IV120 Spojité a hybridní systémy

Hybridní systémy – pokr.

David Šafránek

Jiří Barnat

Jana Fabriková

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

EVROPSKÁ UNIE

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Modelování hybridních systémů

Pozorování

- Hybridní automaty slouží pro teoretický popis reálného hybridního systému.
- Díky abstrakci a zjednodušování, je možné specifikovat nereálné situace.

Rizika modelování

- Lze vytvořit systém, který nemá řešení.
- Lze vytvořit systém, který jehož řešení nejsou reálná.
- Lze vytvořit systém, který má nejednoznačná řešení.

Terminologie

- O systému, který nemá řešení (neexistuje běh systému) říkáme, že je *blokující*.

Reálnost běhů

Pozorování

- Neblokující systém negarantuje, že řešení jsou reálná.
- Neblokující systém neimplikuje časově nekonečná chování.

Nereálná chování

- Běhy, ve kterých se provede nekonečně mnoho diskrétních přechodů v konečném čase – tzv. ZENO běhy.
- Vznikají abstrakcí a zjednodušováním.

Diskuze

- Proč míček neskáče donekonečna?
- Je důležité pochopit abstrakce reálného světa, které mohou vést k ZENO chování.

Nedeterminismus

Nedeterminismus

- Obecně lze charakterizovat jako absenci unikátního řešení, tj hybridní automat akceptuje více různých exekucí pro jeden iniciální stav.
- Při omezení na Lipschitz spojité funkce, které mají unikátní řešení, může být důvodem k nedeterminismu diskrétní složka.

Úmyslný nedeterminismus

- Může být použit pro modelování nejistoty.
- Je důležité umět rozlišit úmyslné použití nedeterminismu od neúmyslného.

Pozorování

- Nedeterminismus přináší problémy při analýze chování hybridních systémů i při syntéze kontrolérů.

Problémy simulace/analýzy hybridních systémů

Existence řešení

- Jak detekovat existenci běhu (neblokujícnost)?
- Jak detekovat ZENO chování?

Unikátnost

- Jak simulovat nedeterminismus?
  - Diskrétní přechod vs spojitá evoluce.
  - Diskrétní přechod vs diskrétní přechod.
- As-soon-as sémantika.

Nespojitost

- Jak detekovat splnitelnost stráží přechodů?
- Invariant stavu končí otevřeným intervalem $[a, b)$ a následný přechod probíhá v čase $[b]$.

Kompozicionalita

- Jak komponovat systém složené z hybridních komponent?

Neblokující a deterministický hybridní automat

Neblokující hybridní automat

- Hybridní automat H se nazývá neblokující, pokud pro všechny iniciální stavy $(\hat{q}, \hat{x}) \in \mathit{Init}$ existuje nekonečný běh začínající v $(\hat{q}, \hat{x})$.

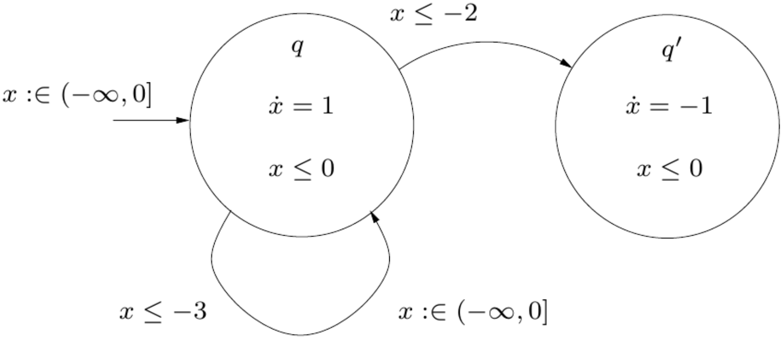
Deterministický hybridní automat

- Hybridní automat H se nazývá deterministický, pokud pro všechny iniciální stavy $(\hat{q}, \hat{x}) \in \mathit{Init}$ existuje nejvýše jeden maximální běh začínající v $(\hat{q}, \hat{x})$.

Příklad

Pozorování

- Následující automat je blokující a nedeterministický.



