Toward tableaux and ODEs... one day

François Pessaux

and Alexandre Chapoutot, Julien Alexandre dit Sandretto

U2IS, ENSTA Paris, Institut Polytechnique de Paris, 828 boulevard des Maréchaux, 91120 Palaiseau, France

23/11/2022

firstname.lastname@ensta-paristech.fr

Long-term target

Context

- Tableaux method : automated proof.
- Hybrid systems verification : guaranteed simulation with intervals.

Long-term objective

- Extend tableaux to automatically prove properties.
- Add an IVP to the context $x_i(0) = \ldots,\ \dot{x}_i = \ldots$
- Check formulae about time (t) and dynamics $x_i(t)$.

$$\dot{x} = 5 + y$$
$$\dot{y} = 6 \times x$$
$$x(0) = 0.9$$
$$y(0) = 0$$
$$\exists t : time, t \in [0, 1.0] \wedge (x(t) \notin [4, 7] \vee x(t) \in [8, 10])$$

Current objective more modest to understand issues

Equations on floats

- Arithmetic equations (non-linear) with 1 parameter : no ODE.
- Naive simulator : ≪ tube ≫ obtained par sampling with arbitrary step.
- No guaranteed arithmetic nor intervals (IEEE floats).
- Arbitrary ϵ parameters :
  - for float equality,
  - interval complementary – bounds exclusion,
  - discretization step.
- Atoms : $t \in\!\!\!\!/\ [a, b]$ and $f(t) \in\!\!\!\!/\ [a, b]$ (a and b constants).
- Mixing meta-variables and ϵ-terms ($\forall/\exists$) not explored.

$f(x) = x - 5 \quad , \quad g(x) = 5 - x$

- $\exists t : \mathit{float}, t \in [0, 4] \wedge f(t) \in [-4, -2] \wedge g(t) \in [2, 4]$ (ok t in $[1, 3]$)
- $\exists t : \mathit{float}, t \in [0, 4] \wedge t \in [1, 2] \wedge t \in [3, 5]$ (ko)

Tableaux method

Generalities

- Automated proof technique.
- Proceeds by refutation.
  - Property P to prove,

  $\Rightarrow$ Refute $\neg P$ (i.e. $\neg P$ is unsatisfiable)
  - Proof by absurd.
- Method by syntactic decomposition.
  - True for propositional calculus.
  - More subtle for first-order logics.
  - Again more subtle with theories extensions.

Rules for propositional calculus

Split in 3 (then 5 for first-order logics)

- Closure rules : do not generate sub-goals.

$$\frac{\bot}{\odot}\,\odot_{\bot} \qquad \frac{\neg\top}{\odot}\,\odot_{\neg\top} \qquad \frac{P \quad \neg P}{\odot}\,\odot$$

- α rules : generate one branch.

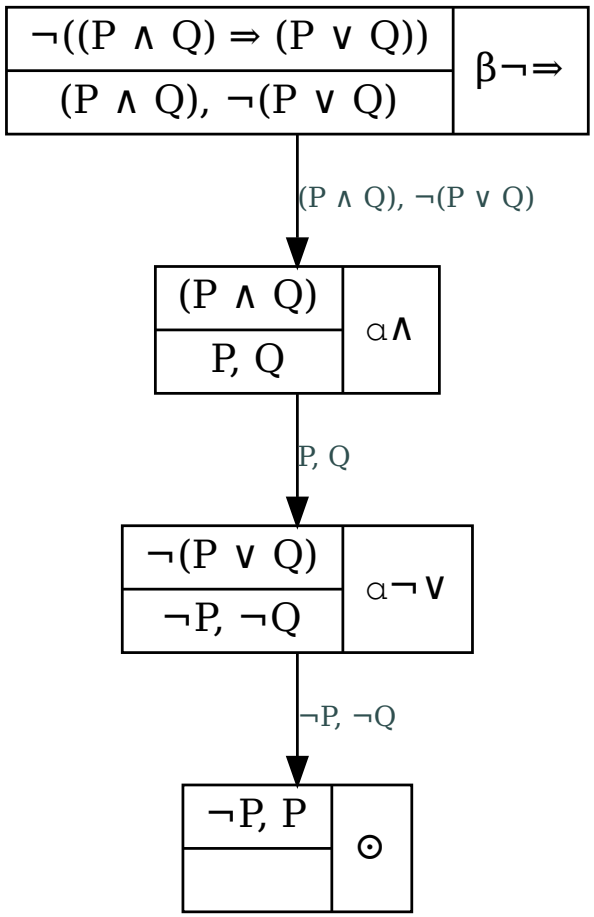
$$\frac{\neg\neg P}{P}\,\alpha_{\neg\neg} \qquad \frac{P \wedge Q}{P, Q}\,\alpha_{\wedge} \qquad \frac{\neg(P \vee Q)}{\neg P, \neg Q}\,\alpha_{\neg\vee}$$

