Analýza systémů založená na modelech

2022/2023

Domácí úloha 2

Pavel Šesták (xsesta07)

Brno, 13. dubna 2023

Obsah

Seznam obrázků

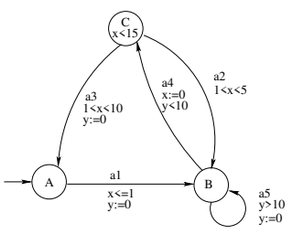
Seznam tabulek

MBA 2022/2023 – Úloha 2: Časované automaty

1. Uvažujme automat $\mathcal{A}_1$ na obrázku 1.

   - Obsahuje tento automat zeno běh? Dokažte, nebo vyvraťte.
   - Obsahuje tento automat timelock? Pokud ano, uveďte běh vedoucí do timelocku.

   2 body

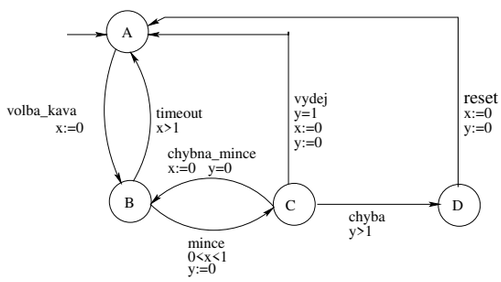


Obrázek 1: Časovaný automat $\mathcal{A}_1$

2. Uvažujme časovaný automat $\mathcal{A}_2$ na obrázku 2 s množinou atomických predikátů $AP = \{init, error, run\}$ a funkcí L definovanou následovně:
   $L(A) = \{init, run\}, L(D) = \{error\}, L(B) = L(C) = \{run\}$.

   - Sestavte abstrakci založenou na regionech (stačí sestrojit pouze stavy dostupné z počáteční konfigurace).
   - Rozhodněte, zda je dostupný stav ve kterém platí predikát $error$.
   - Rozhodněte zda platí $\mathcal{A}_2 \models \exists\ (run\ U^{(3,4)} error)$.
   - Rozhodněte zda platí $(B, x = 3, y = 0.5) \models \forall\ (true\ U^{<2}\ init)$.
   - Rozhodněte zda platí $\mathcal{A}_2 \models \exists \diamond (error \wedge x = 2)$

   Svá tvrzení zdůvodněte. 4 body



Obrázek 2: Časovaný automat $\mathcal{A}_2$

3. V nástroji UPPAAL modelujte automat pro vracení lahví. Automat se nachází v několika stavech: 1. připraven, 2. v činnosti, 3. příjem lahve, 4. timeout, 5. výdej dokladu, 6. chyba, 7. reset.

   - Pokud je stroj v činnosti, tak je možné vložit další lahev, nebo požádat o výdej dokladu.
   - Po vložení lahve se stroj do 1 časové jednotky vrací do stavu v činnosti.
   - Při požadavku na výdej dokladu je stroj do 2 časových jednotek připraven.
   - Pokud je stroj v činnosti 100 časových jednotek, tak nastane timeout, po kterem do 2 časových jednotek následuje výdej dokladu.
   - V jakoukoliv chvíli může nastat chyba.
   - Ze stavu chyba je možné vyvolat reset. Pak do 2 časových jednotek po resetu je stroj připraven.

   Váš model bude splňovat následující požadavky vložené ve formě TCTL formulí do části *Verifier* a ověřené nástrojem.

   - `A[] not deadlock`
   - Vždy je možné dostat se do stavu připraven.

   Dále v části *Verifier* doplňte a ověřte (eventuelně vyvraťte) alespoň jednu další TCTL formuli.

   Poznámka: Uppaal neumožňuje pojmenování akcí. Typ akci "X"modelujte jako přechod do stavu pojmenovaného "X".

   4 body

1 Úloha 1

1.1 Obsahuje tento automat zeno běh?

Pro důkaz neexistence zeno běhu proiterujeme všechny řídící cykly a v každém najdeme hodiny, které se v daném cyklu resetují a je vyžadován běh času na těchto hodinách pro dokončení cyklu.