Množina dosažitelných stavů

Definice dosažitelnosti

- Stav $(\hat{q}, \hat{x}) \in Q \times X$ hybridního automatu H se nazývá dosažitelný, pokud existuje konečný běh (τ, q, x), která končí v $(\hat{q}, \hat{x})$, tj. $\tau = \{[\tau_i, \tau_i']\}_0^N$, $N < \infty$ a $(q_N(\tau_N'), x_N(\tau_n')) = (\hat{q}, \hat{x})$.

Množina dosažitelných stavů

- Množinu dosažitelných stavů hybridního automatu H značíme $Reach$, $Reach \subseteq Q \times X$.
- Fundamentální problém v oblasti hybridních systémů je výpočet množiny $Reach$ pro zadaný hybridní automat.

Cvičení

- Zdůvodněte, proč $Init \subseteq Reach$.

Množina tranzitních stavů

Neformálně

- Množina stavů H, ze kterých není možný spojitý vývoj.

Předpoklady

- Pro $(\hat{q}, \hat{x}) \in Q \times X$ a nějaké $\epsilon > 0$ uvažme řešení $x(\cdot) : [0, \epsilon) \to \mathbf{R}^n$ následující diferenciální rovnice:

$$\frac{dx}{dt} = f(\hat{q}, x), \text{ kde } x(0) = \hat{x}$$

- Za předpokladu Lipschitz spojitosti v x, řešení výše uvedené rovnice existuje a je unikátní.

Definice

- $Trans = \{(\hat{q}, \hat{x}) \in Q \times X \mid \forall \epsilon > 0\ \exists t \in [0, \epsilon) \text{ takové, že } (\hat{q}, x(t)) \notin Dom(\hat{q})\}$.

Spodní odhad množiny tranzitních stavů

Pozorování 1

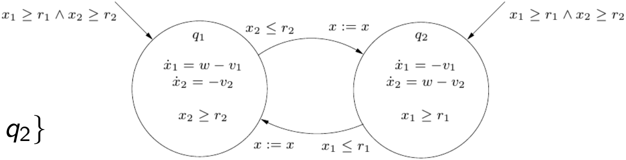
- Spojitá evoluce nemůže probíhat mimo invariant (doménu) stavu.
- Tedy pro každý diskrétní stav $q \in Q$, komplement domény stavu q, značený jako $Dom(q)^c$ musí být součástí množiny $Trans$.

$$\bigcup_{q \in Q} \{q\} \times Dom(q)^c \subseteq Trans$$

Pozorování 2

- Může $Trans$ obsahovat i nějaké části z $\{q\} \times Dom(q)$?
- Ano, pokud je doména uzavřená množina (obsahuje své hranice), části této hranice mohou být součástí $Trans$.

Řešený příklad – Vodní nádrže



- $Q = \{q_1, q_2\}$
- $X = \mathbf{R} \times \mathbf{R}$
- $f(q_1, x) = \begin{bmatrix} w - v_1 \\ -v_2 \end{bmatrix} \quad f(q_2, x) = \begin{bmatrix} -v_1 \\ w - v_2 \end{bmatrix}$
- $Init = \{q_1, q_2\} \times \{x \in \mathbf{R} \times \mathbf{R} \mid x_1 \geq r_1 \wedge x_2 \geq r_2\}$
- $Dom(q_1) = \{x \in \mathbf{R} \times \mathbf{R} \mid x_2 \geq r_2\}$
  $Dom(q_2) = \{x \in \mathbf{R} \times \mathbf{R} \mid x_1 \geq r_1\}$
- $E = \{(q_1, q_2), (q_2, q_1)\}$
- $G(q_1, q_2) = \{x \in \mathbf{R} \times \mathbf{R} \mid x2 \leq r2\}$
  $G(q_2, q_1) = \{x \in \mathbf{R} \times \mathbf{R} \mid x_1 \leq r_1\}$
- $R(q_1, q_2, x) = R(q_2, q_1, x) = \{x\}$

Řešený příklad – Vodní nádrže

Příklad

- Předpokládejme, že $0 < v_1, v_2 < w$. Spočítejte množinu *Reach* a množinu *Trans*.

