Petriho sítě

Poznámka autora

Tento materiál vznikl podle kurzu *Petriho sítě* vyučovaného doc. RNDr. Antonínem Kučerou, Ph.D. v podzimním semestru 2003 na Fakultě informatiky Masarykovy univerzity v Brně. Zdrojem byly především zápisky z přednášek mne a Pavla Šimečka. Na některých místech byly použity materiály poskytnuté Tomášem Kratochvílou.

Protože měl tento materiál sloužit k mé přípravě na zkoušku, dělal jsem vše pro to, aby neobsahoval chyby a nepřesnosti. To však neznamená, že je obsahovat nemůže — nenesu žádnou odpovědnost za škody vzniklé použitím tohoto textu.

Upozornění na chyby, překlepy, špatné formulace, náměty a připomínky, jakož i ocenění, poděkování nebo dotazy na číslo mého účtu pro konkrétnější ocenění můžete poslat na

`holecek [at] informatics.muni.cz`

Honza Holeček
8. 3. 2004

Obsah

Seznam obrázků

Základní pojmy

Motivací pro vznik Petriho sítí bylo modelovat řídící systémy. Neformálně je Petriho síť graf se dvěma typy uzlů (místy a přechody) s násobnými hranami. Hrany jsou přitom pouze mezi uzly různých typů. Obecně žádná další omezení nejsou, zejména tedy nemusí být vyváženy vstupní a výstupní stupně uzlů.

Definice (Petriho síť)
Petriho síť je trojice $\mathcal{N} = (P, T, F)$, kde $P \neq \emptyset$ je konečná množina míst (*places*), $T \neq \emptyset$ je konečná množina přechodů (*transitions*) a F je přechodová funkce (*float*)

$$F : (P \times T) \cup (T \times P) \to \mathbb{N}_0$$

Poznámka (Neprázdnost množin míst a přechodů Petriho sítě)
Zde jsem se dopustil největší odchylky od poznámek z přednášek, kde toto omezení na Petriho sítě nebylo kladeno. Všechny „zajímavé“ sítě jej však jistě splňují. Toto omezení je nutné při analýze free-choice systémů a zavést jej přímo v hlavní definici mi připadalo nejrozumnější. Platnost ostatních tvrzení tím jistě nebude ovlivněna — jedná se o striktní omezení množiny petriho sítí.

Notace (Množiny uzlů, které „berou“ a „dávají“ do uzlu Petriho sítě)
Nechť $\mathcal{N} = (P, T, F)$ je Petriho síť. Pro každý přechod $t \in T$ a pro každé místo $p \in P$ definujeme množiny

$$\begin{aligned} t^\bullet &= \{p \in P \mid F(t,p) > 0\} \\ {}^\bullet t &= \{p \in P \mid F(p,t) > 0\} \\ p^\bullet &= \{t \in T \mid F(p,t) > 0\} \\ {}^\bullet p &= \{t \in T \mid F(t,p) > 0\} \end{aligned}$$

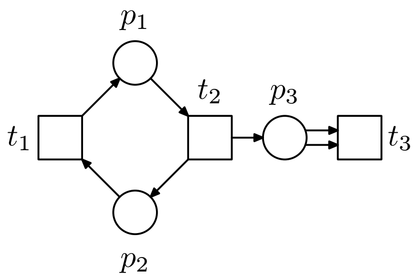
Notace se přirozeně rozšiřuje na množiny přechodů a míst.

Pro místo $p \in P$ je $p^\bullet$ neformálně množina přechodů, z nichž místo může získat token, a ${}^\bullet p$ množina přechodů, do nichž může token odevzdat (viz níže).

Příklad (Jednoduchá Petriho síť)
Na následujícím obrázku je příklad jednoduché sítě, kde

$$\begin{aligned} P &= \{p_1, p_2, p_3\} \\ T &= \{t_1, t_2, t_3\} \\ F &= \{(p_1, t_1, 1), (p_3, t_3, 2), (t_3, p_1, 0, \ldots)\} \end{aligned}$$

$$\begin{aligned} F(p_1, t_2) &= 1 \\ F(p_3, t_3) &= 2 \\ F(t_3, p_1) &= 0 \\ \{p_1, p_2\}^\bullet &= \{t_1, t_2\} \end{aligned}$$



Definice (Označkování, uschopněný přechod)
Nechť $\mathcal{N} = (P, T, F)$ je Petriho síť. *Označkování* (*marking*) je funkce $M : P \to \mathbb{N}_0$. Přechod $t \in T$ je *uschopněn* v M, pokud

$$\forall p \in t^{\bullet} : M(p) \geq F(p, t)$$

Neformálně lze označkování chápat jako distribuci tokenů v síti: udává počet tokenů v jednotlivých místech.