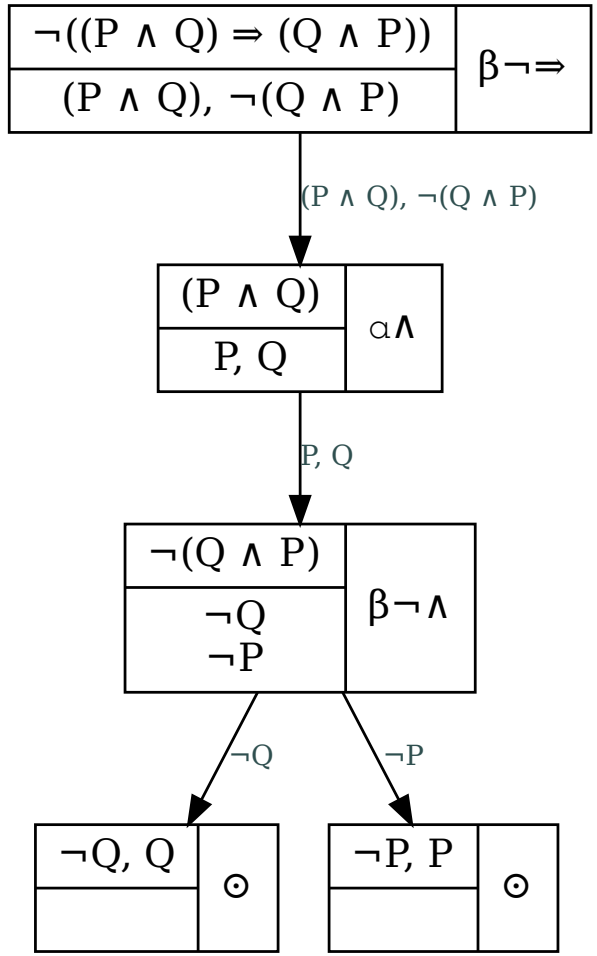
- β rules : generate several branches.

$$\frac{P \vee Q}{P \mid Q}\,\beta_{\vee} \qquad \frac{P \Leftrightarrow Q}{\neg P, \neg Q \mid P, Q}\,\beta_{\Leftrightarrow} \qquad \frac{P \Rightarrow Q}{\neg P \mid Q}\,\beta_{\Rightarrow}$$

$$\frac{\neg(P \Leftrightarrow Q)}{\neg P, Q \mid P, \neg Q}\,\beta_{\neg\Leftrightarrow} \qquad \frac{\neg(P \Rightarrow Q)}{P, \neg Q}\,\beta_{\neg\Rightarrow} \qquad \frac{\neg(P \wedge Q)}{\neg P \mid \neg Q}\,\beta_{\neg\wedge}$$

Graphical representation





Add quantifiers $\forall$, $\exists$

Structural decomposition insufficient

- $\forall x$: introduction of a meta-variable X.
- $\exists x$: introduction of an ϵ-term $\epsilon(x)$.
- Meta-variables : to be instantiated by a term *"that fits well"*.
- ϵ-term : not instantiable, denotes a term *"that fits well"*.
- ... with the hope to exhibit a contradiction.