Náznak řešení

- *Reach* obsahuje iniciální stavy:

$$Reach \supseteq \{q_1, q_2\} \times \{x \in \mathbf{R}^2 \mid (x_1 \geq r_1) \wedge (x_2 \geq r_2)\}$$

- Může *Reach* obsahovat i jiné stavy? Indukcí vzhledem k délce hybridní časové řady hypotetického běhu ukážeme, že ne.

$$Reach \subseteq \{q_1, q_2\} \times \{x \in \mathbf{R}^2 \mid (x_1 \geq r_1) \wedge (x_2 \geq r_2)\}.$$

- Uvážením obou inkluzí dostáváme, že

$$Reach = \{q_1, q_2\} \times \{x \in \mathbf{R}^2 \mid (x_1 \geq r_1) \wedge (x_2 \geq r_2)\}$$

Důkaz matematickou indukcí k délce běhu

Myšlenka použití indukce

- Indukce zahrnuje argumentaci pro spojitý vývoj času v rámci intervalu, a demonstraci, že po provedení diskrétního přechodu, invariant indukce platí.

Indukce

- Mějme běh (τ, q, x). Jestliže $\tau' \sqsubseteq \tau$ a tvrzení platí pro běh (τ', q, x) pak platí i pro běh (τ, q, x).
- BÁZE:
  - $\mathit{Reach} \subseteq \mathit{Init}$
- INDUKČNÍ KROK:
  - Diskuze spojité evoluce.
  - Diskuze diskrétního přechodu.

Řešený příklad – Vodní nádrže

Pozorování 1

- Spojitá evoluce není možná pokud
  $q = q_1$ a $x_2 < r_2$, nebo $q = q_2$ a $x_1 < r_1$
- tudíž

$$Trans \supseteq (\{q_1\} \times \{x \in \mathbf{R}^2 \mid x_2 < r_2\}) \cup (\{q_2\} \times \{x \in \mathbf{R}^2 \mid x_1 < r_1\}).$$

- Naopak víme, že spojitá evoluce je možná, pokud
  $q = q_1$ a $x_2 > r_2$, nebo $q = q_2$ a $x_1 > r_1$
- což dává

$$Trans \subseteq (\{q_1\} \times \{x \in \mathbf{R}^2 \mid x_2 \leq r_2\}) \cup (\{q_2\} \times \{x \in \mathbf{R}^2 \mid x_1 \leq r_1\}).$$

Krajní případy

- Pokud například $q = q_1$ a $x_2 = r_2$. Plynutím času v q_1 by x_2 kleslo pod r_2, což je mimo doménu stavu. Tudíž hraniční hodnoty jsou v tomto případě součástí *Trans*.

$$Trans = (\{q_1\} \times \{x \in \mathbf{R}^2 \mid x_2 \leq r_2\}) \cup (\{q_2\} \times \{x \in \mathbf{R}^2 \mid x_1 \leq r_1\})$$

Úkol

- Zkuste odvodit, nebo alespoň ohraničit množiny *Reach* a *Trans* pro ostatní hybridní systémy definované v rámci minulé přednášky.

Podmínka neblokujícnosti

Pozorování

- Hybridní automat je neblokující pokud pro všechny dosažitelné stavy, ve kterých není možná spojitá evoluce, je možné provést diskrétní přechod.

Lemma 1

- Hybridní automat H je neblokující, pokud pro všechny $(\hat{q}, \hat{x}) \in \mathit{Reach} \cap \mathit{Trans}$ existuje $\hat{q}' \in Q$ takové, že $(\hat{q}, \hat{q}') \in E$ a $\hat{x} \in G(\hat{q}, \hat{q}')$. Pokud H je deterministický, pak je neblokující tehdy a jen tehdy, platí-li uvedená podmínka.

Podmínka determinističnosti

Neformálně

- Automat je nedeterministický, pokud existuje dosažitelný stav, ze kterého se může realizovat alespoň jeden diskrétní přechod a zároveň z tohoto stavu může probíhat spojitá evoluce, anebo se mohou realizovat alespoň dva diskrétní přechody vedoucí do jiných diskrétních stavů.