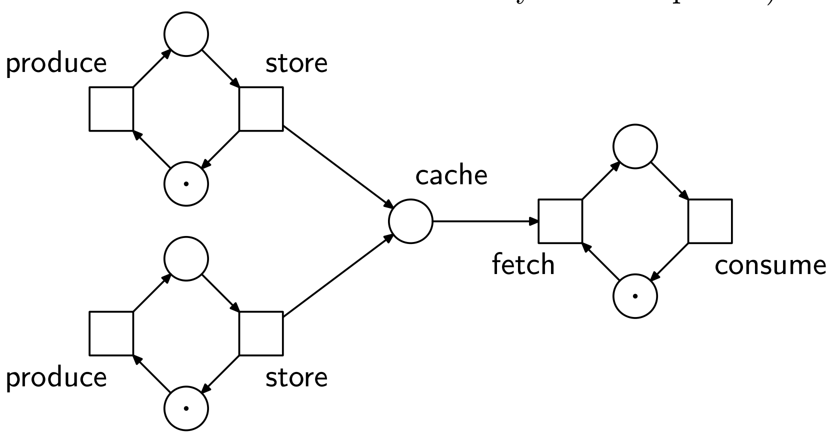
Poznámka (Vyjadřovací síla Petriho sítí)
V definici uschopněného přechodu je klíčové použití relace $\geq$ místo $=$. Při použití rovnosti by Petriho sítě byly stejně silné jako Turingovy stroje a mnoho vlastností sítí by bylo nerozhodnutelných. Cílem je přitom umožnit efektivní verifikaci dostatečně velké třídy systémů — s rovností by třída byla příliš velká.

Definice (Přechodový systém Petriho sítě)
Nechť $\mathcal{N} = (P, T, F)$ je Petriho síť a $\mathcal{A}$ je množina návěští (abeceda). Nechť je dána funkce $l : T \to \mathcal{A}$ přiřazující přechodům ne nutně vzájemně různá návěští. *Přechodový systém s návěštími* pro Petriho síť $\mathcal{N}$ s olabelováním l definujeme jako $\mathcal{T}_{\mathcal{N}} = (S, \mathcal{A}, \to)$,

kde S je množina všech označkování, $\to \subseteq S \times \mathcal{A} \times S$ a $M \xrightarrow{a} M'$ právě tehdy, když existuje přechod $t \in T$ uschopněný v M takový, že $l(t) = a$ a

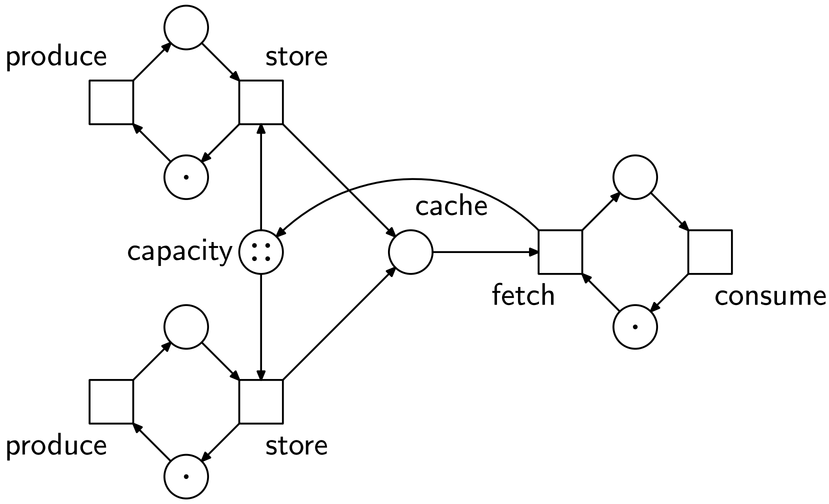
$$\forall p \in P : M'(p) = M(p) - F(p, t) + F(t, p)$$

Příklad (Producent-konzument s neohraničenou vyrovnávací pamětí)



Význam tokenů je verzatilní. Zatímco v místě cache tokeny reprezentují výpočetní zdroje (data), tokeny v ostatních místech udávají tok řízení (uschopňují přechody odpovídající jednotlivým akcím).

Příklad (Producent-konzument s ohraničenou vyrovnávací pamětí)

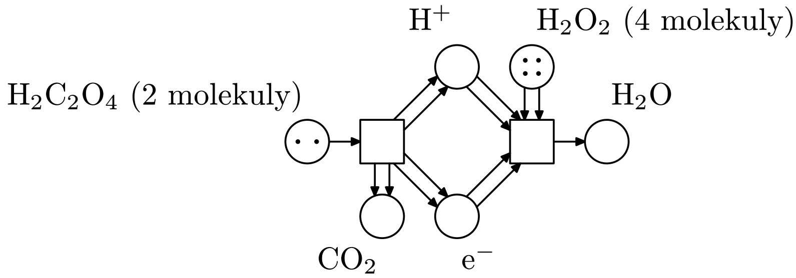


Počet tokenů v místě capacity udává velikost volné vyrovnávací paměti. Přechody store mohou být odpáleny (provedeny) jen tehdy, pokud je v místě capacity alespoň jeden token — v paměti je místo pro uložení. Přechod fetch vybírá data z paměti, takže přidává jeden token do místa capacity. Iniciální počet tokenů v místě capacity udává velikost vyrovnávací paměti.