Additional rules

- δ rules

$$\frac{\exists x\ P(x)}{P(\epsilon(x).P(x))}\,\delta_{\exists} \qquad \frac{\neg\forall x\ P(x)}{\neg P(\epsilon(x).P(x))}\,\delta_{\neg\forall}$$

- γ rules

$$\frac{\forall x\ P(x)}{P(X)}\,\gamma_{\forall M} \qquad \frac{\neg\exists x\ P(x)}{\neg P(X)}\,\gamma_{\neg\exists M} \qquad \frac{\forall x\ P(x)}{P(t)}\,\gamma_{\forall inst} \qquad \frac{\neg\exists x\ P(x)}{\neg P(t)}\,\gamma_{\neg\exists inst}$$

Prerequisites : intervals representation

Or rather of "sets"

- Complementary $\Rightarrow$ non-contiguous intervals (ex. $[0,2] \oplus [4,6]$).
- Use *interval-unions*
  Interval unions, Schichl, Domes, Montanher, Kofler - 2016, BIT Numerical Mathematics, DOI 10.1007/s10543-016-0632-y
- List of disjoints "simple" intervals, with closed bounds.
- Use `infinity` and `neg_infinity` for $+\infty$ and $-\infty$.
- Required operations :
  - Intersection.
  - Complementary (modulo ϵ because bounds always included).
  - Belonging test for a float.
  - Difference (derived operation : $\mathcal{I}_1 \setminus \mathcal{I}_2 = \mathcal{I}_1 \cap \overline{\mathcal{I}_2}$).
  - Choice operator (random element) for Coq proofs.

Interaction with theory

Intuitive view

- Regular logic formulae split by the standard rules.
- Atoms $\in$ and $\notin$ sent to the theory oracle.
  - Can deal with dynamics : $x(t) \in [8, 10]$.
  - Can deal with "time" : $t \notin [8, 10]$.
  - Intervals bounds : constants (plus ∞'s).
  - Intervals bounds : closed.
  - Implicitly a conjunction of atoms in a branch.
- Oracle evaluates (with floats) functions by sampling time and :
  - | does nothing,
  - | concludes to a contradiction,
  - | forces a contradiction,
  - | infers new constraints.

The rules (1/5)

$$\frac{T \in \mathcal{I}_1 \quad \overline{\mathcal{I}_1} \neq \emptyset}{\overline{\mathcal{I}_1} \in \mathcal{I}_1}\,\gamma\forall t\in \qquad \frac{T \notin \mathcal{I}_1}{T \in \overline{\mathcal{I}_1}}\,\gamma\forall t\notin$$

$$\frac{f(T) \in \mathcal{I}_1 \quad \mathcal{I}_2 = \{\, t \mid f(t) \notin \mathcal{I}_1 \,\} \quad \mathcal{I}_2 \neq \emptyset}{f(^\dagger\mathcal{I}_2) \in \mathcal{I}_1}\,\gamma\forall ft\in \qquad \frac{f(T) \notin \mathcal{I}_1}{f(T) \in \overline{\mathcal{I}_1}}\,\gamma\forall ft\notin$$

Aim : get a contradiction (later)

- Instantiate the meta-variable by an "interval" (set).
- Meta-variable $\Rightarrow$ formula holding for all t represented by T.

$\Rightarrow$ Extract the part of [.] such that formula gets false.

- Branch remains open (cf. *The rules (4/5)*).
- Instantiation : intervals physically mutable (written †[.]).
- Physical sharing ensured (for rigid unification) by the γ-instantiation mechanism.