Lemma 2

- Hybridní automat H je deterministický tehdy a jen tehdy, pokud pro všechny stavy $(\hat{q}, \hat{x}) \in \mathit{Reach}$ platí:
  1. pokud $\hat{x} \in G(\hat{q}, \hat{q}')$ pro nějakou $(\hat{q}, \hat{q}') \in E$, pak $(\hat{q}, \hat{x}) \in \mathit{Trans}$
  2. pokud $(\hat{q}, \hat{q}') \in E$ a $(\hat{q}, \hat{q}'') \in E$ takové, že $\hat{q}' \neq \hat{q}''$, pak $\hat{x} \notin G(\hat{q}, \hat{q}') \cap G(\hat{q}, \hat{q}'')$
  3. pokud $(\hat{q}, \hat{q}') \in E$ a $\hat{x} \in G(\hat{q}, \hat{q}')$, pak $R(\hat{q}, \hat{q}', \hat{x}) = \{\hat{x}'\}$, tj množina obsahuje právě jeden konkrétní prvek.

Využití Lemmat 1 a 2

Tvrzení

- Hybridní automat akceptuje unikátní nekonečný běh pro každý iniciální stav, pokud splňuje podmínky Lemat 1 a 2.

Poznámka

- Lemata se vyjadřují o vlastnostech stavů v množině *Reach*. Pokud nás však zajímá existence a unikátnost běhů pouze z počátečních podmínek, je možné formulovaná lemata rozšířit na všechny možné stavy (i nedosažitelné) a tím se vyhnout náročnému výpočtu množiny *Reach*.

Příklad

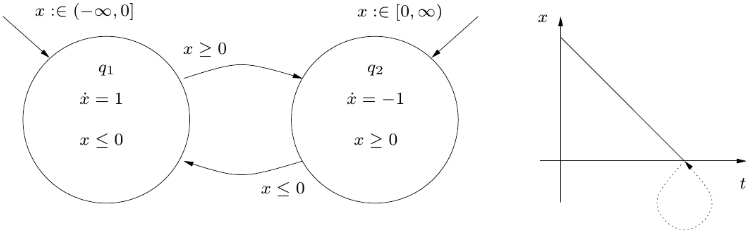
Úkol

- Analyzujte platnost podmínek uvedených lemat na příkladu s vodními nádržemi za předpokladu $0 < v_1, v_2 < w$.
- Je systém deterministický?
- Je systém neblokující?
- Je systém prakticky možný?

Úkol

- Formulujte paradox "Achilles a želva".
- Analyzujte chování hybridních automatů na následujícím slajdu.

Příklady ZENO běhů



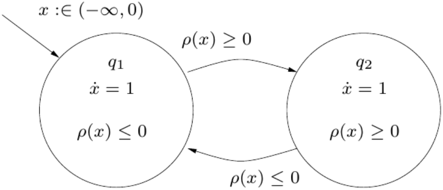
Příklady ZENO běhů

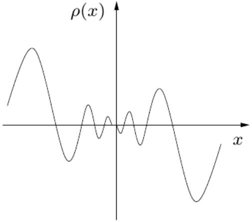
Nechť

$$\rho(x) = \begin{cases} \sin\left(\frac{1}{x^2}\right)\exp\left(-\frac{1}{x^2}\right) & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

pak

- následující hybridní systém má v intervalu $(-\epsilon, 0]$ nekonečně mnoho průniků s osou x.





Analýza a syntéza hybridních systémů (HS)

Motivace modelování

- Cílem modelování HS je odvození vlastností reálných systémů z vlastností modelů, a syntéza kontrolérů (podmínek pro vykonání kontrolních událostí).

Verifikace

- Vykazuje hybridní systém popsaný hybridním automatem požadované chování (splňuje specifikaci)?

Syntéza

- Jestliže je možnost volby při návrhu systému, je možné tento návrh udělat tak, aby výsledný systém splňoval danou specifikaci?

Validace

Validace

- Proces ověření, že teoretický návrh hybridním automatem se při praktické realizaci chová odpovídajícím způsobem.
- Vyhovující teoretický model, může být vzhledem k uvažovaným abstrakcím neimplementovatelný.

Obvyklé workflow

- Syntéza
- Verifikace
- Validace

Specifikace

Stabilita

- Typická vlastnost požadovaná v čistě spojitých systémech.
- Požadovat stabilitu hybridního systému vyžaduje definovat pojem stability v diskrétní složce.

Specifikace množinou stavů

- Specifikace bezpečných a zakázaných oblastí.