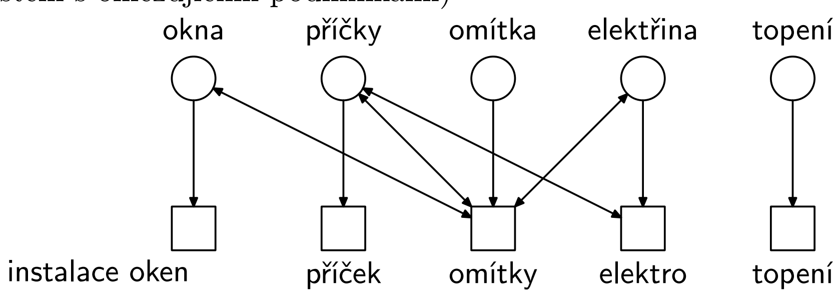
Příklad (Model chemické reakce)
Nechť v systému mohou probíhat následující reakce:

$$H_2C_2O_4 \to 2CO_2 + 2H^+ + 2e^-$$
$$2e^- + 2H^+ + H_2O_2 \to 2H_2O$$

Petriho síť modelující takový systém je na následujícím obrázku. Iniciální marking udává iniciální počet jednotlivých molekul v systému. Jedna reakce je reprezentována jedním přechodem.



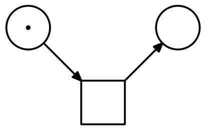
Příklad (Systém s omezujícími podmínkami)



Petriho síť z předchzího obrázku popisuje závislosti mezi jednotlivými pracemi při stavbě domu. Platí-li pro přechod t a místo p vztah $F(p, t) = F(t, p) = 1$, místo p tvoří *omezující podmínku* pro přechod t — odpálení přechodu t nezmění distribuci tokenů v místě p, ale vyžaduje přítomnost alespoň jednoho. V některých případech se hovoří o *run-place* hranách.

Ve větším systému je možné analyzovat, zda je projekt realizovatelný (dosažitelnost koncového markingu z iniciálního), které části jsou kritické apod. V tomto případě není nutná ani dosažitelnost (umožňuje specifikovat přesný počet tokenů v daném místě), ale stačí pokrytelnost — v každém místě musí být alespoň nějaký počet tokenů (zde jeden token).

Model lze navíc modifikovat tak, aby v každém místě mohl být nejvýše jeden token. Modifikace je analogická omezení vyrovnávací paměti v modelu producent-konzument.



Analýza Petriho sítí

Základní problémy řešené u všech formálních modelů jsou dosažitelnost, ukončení a živost. Aby byl model efektivně analyzovatelný, musí být tyto vlastnosti rozhodnutelné. Dalším stupněm je rozhodnutelnost obecnějších temporálních vlastností (formulí temporální logiky) a nejvyšším stupněm je plná formální verifikace (ověření ekvivalence vůči dané specifikaci).

Definice (Dosažitelné označkování)
Označkování M' je *dosažitelné* z M v Petriho síti $\mathcal{N} = (P, T, F)$, jestliže je v přechodovém systému indukovaném sítí $\mathcal{N}$ stav M' dosažitelný z M.

Notace (Množina dosažitelných označkování)
Pro Petriho síť $\mathcal{N}$ a její označkování M definujeme funkci

$$\text{Reach}(\mathcal{N}, M) = \{\text{označkování } M' \text{ sítě } \mathcal{N} \mid M' \text{ je dosažitelné z } M\}$$

Definice (Živost přechodu, živost sítě)
Buď $\mathcal{N} = (P, T, F)$ Petriho síť, M_0 její označkování. Přechod $t \in T$ je *živý* pro M_0, jestliže pro každé M dosažitelné z M_0 existuje M' dosažitelné z M tak, že t je uschopněný v M.

Petriho síť nazveme *živou* pro marking M_0, pokud je pro M_0 živý každý její přechod.

Definice (Mrtvé místo, mrtvý přechod)
Nechť $\mathcal{N} = (P, T, F)$ je Petriho síť. *Místo* $p \in P$ se nazývá *mrtvé* v markingu M, pokud pro všechna označkování M' dosažitelná z M platí $M'(s) = 0$. *Přechod* $t \in T$ se nazývá *mrtvý*, není-li připravený v žádném označkování dosažitelném z M.

Definice (Problémy pro Petriho sítě)
Problém dosažitelnosti (reachability)
Instance: Petriho síť $\mathcal{N} = (P, T, F)$ a její označkování M, M'.
Otázka: Je označkování M' dosažitelné z M v $\mathcal{N}$?

Problém sub-marking reachability
Instance: Petriho síť $\mathcal{N} = (P, T, F)$, její označkování M_0 a částečné označkování M.
Otázka: Existuje označkování M' sítě $\mathcal{N}$ dosažitelné z M_0 takové, že kdykoli je pro $p \in P$ definováno $M(p)$, potom $M'(p) = M(p)$?

Problém zero-reachability
Instance: Petriho síť $\mathcal{N} = (P, T, F)$ a její označkování M_0.
Otázka: Je z M_0 dosažitelné nulové označkování sítě $\mathcal{N}$ (síť neobsahuje žádné tokeny)?

Problém single-place zero-reachability
Instance: Petriho síť $\mathcal{N} = (P, T, F)$, její označkování M_0 a místo $p \in P$.
Otázka: Je z M_0 v síti $\mathcal{N}$ dosažitelné označkování M takové, že $M(p) = 0$?

