On a Decidable Fragment of d$\mathcal{L}$

or, The Next 700 (Un)decidable Fragments of d$\mathcal{L}$

David M Kahn   Siva Somayyajula

Carnegie Mellon University

December 11, 2018

$$\Delta_0\mathcal{L}$$

Motivation

If you or a loved one has been frustrated trying to formally verify systems,

Motivation

If you or a loved one has been frustrated trying to formally verify systems,

you may be entitled to righteous indignation.

Motivation

Why is formal verification so frustrating?

- complicated and tedious proofs
- lots of work for no product change
- people only care it looks like it works

Motivation

Why is formal verification so frustrating?

- complicated and tedious proofs
- lots of work for no user-facing change
- ~~people only care it looks like it works~~
  Cyberphysical systems are life-critical!

Motivation

Results

- Found and implemented decidable fragments of d$\mathcal{L}$ to ease verifying cyberphysical systems
- Found undecidable/inter-decidable fragments of d$\mathcal{L}$ to ease future decidability research

(Un)decidability Results

Arithmetical Approaches

	Integer Arithmetic	d$\mathcal{L}$
positive $\exists$	MRDP's Diophantine	Post Correspondence
positive $\forall$	polynomial ID testing	extended Platzer-Tan
bounded	finitary checking	Post Correspondence
single variable	trivial	Post Correspondence
purely $+$	Presburger	Post Correspondence
purely $\times$	Skolem	Post Correspondence

(Un)decidability Results

Structural Approaches

	d$\mathcal{L}$
without $\cup$	MRDP's Diophantine
without ;	piecewise constant derivative reachability
without $*$	(exponential) polynomial star-free
only $:=$	Post Correspondence
only $?(-)$	reduction to $\mathrm{FOL}_{\mathbb{R}}$
only $x' = f(x)$ & Q	piecewise constant derivative reachability
simultaneously $[\alpha]P \land \langle\alpha\rangle P$	when $[\alpha]P$ is

Polynomial Star-Free Fragment

How can this be used for theorem proving?

- Work with simple ODEs
- Human identifies loop invariant
- That's it! Everything else is free.

Polynomial Star-Free Fragment

- Idea: sound translation to $\mathrm{FOL}_{\mathbb{R}}$

Polynomial Star-Free Fragment

- Idea: sound translation to $\mathrm{FOL}_{\mathbb{R}}$
  - $[x := e]P(x) \leftrightarrow P(e)$
  - $[\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$

Polynomial Star-Free Fragment

- Idea: sound translation to $\mathrm{FOL}_{\mathbb{R}}$
  - $[x := e]P(x) \leftrightarrow P(e)$
  - $[\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$
  - $[x' = f(x)]P(x) \leftrightarrow \forall t \geq 0 \; P(x(t))$ where $x'(t) = f(x(t))$

Polynomial Star-Free Fragment

- Idea: sound translation to $\mathrm{FOL}_{\mathbb{R}}$
  - $[x := e]P(x) \leftrightarrow P(e)$
  - $[\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$
  - $[x' = f(x)]P(x) \leftrightarrow \forall t \geq 0\ P(x(t))$ where $x'(t) = f(x(t))$
- Remove iteration (star/asterate)

Polynomial Star-Free Fragment

- Idea: sound translation to $\mathrm{FOL}_{\mathbb{R}}$
  - $[x := e]P(x) \leftrightarrow P(e)$
  - $[\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$
  - $[x' = f(x)]P(x) \leftrightarrow \forall t \geq 0\ P(x(t))$ where $x'(t) = f(x(t))$
- Remove iteration (star/asterate)
  - $\alpha^* = ?\textbf{true} \cup \alpha; \alpha^*$

Polynomial Star-Free Fragment

- Idea: sound translation to $\mathrm{FOL}_{\mathbb{R}}$
  - $[x := e]P(x) \leftrightarrow P(e)$
  - $[\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$
  - $[x' = f(x)]P(x) \leftrightarrow \forall t \geq 0\ P(x(t))$ where $x'(t) = f(x(t))$
- Remove iteration (star/asterate)
  - $\alpha^* = ?\mathbf{true} \cup \alpha; \alpha^*$
  - Loop invariants?

