \frac{\Gamma, x = e, p(e) \vdash \Delta}{\Gamma, x = e, p(x) \vdash \Delta}$$

$$\rightarrow\!\mathrm{R}\ \dfrac{\land\mathrm{L}\ \dfrac{\mathrm{cut}\ \dfrac{\mathrm{WL}\ \dfrac{\mathrm{WR}\ \dfrac{\mathbb{R}\ \dfrac{*}{(x-y)^2 \le 0 \vdash x = y}}{(x-y)^2 \le 0 \vdash x = y, p(x)}}{(x-y)^2 \le 0, p(y) \vdash x = y, p(x)} \qquad \mathrm{WL}\ \dfrac{=\!\mathrm{R}\ \dfrac{\mathrm{id}\ \dfrac{*}{p(y), x = y \vdash p(y)}}{p(y), x = y \vdash p(x)}}{(x-y)^2 \le 0, p(y), x = y \vdash p(x)}}{(x-y)^2 \le 0, p(y) \vdash p(x)}}{(x-y)^2 \le 0 \land p(y) \vdash p(x)}}{\vdash (x-y)^2 \le 0 \land p(y) \rightarrow p(x)}$$

Taming Arithmetic: Abbreviating Terms

$$a{\geq}0, t{\geq}0, 0 \leq \underbrace{\frac{a}{2}t^2 + vt + x}_{z}, \underbrace{\frac{a}{2}t^2 + vt + x}_{z} \leq d, d{\leq}8 \vdash \underbrace{\frac{a}{2}t^2 + vt + x}_{z} \leq 8$$

Abbreviate fancy term $\frac{a}{2}t^2 + vt + x$ by new variable z:

$$a \geq 0, t \geq 0, 0 \leq z, z \leq d, d \leq 8 \vdash z \leq 8$$

André Platzer.
Foundations of cyber-physical systems.
Lecture Notes 15-424/624/824, Carnegie Mellon University, 2017.
URL: `http://www.cs.cmu.edu/~aplatzer/course/fcps17.html`.

André Platzer.
Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.
Springer, Heidelberg, 2010.
doi:10.1007/978-3-642-14509-4.