Problém pokrytelnosti
Instance: Petriho síť $\mathcal{N} = (P, T, F)$ a její označkování M, M'
Otázka: Existuje označkování M'' dosažitelné v Petriho síti $\mathcal{N}$ z markingu M takové, že $\forall p \in P : M''(p) \geq M'(p)$?

Problém ohraničenosti místa
Instance: Petriho síť $\mathcal{N} = (P, T, F)$, její označkování M a místo p
Otázka: Existuje $k \in \mathbb{N}_0$ takové, že pro každé označkování M' dosažitelné z M v $\mathcal{N}$ platí $M'(p) \leq k$?

Problém k-ohraničenosti místa
Instance: Petriho síť $\mathcal{N} = (P, T, F)$, její označkování M, místo p a $k \in \mathbb{N}_0$
Otázka: Platí pro každé označkování M' dosažitelné z M v $\mathcal{N}$ nerovnost $M'(p) \leq k$?

Problém ohraničenosti sítě
Instance: Petriho síť $\mathcal{N} = (P, T, F)$ a její označkování M
Otázka: Je každé místo sítě ohraničené? Alternativně (množina míst je konečná): Existuje $k \in \mathbb{N}_0$ tak, že každé místo je k-ohraničené?

Problém k-ohraničenosti sítě
Instance: Petriho síť $\mathcal{N} = (P, T, F)$, její označkování M, $k \in \mathbb{N}_0$
Otázka: Je každé místo sítě k-ohraničené?

Problém inkluze množin dosažitelných označkování
Instance: Petriho sítě $\mathcal{N}_1 = (P, T_1, F_1)$, $\mathcal{N}_2 = (P, T_2, F_2)$ nad stejnou množinou míst a jejich počáteční označkování M_1, M_2.
Otázka: Platí $\mathrm{Reach}(\mathcal{N}_1, M_1) \subseteq \mathrm{Reach}(\mathcal{N}_2, M_2)$?

Problém rovnosti množin dosažitelných označkování
Instance: Petriho sítě $\mathcal{N}_1 = (P, T_1, F_1)$, $\mathcal{N}_2 = (P, T_2, F_2)$ nad stejnou množinou míst a jejich počáteční označkování M_1, M_2.
Otázka: Platí $\mathrm{Reach}(\mathcal{N}_1, M_1) = \mathrm{Reach}(\mathcal{N}_2, M_2)$?

Problém živosti přechodu
Instance: Petriho síť $\mathcal{N} = (P, T, F)$, její označkování M_0 a přechod $t \in T$.
Otázka: Je přechod t živý pro M_0 v $\mathcal{N}$?

Problém živosti sítě
Instance: Petriho síť $\mathcal{N} = (P, T, F)$ a její označkování M_0.
Otázka: Je síť $\mathcal{N}$ živá pro M_0? (Je živý každý její přechod pro M_0?)

Problém uváznutí sítě (mrtvost sítě)
Instance: Petriho síť $\mathcal{N} = (P, T, F)$ a její označkování M_0.
Otázka: Existuje pro $(\mathcal{N}, M_0)$ dosažitelné označkování M takové, že $(\mathcal{N}, M)$ je mrtvá, tj. není připraven žádný přechod?

Strom pokrytelnosti

Definice (Rozšířené označkování)
Rozšířené označkování M Petriho sítě $\mathcal{N} = (P, T, F)$ je funkce $M : P \to \mathbb{N}_0 \cup \{\omega\}$, kde definujeme $\forall a \in \mathbb{N}_0$

$$\begin{aligned} \omega \pm a &= \omega \\ a &< \omega \\ \omega &\leq \omega \end{aligned}$$

Definice (Strom pokrytelnosti)
Strom pokrytelnosti (*coverability tree*, *Karp-Miller tree*) pro danou Petriho síť $\mathcal{N} = (P, T, F)$ a její marking M_0 je strom, který vznikne následující iterativní konstrukcí.

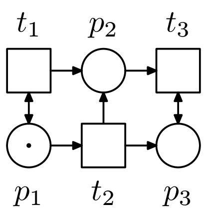
Každý uzel x stromu pokrytelnosti je ohodnocen právě jedním rozšířeným označkováním sítě $\mathcal{N}$. V každém okamžiku konstrukce stromu pokrytelnosti má každý uzel právě jeden z následujících módů: hraniční, duplikovaný, vnitřní, koncový. Konstrukce končí, pokud ve stromě nejsou již žádné hraniční uzly.

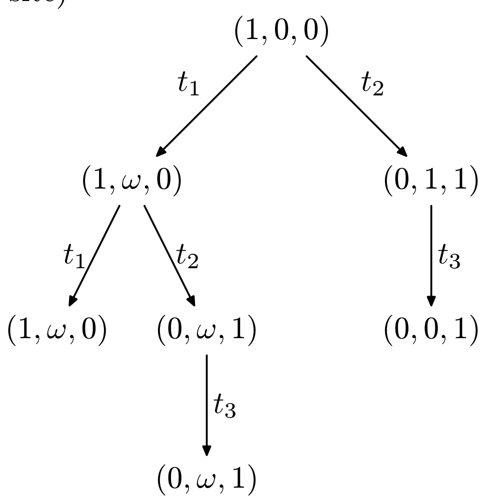
vytvoř hraniční uzel ohodnocený markingem M_0.
while existuje hraniční uzel x **do**
  if existuje nehraniční uzel y takový, že $M_x = M_y$ **then**
    x se stává duplikovaným
  elseif v M_x nejsou uschopněny žádné přechody **then**
    x se stává koncovým
  else