The rule (2/5)

$$\frac{\epsilon t \in \mathcal{I}_1 \quad \epsilon t \in \mathcal{I}_2}{\epsilon t \in \mathcal{I}_1 \cap \mathcal{I}_2}\,\delta_{\exists t\in} \qquad \frac{\epsilon t \in \emptyset}{\odot}\,\odot_{t\in} \qquad \frac{\epsilon t \notin \mathcal{I}_1}{\epsilon t \in \overline{\mathcal{I}_1}}\,\delta_{\exists t\notin}$$

Aim : is intersection of $\epsilon t \in [.]$ constraints unsatisfiable ?

- If yes, branch gets closed, if not, no conclusion.
- Rules : add new constraint | detection $\in \emptyset$.
- Implementation :
  - Constraints recorded and accumulated in the oracle.
  - Directly verifies the intersection emptiness.
  - Does not add a new formula (constraint) to the context.

The rules (3/5)

$$\frac{f(\epsilon t) \in \mathcal{I}_1 \quad \mathcal{I}_2 = \{\, t \mid f(t) \in \mathcal{I}_1 \,\}}{\epsilon t \in \mathcal{I}_2}\ \delta_{\exists ft\in} \qquad \frac{f(\epsilon t) \notin \mathcal{I}_1}{f(\epsilon t) \in \overline{\mathcal{I}_1}}\ \delta_{\exists ft\notin}$$

Aim : infer a new formula

- Determine the set for ϵt such that formula is valid.
- Add formula to the context.
- Implementation :
  - Directly verifies if inferred formula is $\in \emptyset$.
  - If yes, branch gets closed, if not, new formula added to the context.

The rules (4/5)

$$\frac{{}^{\dagger}\mathcal{I}_1 \in \mathcal{I}_2 \quad {}^{\dagger}\mathcal{I}_1 \setminus \mathcal{I}_2 \neq \emptyset}{\odot \;/\; {}^{\dagger}\mathcal{I}_1 \leftarrow {}^{\dagger}\mathcal{I}_1 \setminus \mathcal{I}_2}\ \odot_{\forall i \in} \qquad \frac{{}^{\dagger}\mathcal{I}_1 \notin \mathcal{I}_2}{{}^{\dagger}\mathcal{I}_1 \in \overline{\mathcal{I}_2}}\ \gamma_{\forall i \notin}$$

Aim : get a contradiction (now)

- Formulae only possible after a meta-variable instantiation.
- Make the formula false **and** close the branch.
- Reminder : instantiation comes from meta-variable, hence from $\forall$.
- Semantics $\mathcal{I}_1 \in \mathcal{I}_2$: $\quad \forall t, t \in \mathcal{I}_1 \Rightarrow t \in \mathcal{I}_2$.
- Re-instantiate $\mathcal{I}_1$ by the part making formula false :
  - everything that is in $\mathcal{I}_1$ and not in $\mathcal{I}_2$: $\mathcal{I}_1 \setminus \mathcal{I}_2 \equiv \mathcal{I}_1 \cap \overline{\mathcal{I}_2}$
  - except if $= \emptyset$ (would re-open the branch having previously instantiated).

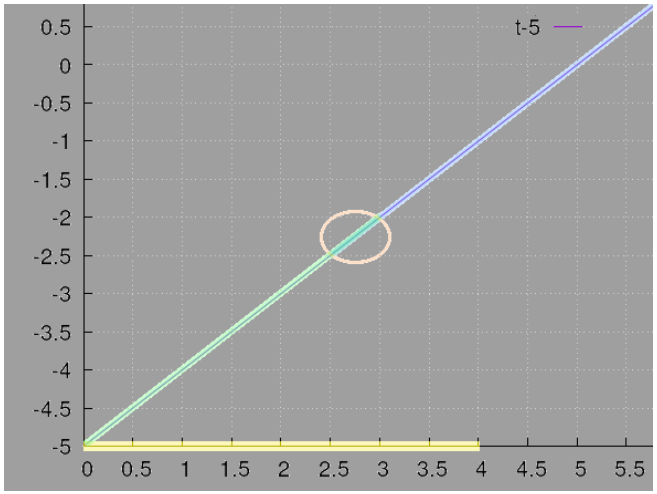
The rules (5/5)

