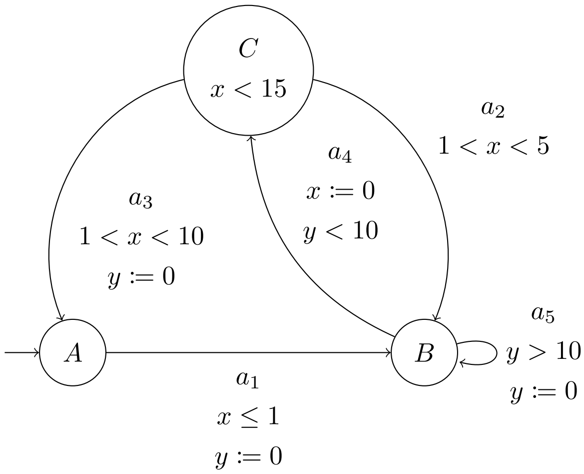
Analýza systémů založená na modelech (MBA) – 2022/2023
Domácí úloha 2

Domink Nejedlý (xnejed09)

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



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

- Automat $\mathcal{A}_1$ neobsahuje zenoběh.

  Důkaz. Využijme podmínku neexistence zeno běhů. Nalezněme a prověřme tedy všechny řídící cykly – cykly bez opakujících se hran i stavů (opakující se stav signalizuje, že cyklus v sobě obsahuje podcyklus, přičemž i ten dle podmínky neexistence zeno běhů musí obsahovat nějaké hodiny, které jsou resetovány a současně alespoň jeden krok tohoto podcyklu vyžaduje jejich běh času):

  - $A \to B \to C \to A$ – hodiny x jsou resetovány a je zde podmínka $1 < x < 10$ (tento cyklus může navíc proběhnout pouze jednou – po návratu do A již nelze splnit podmínku na hraně a_1),
  - $B \to B$ – hodiny y jsou resetovány a je zde podmínka $y > 10$,
  - $B \to C \to B$ – hodiny x jsou resetovány a je zde podmínka $1 < x < 5$.

  Podmínka neexistence zeno běhů je zřejmě pro časovaný automat $\mathcal{A}_2$ splněna – každý řídící cyklus vyžaduje alespoň v jednom kroku běh času hodin (zajišťuje vždy zmíněná podmínka např. $x > 1$ pro hodiny x), jež jsou v tomto cyklu resetovány. Z toho důvodu časovaný automat $\mathcal{A}_2$ neumožňuje zeno běhy. $\square$

- Automat $\mathcal{A}_1$ obsahuje timelock.

  Důkaz. Uvažujme běh:

  $$(A, x = 0, y = 0) \xrightarrow{a_1} (B, x = 0, y = 0) \xrightarrow{a_4} (C, x = 0, y = 0) \xrightarrow{10} (C, x = 10, y = 10)$$

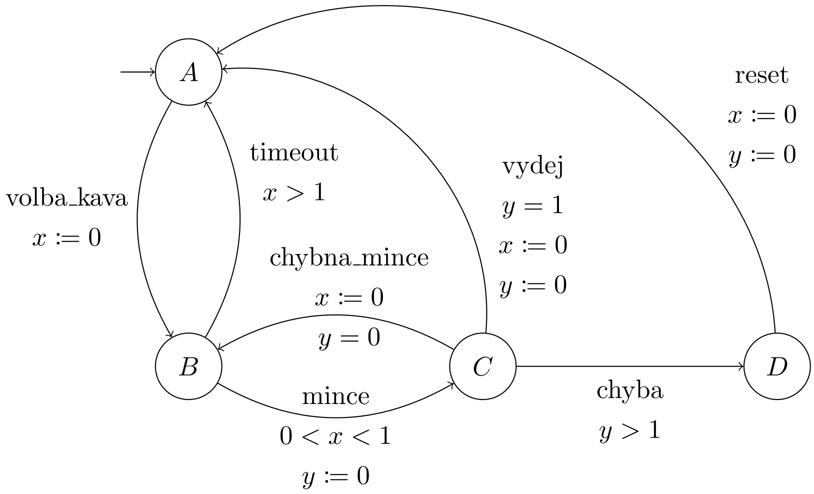
  Konfigurace $c = (C, x = 10, y = 10)$ je timelock, jelikož $\mathit{Paths}_{div}(c) = \emptyset$. Z této konfigurace již nelze provést žádný diskrétní krok, neboť přechod do místa B podmiňuje predikát $1 < x < 5$ a přechod do místa A zase predikát $1 < x < 10$. Ani jeden z těchto predikátů však nemůže být splněn, jelikož $x = 10$. Z konfigurace c lze tedy provádět pouze nekonečné množství časových kroků. Ty však konvergují k číslu 15, protože místo C obsahuje invariant $x < 15$. Z konfigurace c tedy nelze provést žádný časově divergentní běh. $\square$