Polynomial Star-Free Fragment

- Idea: sound translation to $\text{FOL}_{\mathbb{R}}$
  - $[x := e]P(x) \leftrightarrow P(e)$
  - $[\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$
  - $[x' = f(x)]P(x) \leftrightarrow \forall t \geq 0 \; P(x(t))$ where $x'(t) = f(x(t))$
- Remove iteration (star/asterate)
  - $\alpha^* = ?\textbf{true} \cup \alpha; \alpha^*$
  - Loop invariants?
  - Encode integer arithmetic: undecidable

Polynomial Star-Free Fragment

- Idea: sound translation to $\mathrm{FOL}_{\mathbb{R}}$
  - $[x := e]P(x) \leftrightarrow P(e)$
  - $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$
  - $[x' = f(x)]P(x) \leftrightarrow \forall t \geq 0\ P(x(t))$ where $x'(t) = f(x(t))$
- Remove iteration (star/asterate)
  - $\alpha^* = ?\mathbf{true} \cup \alpha;\alpha^*$
  - Loop invariants?
  - Encode integer arithmetic: undecidable
- Restrict to polynomial solutions of ODEs

Polynomial Star-Free Fragment

Theorem (DAG condition)

Given $S \equiv x_i' = e_1, \ldots, x_n' = e_n$, *let* G *be a digraph s.t.*

$$\text{edge from } x_i' = e_i \text{ to } x_j' = e_j \iff x_i \text{ occurs in } e_j$$

Then, S *has a polynomial solution* $\Longleftarrow$ G *is acyclic.*

Polynomial Star-Free Fragment

Theorem (DAG condition)

Given $S \equiv x_i' = e_1, \ldots, x_n' = e_n$*, let* G *be a digraph s.t.*

$$\textit{edge from } x_i' = e_i \textit{ to } x_j' = e_j \iff x_i \textit{ occurs in } e_j$$

Then, S *has a polynomial solution* $\Longleftarrow$ G *is acyclic.*

Proof sketch.

Back-sub in the topological order of G. □

Polynomial Star-Free: Implementation

- $\sim$ 500 lines in OCaml

Polynomial Star-Free: Implementation

- $\sim$ 500 lines in OCaml
- Shallow embedding of d$\mathcal{L}$ using weak higher-order abstract syntax

Polynomial Star-Free: Implementation

- ~ 500 lines in OCaml
- Shallow embedding of d$\mathcal{L}$ using weak higher-order abstract syntax
- Polynomial manipulation and ODE solver

Polynomial Star-Free: Implementation

- ~ 500 lines in OCaml
- Shallow embedding of d$\mathcal{L}$ using weak higher-order abstract syntax
- Polynomial manipulation and ODE solver
- Z3 for quantifier elimination

Polynomial Star-Free: Demo

Verifying $x \geq 0 \land v \geq 0 \land a \geq 0 \rightarrow [x' = v, v' = a]\; x \geq 0$

```
utop # check
((x >= !0. && v_ >= !0. && a >= !0.) =>
  (!| (["x" ^= v_; "v" ^= a] & tt) |! (x >= !0.)));;
```

```
Common.Valid
 "unsat\n((declare-fun _x0!0 () Real)\n(proof\n
 ((?x254 (* a _x0!0 _x0!0)))\n (let ((?x257 (*
251 ?x257)))\n (let (($x287 (>= ?x260 0.0)))\n
```

Conclusion and Future Work

- Survey of restrictions for (un)decidability

Conclusion and Future Work

- Survey of restrictions for (un)decidability
- Decision procedures for theorem proving

imgflip.com