Specifikace množinou trajektorií

- Vlastnosti hybridních automatů, které se dají popsat vlastnostmi běhů.
- Množina povolených běhů hybridního automatu.
- Formální popis vlastností běhů s využitím modálních a temporálních logik. (CTL, LTL, CTL*).

Metody analýzy

Deduktivní metody

- Matematické metody dokazování/odvozování vlastností hybridních systémů (matematická indukce).
- Nealgoritmizovatelné.

Model Checking

- Algoritmická procedura rozhodující, zda formálně popsaný hybridní systém splňuje formálně specifikované požadavky.
- Problém je rozhodnutelný pouze pro vybrané podtřídy hybridních automatů.

Softwarové simulace

- Používané za účelem výpočtu množiny *Reach*.
- Výsledek je často pouze aproximací skutečné množiny.

Deduktivní metody – Invariantní množina

Použití deduktivních metod

- Typickým cílem metody je stanovit hranice množiny *Reach* skrze tzv. **invariantní množinu**.
- Invariantní množina je množina pro níž platí, že začne-li výpočet hybridního systému v dané množině, tak tuto množinu nikdy neopustí.

Definice invariantní množiny

- Množina stavů $M \subseteq Q \times X$ hybridního automatu H se nazývá *invariantní* pokud pro všechna $(\hat{q}, \hat{x}) \in M$, všechna řešení (τ, q, x) začínající v $(\hat{q}, \hat{x})$, všechna $I_i \in \tau$ a všechna $t \in I_i$ platí, že $(q_i(t), x_i(t)) \in M$.

Deduktivní metody – Vlastnosti invariantní množiny

Pozorování

- Sjednocení a průnik dvou invariantních množin automatu H jsou také invariantní množiny H.
- Pokud M je invariantní množina a $Init \subseteq M$, pak $Reach \subseteq M$.

Využití

- Je-li dána specifikace povolených stavů hybridního automatu (množina F), je možné identifikovat různé invariantní množiny splňující

$$Init \subseteq M \subseteq F$$

  a pro účely přesného odhadu množiny $Reach$ tyto proniknout.

Cvičení

- Zdůvodněte výše uvedená tvrzení.
- Rozmyslete, jak postupovat při ukazování faktu, že nějaká množina M je invariantní množinou hybridního automatu H.

Model Checking

Zjednodušení

- V rámci tohoto kurzu se omezíme pouze na algoritmický test dosažitelnosti daného stavu pro vybrané podtřídy hybridních automatů.

Uvažované podtřídy hybridních automatů

- Časové automaty (TA).
- Rektangulární hybridní automaty (RHA).
- Lineární hybridní automaty (LHA).

Softwarové nástroje

- UPPAAL – časové automaty
- PHaVer – RHA, částečně LHA (HyTech)

Časové automaty

Omezení

- Všechny derivace podle nichž se automat řídí při spojité evoluci stavu mají tvar:

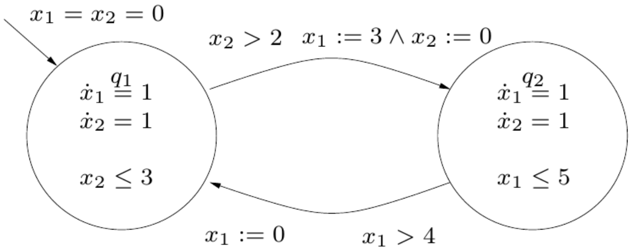
$$\frac{dx_i(t)}{dt} = 1$$

- V diskrétní složce je navíc položeno omezení na R, kdy je dovoleno buď ponechat stávající hodnotu spojité proměnné, nebo ji „nastavit“ na jinou celočíselnou hodnotu (typicky 0).
- *Dom* a *G* definováno pouze s použitím relací $\leq$ a $\geq$ na celočíselných hodnotách.

Intuice

- Konečný automat s množinou spojitých proměnných pro měření uplynulého času.
- Měřené hodnoty je možné resetovat při provedení diskrétního přechodu.

Příklad časového automatu



Cvičení

- Zakreslete vývoj hodnot spojitých proměnných v čase.
- Na dvourozměrném grafu s osami x_1 a x_2 ukažte jak se mění hodnoty proměnných v čase.
- Jak se projeví fakt, že dovolíme pouze resety na hodnotu 0?