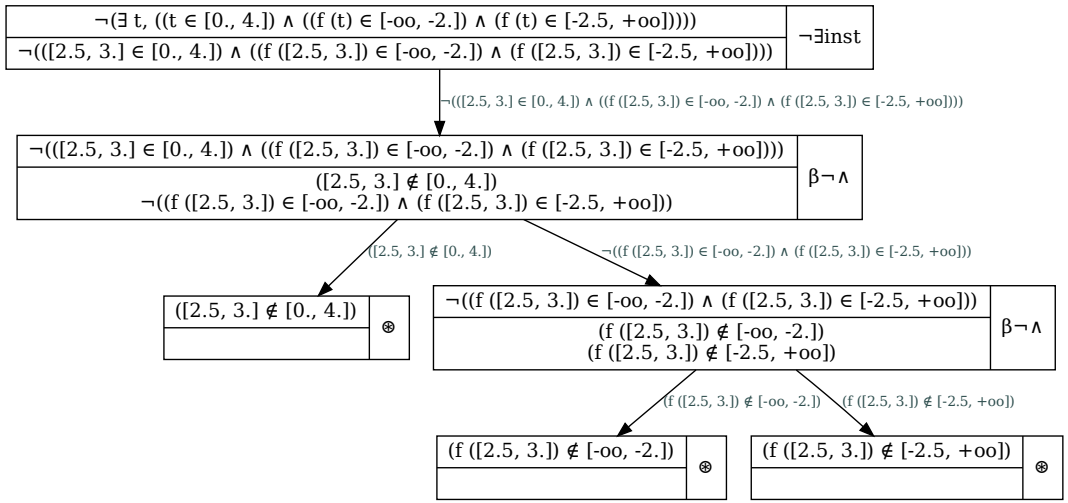
$$\frac{f({}^{\dagger}\mathcal{I}_1) \in \mathcal{I}_2 \quad \mathcal{I}_3 = \{\, t \mid f(t) \notin \mathcal{I}_2 \,\} \quad {}^{\dagger}\mathcal{I}_1 \cap \mathcal{I}_3 \neq \emptyset}{\odot \;/\; {}^{\dagger}\mathcal{I}_1 \leftarrow {}^{\dagger}\mathcal{I}_1 \cap \mathcal{I}_3}\ \odot_{\forall fi \in} \qquad \frac{f({}^{\dagger}\mathcal{I}_1) \notin \mathcal{I}_2}{f({}^{\dagger}\mathcal{I}_1) \in \overline{\overline{\mathcal{I}_2}}}\ \gamma_{\forall fi \notin}$$

Aim : get a contradiction (now)

- Same principle as ${}^{\dagger}\mathcal{I}_1 \in \mathcal{I}_2$.
- Re-instantiate $\mathcal{I}_1$ by the part making formula false :
  - everything that is in $\mathcal{I}_1$ and invalidates $f(t) \in \mathcal{I}_2$
  - except if $= \emptyset$ (would re-open the branch having previously instantiated).

$\exists t, t \in [0,4] \wedge f(t) \in [-\infty,-2] \wedge f(t) \in [-2.5,+\infty]$