forall přechod t uschopněný v M_x **do**
přidej nový hraniční uzel z jako následníka uzlu x
uzlu z přiřaď marking M_z definovaný následovně:
forall $p \in P$ **do**
if $M_x(p) = \omega$ **then**
$M_z(p) = \omega$
elseif
na cestě z kořene do x existuje uzel y tak, že
$\forall q \in P : M_y(q) \leq M_x(q) - F(q,t) + F(t,q)$ a
$M_y(p) < M_x(p) - F(p,t) + F(t,p)$
then
$M_z(p) = \omega$
else
$M_z(p) = M_x(p) - F(p,t) + F(t,p)$
fi
done
x se stává vnitřním
done
fi
done

Poznámka (Rozhodnutelnost problému pokrytelnosti)
Strom pokrytelnosti umožňuje rozhodovat pokrytelnost a ohraničenost sítě. Neumožňuje však rozhodovat dosažitelnost.

Příklad (Strom pokrytelnosti Petriho sítě)





Lemma (Nekonečná neklesající podposloupnost)
Z libovolné nekonečné posloupnosti $s = s_1, s_2, \ldots$ prvků z $\mathbb{N}_0 \cup \{\omega\}$ lze vybrat nekonečnou neklesající podposloupnost.

Důkaz: Pokud posloupnost obsahuje nekonečnou podposloupnost prvků ω, pak je to podposloupnost hledaných vlastností. V opačném případě po vynechání všech prvků ω dostaneme nekonečnou posloupnost přirozených čísel s nulou. Je-li tato neohraničená, pak obsahuje nekonečnou ostře rostoucí podposloupnost, kterou lze vybrat i z původní posloupnosti. Je-li ohraničená, pak obsahuje nějaké přirozené číslo nekonečněkrát a nekonečná podposloupnost tvořená tímto číslem je podposloupnost hledaných vlastností.

Lemma (Dicksonovo lemma, Dickson's Lemma)
Z libovolné nekonečné posloupnosti prvků z $(\mathbb{N}_0 \cup \{\omega\})^k$, $k \in \mathbb{N}$, lze vybrat nekonečnou (po složkách) neklesající podposloupnost.

Důkaz: Indukcí vzhledem ke k. Pro $k = 1$ dle předchozího lemmatu. Nechť tvrzení platí pro k, uvažujme případ pro $k+1$. Podle předchozího lemmatu lze vybrat nekonečnou neklesající podposloupnost podle složky $k+1$. Nekonečnou neklesající podposloupnost $(k+1)$-tic z ní můžeme vybrat podle indukčního předpokladu, uvažujeme-li pouze prvních k složek.

Věta (Ukončení konstrukce stromu pokrytelnosti)
Algoritmus konstrukce stromu pokrytelnosti vytvoří konečný strom.

Důkaz: Protože počet přechodů Petriho sítě je z definice konečný, obsahuje strom pokrytelnosti vždy jen konečné větvení. Pokud by měl být nekonečný, musel by obsahovat nekonečnou větev. Podle důkazu Dicksonova lemmatu však tato větev musí obsahovat buď opakující se uzly nebo ostře rostoucí podposloupnost. V prvním případě bude opakující se uzel označen jako duplicitní, v druhém případě vznikne ω. V obou případech dojde k ukončení větve.

Obarvíme-li v klice $\mathcal{K}$ každou hranu náhodně jednou ze dvou barev, vznikne monochromatická klika $\mathcal{K}$.

Definice (Ramseova funkce)
Funkce $\mathbf{R} : \mathbb{N} \to \mathbb{N}$, kde $\mathbf{R}(m) = k$, se nazývá Ramseova, jestliže při náhodném obarvení hran dvěma barvami v $\mathcal{K}_\mathrm{k}$ vznikne monochromatická klika $\mathcal{K}_\mathrm{m}$.

Věta (Ramseova věta)
Ramseova funkce je definována pro každé $m \in \mathbb{N}$. Existuje limita Ramseovy funkce pro $m \to \infty$.

Důkaz: Není snadný a patří do kombinatoriky.

Definice (Hilbert-Ackermannova funkce)
Pro každé $i \in \mathbb{N}_0$ definujme induktivně funkci $A_i : \mathbb{N}_0 \to \mathbb{N}_0$

$$\begin{aligned} A_0(x) &= 2x + 1 \\ A_{i+1}(0) &= 1 \\ A_{i+1}(x+1) &= A_i(A_{i+1}(x)) = \underbrace{A_i \circ \cdots \circ A_i}_{x\text{-krát}}(1) \end{aligned}$$

Funkce A_i je primitivně rekurzivní pro každé $i \in \mathbb{N}_0$, ale počet for-cyklů potřebných pro její výpočet roste s i. Funkce

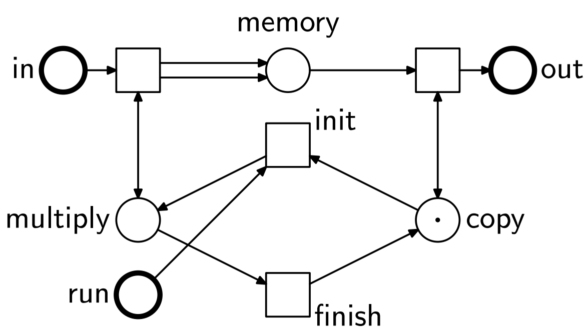
$$\mathbf{A}(x) = A_x(2)$$

tedy není primitivně rekurzivní. Důkaz patří do vyčíslitelnosti.