- ABCA událost a4 mezi místy B,C resetuje hodiny x a zároveň událost a3 mezi místy C,A vyžaduje tyto hodiny větší jak 1.
- BB událost a5, která je smyčkou nad místem B resetuje hodiny y a zároveň vyžaduje pro provedení y větší jak 10.
- BCB událost a4 mezi místy B,C resetuje hodiny x a zároveň událost a2 mezi místy C,B vyžaduje hodiny X větší jak 1.

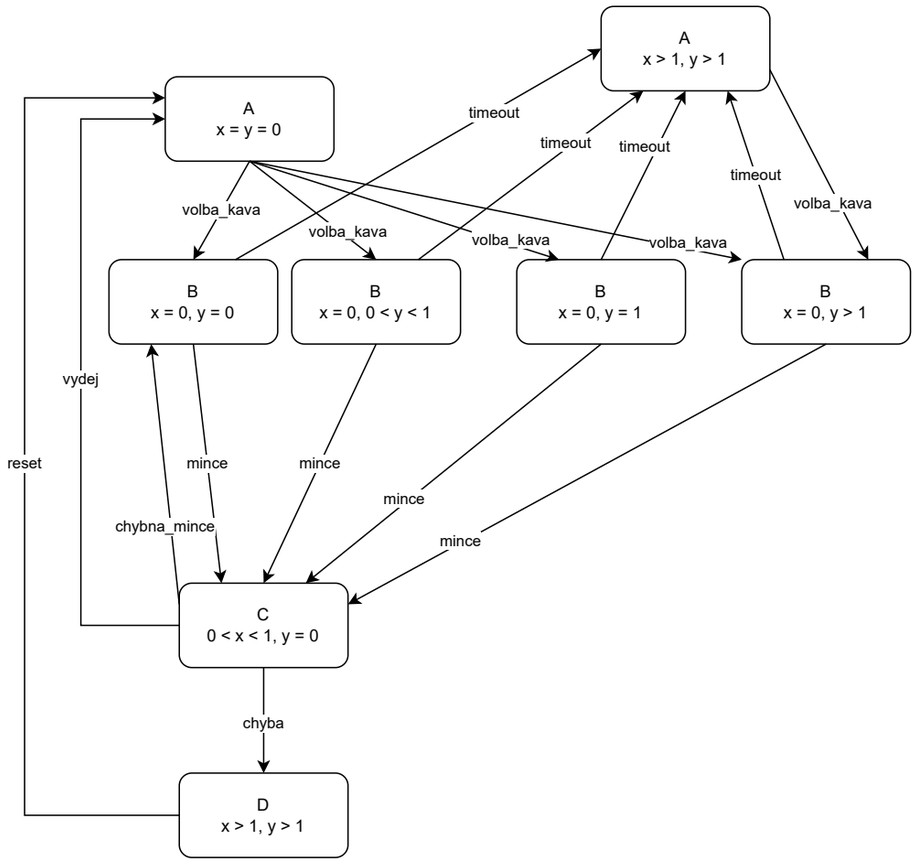
Toto jsou všechny řídící cykly časovaného automatu $\mathcal{A}_1$, takže automat neobsahuje zeno běh.

1.2 Obsahuje tento automat timelock?

Ano, zadaný časovaný automat obsahuje timelock. Uvažujme například běh časovaného automatu: (A, x=0, y=0) $\xrightarrow{0,a1}$ (B, x=0, y=0) $\xrightarrow{0,a4}$ (C, x=0, y=0) $\xrightarrow{2,a3}$ (A, x=2, y=0). Jelikož je hodnota hodin x větší než jedna, tak se jediný přechod a1 ze stavu A stává neproveditelný.