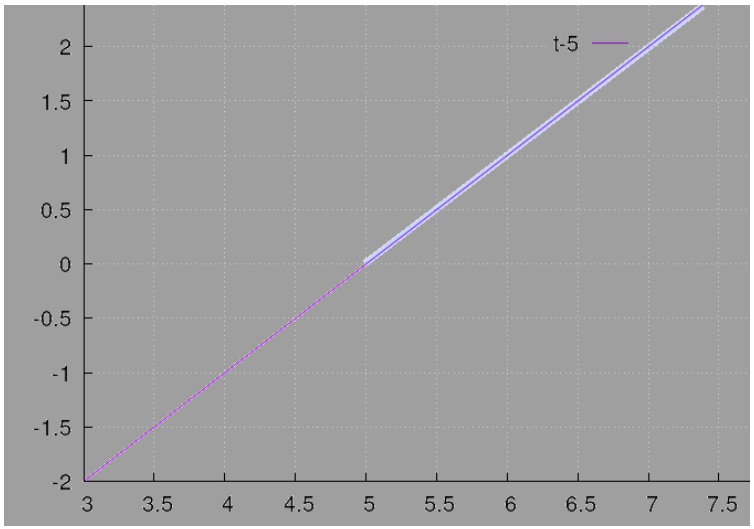


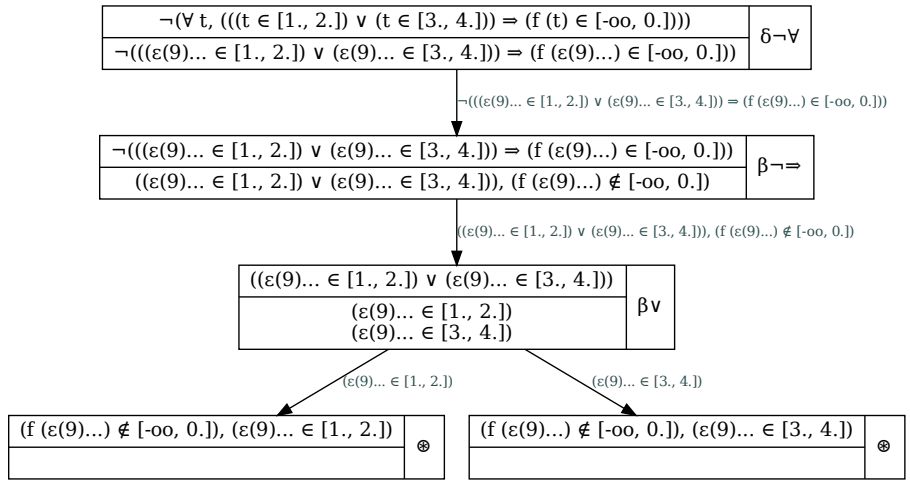
Provable

- Instantiation T on left by $[0,4]$
- Instantiation T on right-left by $[-\infty,3]$ (re-inst. by $[0,3]$)
- Instantiation T on right-right par $[2.5,+\infty]$ (re-inst. by $[2.5,3]$)

$\Rightarrow$ Intersection $= [2.5,3]$

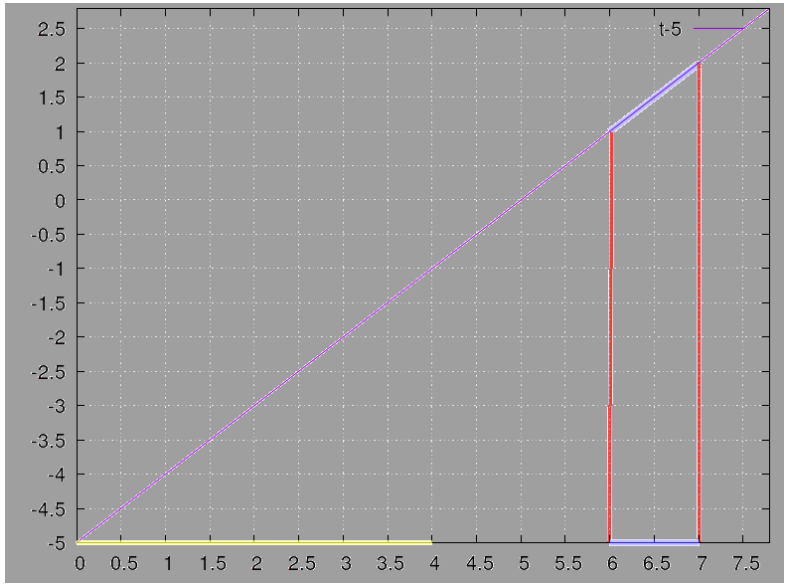
$\forall t, (t \in [1,2] \vee t \in [3,4]) \Rightarrow f(t) \in [-\infty, 0]$





- $f(\epsilon t) \notin]-\infty, 0] \Rightarrow \epsilon t \in]5, +\infty[$
- Left branch : and $\epsilon t \in [1,2] \Rightarrow$ contradiction.
- Right branch : and $\epsilon t \in [3,4] \Rightarrow$ contradiction.