Věta (Velikost stromu pokrytelnosti)
Velikost stromu pokrytelnosti Petriho sítě nelze ohraničit žádnou primitivně rekurzivní funkcí.

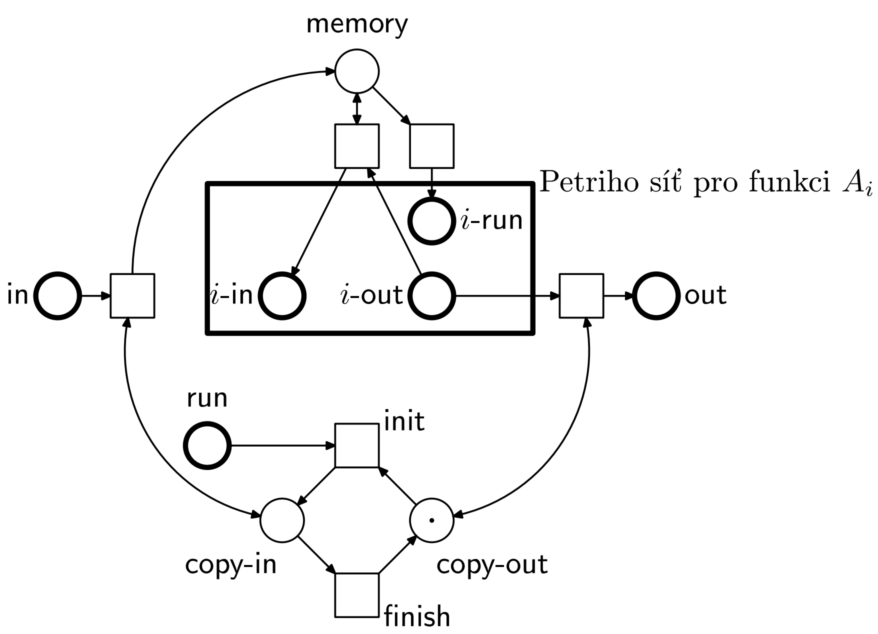
Důkaz: Pro každé $i \in \mathbb{N}_0$ sestrojíme Petriho síť a její označkování velikosti $\mathbf{O}(n)$ tak, aby síť počítala Hilbert-Ackermannovu funkci A_i. Petriho sítě definujeme induktivně tak, že každá bude obsahovat místa in, out a run. Vložíme-li m tokenů do in a jeden token do run, bude existovat takový běh sítě, který skončí s $A_i(m)$ tokeny v out.

Síť pro A_0



Na počátku lze odpálit pouze přechod init, čímž se řídící token dostane do místa multiply, a do paměti memory se vloží jeden token, což odpovídá přičtení jedničky. Dokud zůstává řídící token v multiply, je možné násobením dvěma přesouvat tokeny z in do memory. Jakmile se provede přechod finish, token se do multiply už nemůže nevrátit, protože místo run je již prázdné. Řídící token zůstává v místě copy a přesunuje (kopíruje) tokeny z memory do out.

Síť pro A_{i+1}



Vložíme-li m tokenů do in a jeden token do run, výpočet, jehož výsledkem bude $A_{i+1}(m)$ tokenů v out, bude probíhat následovně. Nejprve se odpálí přechod init, čímž se do i-out vloží jeden token (argument m složených funkcí A_i). Řídící token potom zůstane v copy-in, dokud se nepřemístí všechny tokeny z in do memory.

Nyní se m-krát spustí síť pro A_i. Dokud je v memory alespoň jeden token, mohou se přemístit tokeny z i-out do i-in. Potom se vloží jeden token do i-run a nechá se počítat síť pro A_i tak, aby po skončení jejího výpočtu v i-out bylo $A_i(x)$ tokenů, kde x byl počáteční počet tokenů v i-in. Dokud jsou v memory tokeny, postup se opakuje.

Nakonec se odpálí přechod finish, čímž se řídící token dostane do copy-out. To umožní přemístit všechny tokeny z i-out do out.

Pro velikost sítí (velikost grafů a velikost markingů) se vstupem m platí

$$
\begin{aligned}
|\mathcal{N}_{A_0}| &= c + \mathbf{O}(m) \\
|\mathcal{N}_{A_{i+1}}| &= k \;\; + |\mathcal{N}_{A_i}| \\
|\mathcal{N}_{A_i}| &= \mathbf{O}(i+m)
\end{aligned}
$$

Protože je síť ohraničená, při konstrukci stromu pokrytelnosti nevznikne ω a je tedy totožný se stromem dosažitelnosti. Do out se navíc tokeny přemísťují po jednom, takže pro síť $\mathcal{N}_{A_i}$ existuje alespoň $A_i(m)$ markingů dosažitelných z počátečního markingu s m tokeny v in. Velikost stromu pokrytelnosti sítě $\mathcal{N}_{A_i}$ je tedy zdola ohraničena funkcí $\mathbf{A}(i)$, tedy je rovna $\Omega(\mathbf{A}(i+m))$. Protože $\mathbf{A}(x)$ není primitivně rekurzívní, nelze velikost stromu pokrytelnosti ohraničit žádnou primitivně rekurzívní funkcí.