Příklad 2. Uvažujme časovaný automat $\mathcal{A}_2$ na obrázku 2 s množinou atomických predikátů

$$AP = \{\mathit{init}, \mathit{error}, \mathit{run}\}$$

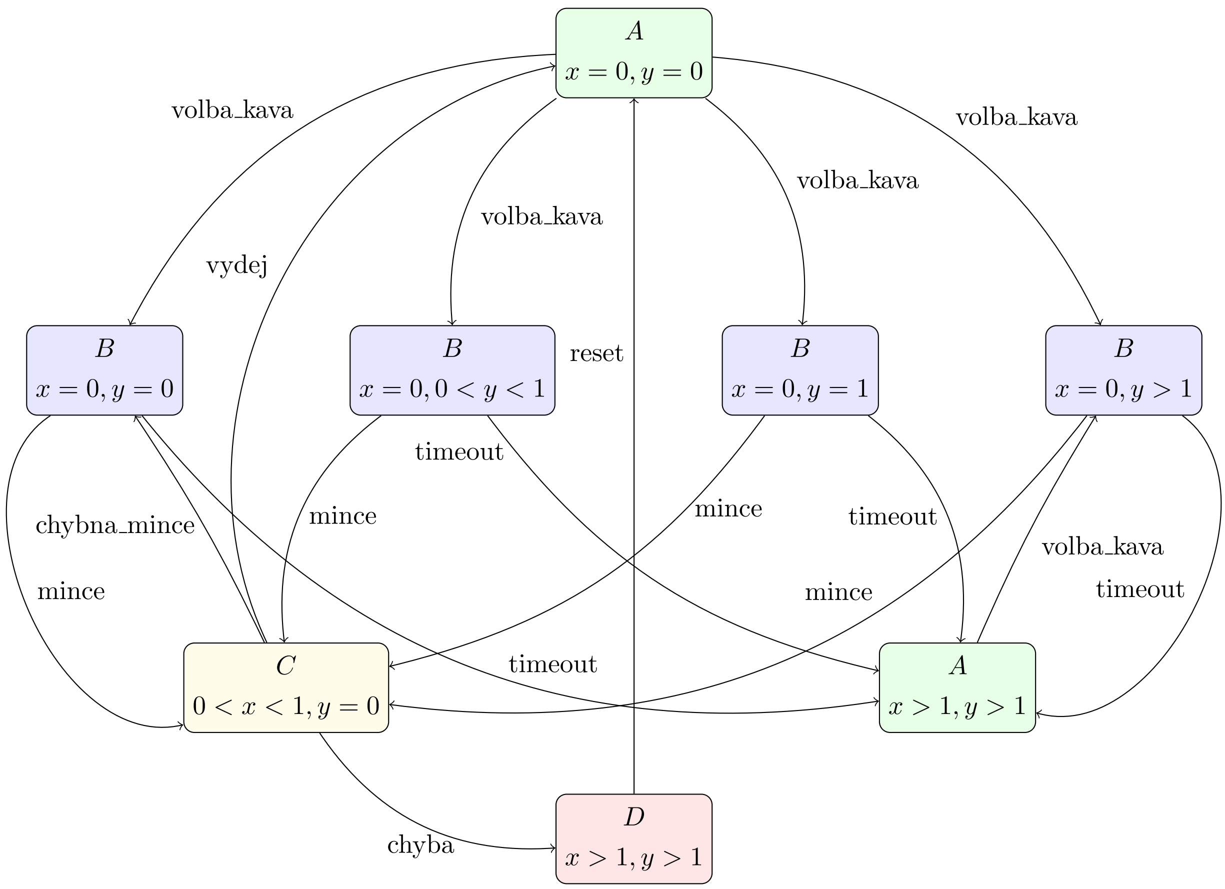
a funkcí L definovanou následovně:

$$\begin{aligned} L(A) &= \{init, run\}, \\ L(D) &= \{error\}, \\ L(B) = L(C) &= \{run\}. \end{aligned}$$



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

- Abstrakce založená na regionech (obrázek 3):



Obrázek 3: Abstrakce založená na regionech časovaného automatu $\mathcal{A}_2$

- Stav, ve kterém platí predikát *error*, je dostupný.

  Důkaz. Existuje totiž např. běh:

  $$(A, x = 0, y = 0) \xrightarrow{\text{volba\_kava}} (B, x = 0, y = 0) \xrightarrow{0.5,\text{mince}} (C, x = 0.5, y = 0) \xrightarrow{1.5,\text{chyba}} (D, x = 2, y = 1.5),$$

  kde $A \in \mathit{Loc}_0$ je počáteční stav a $\mathit{error} \in L(D)$. Dostupnost lze také vidět přímo v regionové abstrakci. $\square$

- Tvrzení $\mathcal{A}_2 \models \exists(\mathit{run}\, U^{(3,4)}\, \mathit{error})$ platí.

