

SAT s diferenciálními rovnicemi

Diplomová práce

Kolárik Tomáš

kolarto5@fit.cvut.cz

Vedoucí práce: doc. Dipl.-Ing. Dr. techn. Stefan Ratschan

13. května 2018

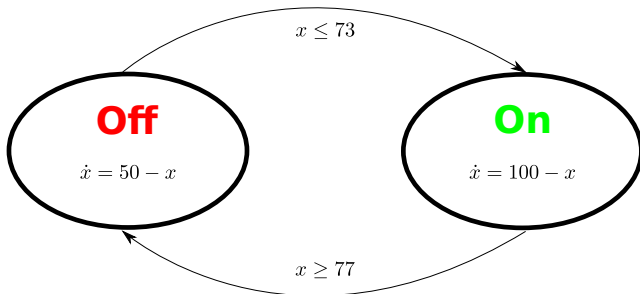
11 slajdů, 10 minut

Obsah prezentace

- 1 Motivace.
- 2 Cíle práce.
- 3 Výsledky.
- 4 Ukázka úloh.
- 5 Realizace.

Motivační příklad

- Ke *spolehlivé* činnosti přístroje je nutné dodržet provozní teplotu.
- Řešení: použití *termostatu*.
- Termostat popíšeme *automatem*.
 - ▶ Rozsah povolené teploty specifikujeme jako invarianty (nejsou na obrázku).
- Jak verifikovat správnou funkci termostatu?
 - ▶ Tj. dodržení invariant.



Motivace (1)

- Používanou spolehlivou metodou *garance* dodržení specifikací je **formální verifikace**.
 - ▶ K tomu je nutné sestavit matematický *model* systému.
- Dnes hojně využívaný způsob: **SAT**.

Problém

- *Vestavné systémy* interagují s *fyzikálním okolím*.
- Přirozený popis fyzikálních jevů: **diferenciální rovnice**.
 - ▶ Ordinary differential equation (ODE).
- SAT (ani jeho aritmetická rozšíření) *neumí* ODE.

Motivace (2)

Současný stav

- Řešice kombinující SAT a soustavy ODE již existují.
- K řešení ODE ale používají intervalovou aritmetiku.
- Důsledky:
 - ▶ Umožňují intervalové počáteční podmínky ODE.
 - ▶ Garantují maximální dosaženou chybu.
 - ▶ Ale jsou **pomalé**.

Cíl práce

K řešení ODE použít **klasické numerické metody**:

- Vyžadují jednoznačné počáteční podmínky.
- Garantují (jen) *konvergenci* dosažené chyby.
- Mohou být méně přesné, ale jsou rychlejší.

- ① Ověřit koncept, který k řešení ODE používá klasické numerické metody.
- ② Kombinovat zvolené řešení ODE s řešením problému SMT.
 - ▶ SMT: Satisfiability Modulo Theories (rozšíření SAT o aritmetické teorie).
- ③ Realizovat prototypovou implementaci řešiče SMT a ODE.
- ④ Srovnat výkonnost prototypu se stávajícím řešičem dReal.
 - ▶ dReal pochází z disertační práce na Carnegie Mellon University.

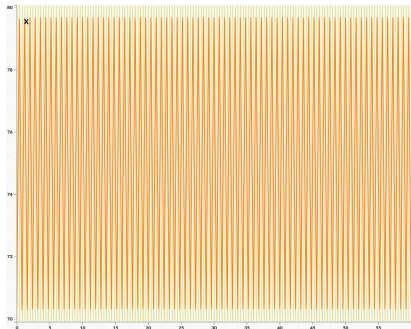
- Náš prototyp si v některých úlohách počíná mnohem **rychleji** než dReal.
 - ▶ Zatím se jedná zejména o úlohy řízené časem.
- Tj. podařilo se mi **potvrdit**, že zvolený **koncept** je **nadějný** pro lepší použití **v praxi**.
- Velký rozdíl ve výpočtu úloh s pevnými a intervalovými podmínkami.
 - ▶ Intervalové podmínky lze aproximovat výčtem hodnot v logickém součtu.
 - ▶ I dReal si pak počíná mnohem rychleji.

Ukázkové úlohy (1)

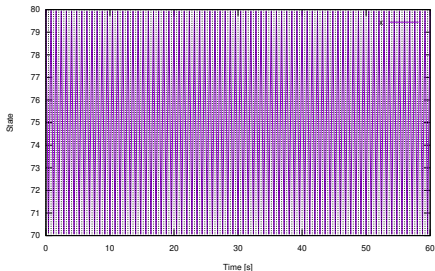
Termostat

- x ... provozní teplota.
- Nutné dodržet invariant $70 \leq x \leq 80$.
- Systém je řízen *časem* o fixní periodě.
- Srovnání délky výpočtu dReal a našeho prototypu: 46 a 0,5 s.

(a) dReal



(b) Náš koncept



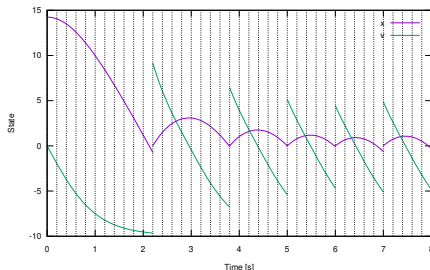
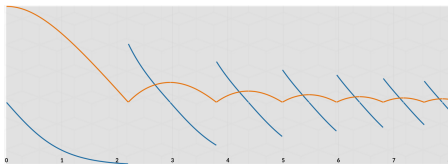
Ukázkové úlohy (2)

Skákající míč

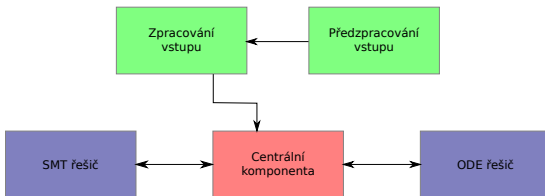
- x ... výška míče, v ... rychlost.
- Nutné dodržet invariant $x \geq 0$ nezávisle na časové periodě.
- Systém je řízen *událostmi* (změna pád/odraz).
- Srovnání délky výpočtu dReal a našeho prototypu: 0,1 a 0,5 s.
- Naše *implementace* je nevhodná kvůli nezávislosti na časové periodě.

(b) Náš koncept

(a) dReal



- Vstupní jazyk je podobný standardu SMT-LIB.
 - ▶ Přidány makra pro parametrizované generování kódu.
- SMT i ODE řešič realizovány jako výměnné samostatné komponenty.
- Centrální komponenta zajišťuje:
 - ▶ vzájemnou komunikaci řešičů,
 - ▶ prohledání všech potřebných vstupních kombinací.



- Cílem bylo aplikovat **odlišný přístup** v integraci ODE.
 - ▶ Použít potenciálně méně přesné, ale rychlejší metody.
 - ▶ Kombinovat ODE s problémem SAT či jeho rozšířením.
- Navržený koncept jsem aplikoval v prototypové implementaci.
- Prototyp jsem srovnal se stávajícím řešičem dReal.
 - ▶ V některých úlohách jsem dosáhl výrazně **rychlejšího výpočtu**.
 - ▶ Podařilo se mi **potvrdit zvolený koncept**.
- Prototyp přijímá vstupní jazyk, který lze parametrizovat pomocí maker.