Regionová abstrakce

Klíčové pozorování

- Vzhledem k tomu, že všechna porovnání v časových automatech jsou celočíselná, automat není schopen rozlišit dvě různé hodnoty spojité proměnné se stejnou celočíselnou částí.

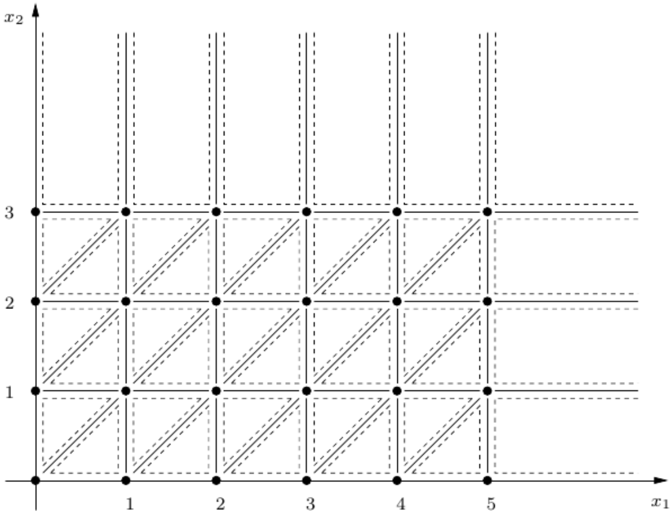
Třídy ekvivalence na spojité doméně

- Je-li c nejvyšší celé číslo, na které je spojitá proměnná porovnávána, pak lze tuto spojitou proměnnou ekvivalentně reprezentovat jednou hodnotou z následující posloupnosti:

$$[0], (0, 1), [1], (1, 2), [2], \ldots [c-1], (c-1, c), [c], (c, \infty)$$

- Abstrahovaná doména je konečná pro každou proměnnou.
- Lze sestrojit konečný automat, který věrně simuluje časový automat a otázku verifikace algoritmicky rozhodnout nad tímto konečným automatem.

Regionová abstrakce



Rektangulární hybridní automaty (RHA)

Omezení

- Všechny derivace podle nichž se automat řídí při spojité evoluci stavu mají tvar:

$$a \leq \frac{dx_i(t)}{dt} \leq b,$$

  kde a a b jsou racionální konstanty.
- Při specifikaci automatu se neuvádí diferenciální rovnice, ale pouze konstanty a a b, jakožto krajní meze.

Cvičení

- Uvažte rektangulární automat s dvěmi spojitými proměnnými x_1 a x_2 . Na dvojrozměrném grafu s osami x_1 a x_2 demonstrujte vývoj hodnot proměnných, který odpovídá spojité evoluci.
- Odkud pochází název této třídy hybridních automatů?

Algoritmická rozhodnutelnost RHA

Dosažitelnost

- Problém dosažitelnosti daného stavu z konkrétního daného iniciální stavu je rozhodnutelný, pokud diskrétní přechody automatu resetují (reinicializují) hodnoty proměnných na konečnou množinu konkrétních hodnot.
- Největší známá rozhodnutelná podtřída RHA.

Nerozhodnutelnost

- Relaxace od přesných reinicializací vede k podtřídě hybridních automatů, pro níž je problém dosažitelnosti nerozhodnutelný.

Lineární hybridní automaty (LHA)

Definice

- Pokud $k_0, \ldots, k_m$ jsou definované konstanty a $x_1, \ldots, x_m$ proměnné, pak výraz tvaru $k_0 + k_1x_1 + k_2x_2 + \cdots + k_mx_m$ se nazývá *lineární výraz*.
- Pokud t_1, t_2 jsou lineární výrazy pak výraz tvaru $t_1 \leq t_2$ se nazývá *lineární nerovnost*.
- Hybridní automat H se nazývá **lineární**, pokud *Init*, *Dom*, G a f jsou definovány jako boolovské kombinace lineárních nerovností.

Nerozhodnutelnost

- Problém dosažitelnosti stavu je pro LHA nerozhodnutelný.
- Dokázáno redukcí z problému zastavení.
- Implementované algoritmy negarantují terminaci (HyTech).