Example not provable (fine) (1/2)

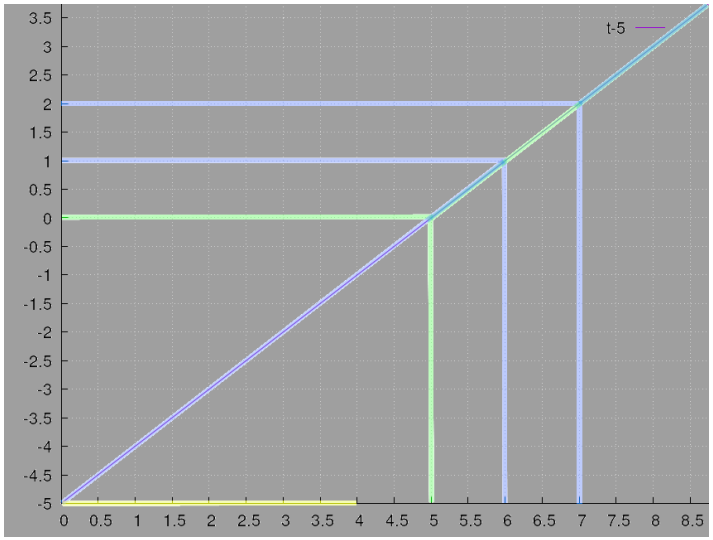


$\exists t, t \in [0,4] \wedge f(t) \in [1,2]$

Two branches : $T \notin [0,4]$ $f(T) \notin [1,2]$

- $T \notin [0,4] \rightarrow \quad T \in \overline{[0,4]} \rightarrow \quad T \leftarrow [0,4]$
  - Closure.
- $f([0,4]) \notin [1,2] \rightarrow \quad f([0,4]) \in \overline{[1,2]} \rightarrow \quad T \leftarrow [6,7]$
  - $[0,4] \cap [6,7] = \emptyset$
  - Remains open.

Example no provable (fine) (2/2)



$\forall t, t \in [0,4] \Rightarrow (f(t) \in [-6,0] \vee f(t) \in [1,2])$

Two branches :

- $\epsilon t \in [0,4], f(\epsilon t) \notin [-6,0]$
  - $f(t) \notin [-6,0]$: new formula $\epsilon t =]5, +\infty[$
  - $[0,4] \cap]5, +\infty[= \emptyset$, contradiction, closure.
- $\epsilon t \in [0,4], f(\epsilon t) \notin [1,2]$
  - $f(t) \notin [1,2]$: new formula $\epsilon t = [0,6[\oplus]7, +\infty[$
  - $[0,4] \cap ([0,6[\oplus]7, +\infty[) \neq \emptyset$, remains open.

Rules correctness

Principle : premises are provable ⇒ conclusions also

- Encode meta-variables by universal quantification.
- Encode ϵ-terms by existential quantification.
- Encode $\mathcal{I}_1 \in \mathcal{I}_2$ by : $\forall/\exists x : Num, x \in \mathcal{I}_1 \Rightarrow x \in \mathcal{I}_2$
- Encode $f(\mathcal{I}_1) \in \mathcal{I}_2$ by : $\forall/\exists x : Num, x \in \mathcal{I}_1 \Rightarrow f(x) \in \mathcal{I}_2$
- Use sets formalization `Ensembles` (Coq stdlib).