Hierarchie problémů vzhledem k redukci

Věta (Polynomiální ekvivalence reachability problémů)
Reachability, zero-reachability, single-place zero-reachability a sub-marking reachability problémy jsou polynomiálně ekvivalentní.

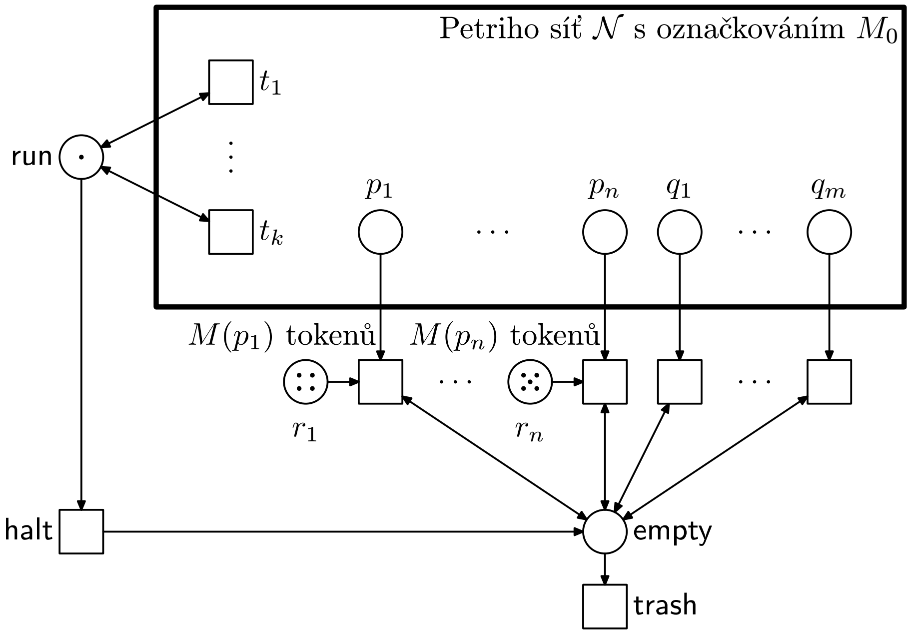
Důkaz: Ukážeme následující redukce:

$$
\begin{aligned}
\text{single-place zero-reachability redukujeme na sub-marking reachability} \quad &(1) \\
\text{sub-marking reachability redukujeme na zero-reachability} \quad &(2) \\
\text{zero-reachability redukujeme na reachability} \quad &(3) \\
\text{reachability redukujeme na sub-marking reachability} \quad &(4) \\
\text{zero-reachability redukujeme na single-place zero-reachability} \quad &(5)
\end{aligned}
$$

Vzniknou tedy následující cykly redukcí: (1) $\rightarrow$ (2) $\rightarrow$ (5) a (2) $\rightarrow$ (3) $\rightarrow$ (4).

Redukce single-place zero-reachability na sub-marking reachability Problém single-place zero-reachability je speciálním případem sub-marking-reachability, redukce je triviální.

Redukce sub-marking reachability na zero-reachability Mějme instanci problému sub-marking reachability, tedy Petriho síť $\mathcal{N}$, její počáteční označkování M_0 a částečné označkování M. Označme $p_1, \ldots, p_n$ místa, na nichž je M definováno, a $q_1, \ldots, q_m$ místa ostatní. Dále označme $t_1, \ldots, t_k$ všechny přechody $\mathcal{N}$. Vytvoříme síť $\mathcal{N}'$ a její počáteční označkování M'_0 (instanci problému zero-reachability) následovně:



Dokud je řídící token v run, provádí síť $\mathcal{N}'$ výpočet sítě $\mathcal{N}$. V určitém okamžiku se $\mathcal{N}'$ nedeterministicky rozhodne provést přechod halt a ověří se shoda označkování sítě $\mathcal{N}$ se sub-markingem M. Nakonec se řídící token zahodí přechodem trash a výpočet končí. Nulový marking je v $\mathcal{N}'$ dosažitelný právě tehdy, pokud je v síti $\mathcal{N}$ dosažitelný sub-marking M. Jinak by nutně zůstaly tokeny buď v r_i nebo p_i podle toho, kde by jich bylo více v okamžiku provedení halt.