  Důkaz. Nechť $\phi \equiv \mathit{run}\, U^{(3,4)}\, \mathit{error}$ a $\tau \in \mathbb{R}^+$. Zřejmě $\mathit{Init}_{\mathcal{A}_2} = \{c_0 = (A, x = 0, y = 0)\}$. Uvažujme časově divergentní cestu

  $$\pi = (A, x = 0, y = 0) \xrightarrow{\text{volba\_kava}} (B, x = 0, y = 0) \xrightarrow{0.4,\text{mince}} (C, x = 0.4, y = 0) \xrightarrow{3.1,\text{chyba}} (D, x = 3.5, y = 3.1)$$
  $$\xrightarrow{\tau} (D, x = 3.5 + \tau, y = 3.1 + \tau) \xrightarrow{\tau} \cdots \in \mathit{Paths}_{\mathit{div}}(c_0).$$

  Jistě platí, že $\pi \models \phi$, neboť existuje časový okamžik $t = 0.4 + 3.1 = 3.5$ z intervalu $(3, 4)$ ($t \in (3, 4)$), ve kterém platí formule *error* ($\mathit{error} \in L(D)$) a pro libovolný časový okamžik menší než t platí formule $\mathit{run} \vee \mathit{error}$. Zřejmě tedy také platí, že $c_0 \models \exists\phi$ (existuje cesta $\pi \in \mathit{Paths}_{\mathit{div}}(c_0)$, pro kterou platí, že $\pi \models \phi$) a $\mathit{Init}_{\mathcal{A}_2} \subseteq \mathit{Sat}(\exists\phi)$. Z toho důvodu časovaný automat $\mathcal{A}_2$ splňuje formuli $\exists(\mathit{run}\, U^{(3,4)}\, \mathit{error})$ (tj. $\mathcal{A}_2 \models \exists\phi$). $\square$

- Tvrzení $(B, x = 3, y = 0.5) \models \forall(\mathit{true}\, U^{<2}\, \mathit{init})$ neplatí.

  Důkaz. Nechť $\phi \equiv \mathit{true}\, U^{<2}\, \mathit{init}$, $c_0 = (B, x = 3, y = 0.5)$ a $\tau \in \mathbb{R}^+$. Uvažujme časově divergentní cestu

  $$\pi = (B, x = 3, y = 0.5) \xrightarrow{3} (B, x = 6, y = 3.5) \xrightarrow{\tau} (B, x = 6 + \tau, y = 3.5 + \tau) \xrightarrow{\tau} \cdots \in \mathit{Paths}_{\mathit{div}}(c_0).$$

  Tvrzení $\pi \models \phi$ zřejmě neplatí, neboť neexistuje žádný časový okamžik t z intervalu $\langle 0, 2)$, ve kterém by platila formule *init*. Z toho důvodu nemůže platit ani tvrzení $c_0 \models \forall\phi$ (tj. $(B, x = 3, y = 0.5) \models \forall(\mathit{true}\, U^{<2}\, \mathit{init})$), jelikož to vyžaduje, aby pro každou cestu $\pi' \in \mathit{Paths}_{\mathit{div}}(c_0)$ tvrzení $\pi' \models \phi$ platilo. $\square$

- Tvrzení $\mathcal{A}_2 \models \exists \diamond (\mathit{error} \wedge x = 2)$ platí.

  Důkaz. Nechť $\phi \equiv \diamond(\mathit{error} \wedge x = 2)$ a $\tau \in \mathbb{R}^+$. Zřejmě $\mathit{Init}_{\mathcal{A}_2} = \{c_0 = (A, x = 0, y = 0)\}$. Uvažujme časově divergentní cestu

  $$\pi = (A, x = 0, y = 0) \xrightarrow{\text{volba\_kava}} (B, x = 0, y = 0) \xrightarrow{0.5,\text{mince}} (C, x = 0.5, y = 0) \xrightarrow{1.5,\text{chyba}} (D, x = 2, y = 1.5)$$
  $$\xrightarrow{\tau} (D, x = 2 + \tau, y = 1.5 + \tau) \xrightarrow{\tau} \cdots \in \mathit{Paths}_{\mathit{div}}(c_0).$$

  Jistě platí, že $\pi \models \phi$, neboť existuje časový okamžik $t = 0.5 + 1.5 = 2 \in \langle 0, \infty)$, ve kterém platí formule $\mathit{error} \wedge x = 2$. Zřejmě tedy též platí, že $c_0 \models \exists\phi$ (existuje cesta $\pi \in \mathit{Paths}_{\mathit{div}}(c_0)$, pro kterou platí, že $\pi \models \phi$) a $\mathit{Init}_{\mathcal{A}_2} \subseteq \mathit{Sat}(\exists\phi)$. Z toho důvodu časovaný automat $\mathcal{A}_2$ splňuje formuli $\exists \diamond (\mathit{error} \wedge x = 2)$ (tj. $\mathcal{A}_2 \models \exists\phi$). $\square$