$$\frac{f(\epsilon t) \in \mathcal{I}_1 \quad \mathcal{I}_2 = \{\, t \mid f(t) \in \mathcal{I}_1 \,\}}{\epsilon t \in \mathcal{I}_2}\, \delta_{\exists ft\in}$$

```
Theorem sound_delta_exists_ft_in :
  forall S1 S2:Ensemble Num,
    ((exists t:Num, In S1 (f t))
     /\ (forall y:Num, In S2 y <-> In S1 (f y))) ->
    (exists t:Num, In S2 t).
Proof.
  unfold In. intros. destruct H. destruct H. apply H0 in H. exists x. exact H.
Qed.
```

Remarks about correctness

Correction versus optimization

- Side-conditions of $\gamma_{\forall t\in}$ and $\gamma_{\forall ft\in}$ useless for correction
  - prevent instantiations fruitless in contradictions.
- (But required for $\delta_{\exists ft\in}$.)
- Re-instantiation in $\odot_{\forall i\in}$ and $\odot_{\forall fi\in}$ useless for correction
  - needed for efficient implementation and Coq term construction.
- Rules $\notin$: can be rewritten without adding formula to the context
  - reduces the number of formulae to examine.

$$\frac{T \notin [1] \quad [1] \neq \emptyset}{[1] \in [1]}\,\gamma_{\forall t\notin}{}' \qquad \frac{f(T) \notin [1] \quad [2] = \{\, t \mid f(y) \in [1] \,\} \quad [2] \neq \emptyset}{f(^{\dagger}[2]) \notin [1]}\,\gamma_{\forall ft\notin}{}'$$

$$\frac{f(\epsilon t) \notin [1] \quad [2] = \{\, t \mid f(t) \notin [1] \,\}}{\epsilon t \in [2]}\,\delta_{\exists ft\notin}{}' \qquad \frac{^{\dagger}[1] \notin [2] \quad {}^{\dagger}[1] \cap [2] \neq \emptyset}{\odot \;/\; {}^{\dagger}[1] \leftarrow {}^{\dagger}[1] \cap [2]}\,\gamma_{\forall i\notin}{}'$$

Implementation

- Base prover with subsumption and pruning.
- Addition 2 new memos for rules already used : $\epsilon \in \notin$ and *interval*.
- One new function for rules (priority $<$ standard rules) :
  - filters formulae $\in$ and $\notin$, send them to the oracle,
  - gets the oracle's result and closes or not.

Coq proof term generation

- One unique kind of node in the proof tree.
- Construction of the term : `unfold` functions then tactic `lra`.
- Need to chose a member in an interval (handling of ϵ-terms) :
  - choice function excluding ∞'s
  - first lower bound $\neq \infty$
  - 0 if interval $=]-\infty, +\infty[$
- Encode $e \in [l, u]$ by $l \leq e \wedge e \leq u$.

Future work (1/2)

Simple things (really bad idea)

- Replace floats by rationals in arbitrary precision.
  - Remain : rounding issues due to complementary representation.
  - Remain : rounding issues due to non-rational functions
    - there are reasons why `Zarith` does not provide cos etc. !
  - Remain : rounding due to time discretization step.

Future work (2/2)

Clearly less simple

- ODEs, integration by intervals, guaranteed arithmetic (DynIbex).
  - − Do not solve rounding due to complementary representation.
  - \+ Should solve other rounding issues.
  - o Theory decidability (≪ provable ≫, ≪ $\overline{\text{provable}}$ ≫ + ≪ may-be ≫) ?
  - o Coq term production ?

Clearly less simple even without ODEs etc.

- Other relational operators : $\exists t_1, \forall t_2, t_2 > t_1 \Rightarrow f(t_2) > f(t_1)$
- Mix meta-variables and ϵ-terms :
  - Interesting if quantification on intervals or other operators.
  - $\exists b : \mathit{interv}, \forall t : \mathit{float}, t \in [2,3] \Rightarrow f(t) \in b \wedge g(t) \notin b$
- Quantify on bounds :
  - $\forall b_1, b_2 : \mathit{float}, t \in [2,3] \Rightarrow f(t) \in [b_1, b_2] \wedge g(t) \notin [b_1, b_2]$

Thanks

The end