2 Analýza časovaného automatu $\mathcal{A}_2$

2.1 Abstrakce založená na regionech



Obrázek 1: Abstrakce založená na regionech

2.2 Analýza dostupnosti stavu, ve kterém platí predikát error

Ano, stav s predikátem error je dostupný v zadaném časovaném automatu. Uvažme například následující běh: (A, x=0, y=0) $\xrightarrow{0,volba\_kava}$ (B, x=0, y=0) $\xrightarrow{0.5,mince}$ (C, x=0.5, y=0) $\xrightarrow{1.5,chyba}$ (D, x=2, y=1.5). Vidíme, že stav D, kterému je přiřazen predikát error je dostupný.

2.3 Analýza tvrzení $\mathcal{A}_2 \models (run\, U^{(3,4)}\, error)$

Ano, existuje běh, kde se mezi třemi až čtyřmi časovými jednotkami dostaneme ze stavu označeného predikátem run do stavu označeného predikátem error. Uvažme například následující běh: (A, x=0, y=0) $\xrightarrow{0,volba\_kava}$ (B, x=0, y=0) $\xrightarrow{0.5,mince}$ (C, x=0.5, y=0) $\xrightarrow{3,chyba}$ (D, x=3.5, y=3). Jak je vidět celou dobu jsme ve stavech s predikátem run a následně v čase 3.5 přecházíme do stavu R označeného predikátem error.

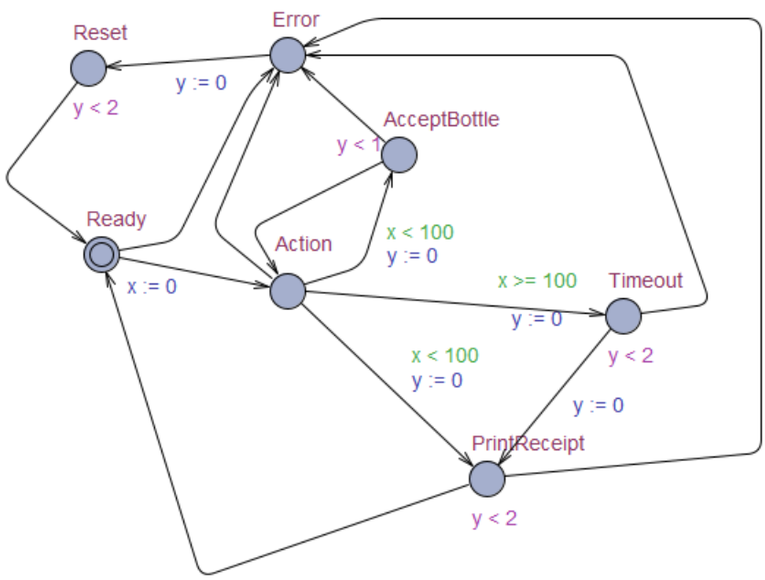
2.4 Analýza tvrzení $(B, x = 3, y = 0.5) \models \forall(true\, U^{<2}\, init)$

Dle mého názoru tvrzení neplatí. Tvrzení říká, že do dvou časových jednotek systém vždy přejde do stavu s labelem init. Nicméně, jelikož stav B neobsahuje žádný invariant, který by omezoval hodiny x, tak dle mého můžeme provést následující přechod: (B, x=3, y=0.5) $\xrightarrow{3,timeout}$ (A, x=6, y=3.5), což nesplňuje, že do dvou časových jednotek se dostaneme do stavu ohodnoceného labelem init.

2.5 Analýza tvrzení $\mathcal{A}_2 \models \exists \diamond (error \wedge x = 2)$

Ano, tvrzení platí. Uvažme například následující běh automatu: (A, x=0, y=0) $\xrightarrow{0,volba\_kava}$ (B, x=0, y=0) $\xrightarrow{0.5,mince}$ (C, x=0.5, y=0) $\xrightarrow{1.5,chyba}$ (D, x=2, y=1.5). Vidíme, že jsme se dostali do stavu D, který je označen predikátem error a hodiny x jsou na hodnotě 2.

3 Automat na vracení lahví modelovaný časovaným automatem



Obrázek 2: Časovaný automat modelující proces vracení lahví