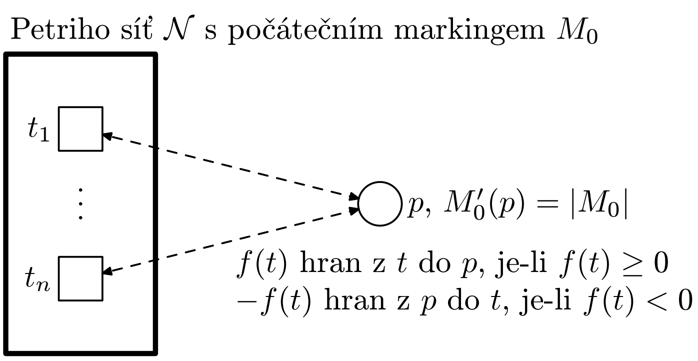
Redukce zero-reachability na reachability Problém zero-reachability je speciálním případem reachability, redukce je triviální.

Redukce reachability na sub-marking reachability Problém reachability je speciálním případem sub-marking reachability, redukce je triviální.

Redukce zero-reachability na single-place zero-reachability Mějme instanci problému zero-reachability, tedy Petriho síť $\mathcal{N} = (P, T, F)$ a její označkování M_0. Nechť $T = \{t_1, \ldots, t_n\}$. Definujme dále funkci $f : T \to \mathbb{N}_0$ předpisem

$$f(t) = \sum_{p \in P} \big(F(t,p) - F(p,t)\big)$$

Funkce f udává efekt přechodu na celkový počet tokenů v síti. Instanci problému single-place zero-reachability $\mathcal{N}'$, M'_0, p, $p \notin P$ vytvoříme takto:

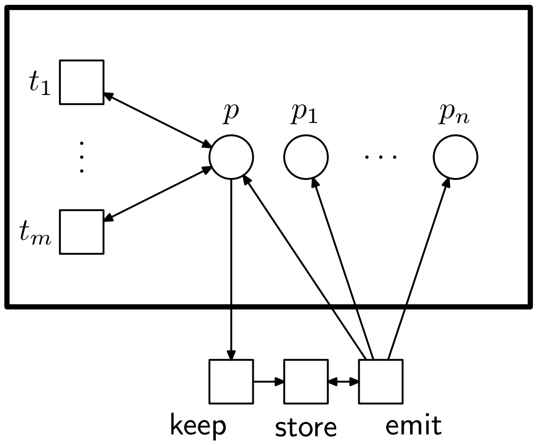


Místo p slouží jako počítadlo tokenů v síti $\mathcal{N}$. Síť $\mathcal{N}'$ je ekvivalentní síti $\mathcal{N}$, ale navíc v p udržuje počet tokenů ve zbylé části sítě. Pokud ve zbylé části (v síti $\mathcal{N}$) nejsou žádné tokeny, je i místo p prázdné.

Věta (Živost sítě a single-place zero-reachability)
Problém single-place zero-reachability je polynomiálně redukovatelný na problém živosti sítě.

Důkaz: Nechť Petriho síť $\mathcal{N} = (P, T, F)$, označkování M_0 a $p \in P$ tvoří instanci problému single-place zero-reachability. Označme $t_1, \ldots, t_m$ všechny přechody sítě $\mathcal{N}$ a $p_1, \ldots, p_n$ všechna místa sítě $\mathcal{N}$ kromě místa p. Instanci $\mathcal{N}'$, M_0 problému živosti sítě vytvoříme tak, že z místa p přidáme run-place hranu do všech přechodů sítě $\mathcal{N}$ a dále přechody keep, emit a místo store podle obrázku.

Petriho síť $\mathcal{N}$ s počátečním markingem M_0



Každý výpočet sítě $\mathcal{N}$ lze provést i v $\mathcal{N}'$. Pokud se zejména může vyprázdnit místo p v $\mathcal{N}$ (je dosažitelný příslušný marking), může se vyprázdnit i v $\mathcal{N}'$ a síť se zastaví kvůli run-place hranám — tedy není živá. Pokud se místo p naopak vyprázdnit nemůže, vždy lze provést přechod keep, který umístí token do místa store. Je-li v místě store alespoň jeden token, lze libovolně provádět přechod emit a připravit tak libovolný přechod v $\mathcal{N}'$ — síť je tedy živá.

Poznámka (Ostatní varianty živosti a single-place zero-reachability)
Problém single-place zero-reachability lze analogicky polynomiálně redukovat na problémy neživosti sítě, živosti přechodu i neživosti přechodu. Živost přechodu je speciální případ živosti sítě, lze použít totožnou redukci. Při redukci na neživost sítě by konstrukce byla také totožná, změnila by se jen interpretace výsledků: pokud instance nesplňuje single-place zero-reachability, redukcí vznikne neživá síť; pokud instance splňuje single-place zero-reachability, redukcí vznikne síť, která nebude neživá.

Věta (Živost přechodu a dosažitelnost)
Problém živosti přechodu je redukovatelný (v Turingově smyslu — Turingovým strojem s orákulem) na problém dosažitelnosti.

Minského stroj

Definice (Minského stroj)
Minského stroj je posloupnost instrukcí

$$\begin{aligned} l_1 &: \mathrm{Com}_1 \\ \vdots &\ \vdots \\ l_m &: \mathrm{Com}_\mathrm{m} \\ l_{m+1} &: \mathrm{halt} \end{aligned}$$

kde každá instrukce Com_i je typu I

l_i: inc c_j

nebo typu II

l_i: **if** $c_j = 0$
then goto l_k
else dec c_j; **goto** l_n

kde $c_j \in \mathbb{N}_0$, $j \in \{1, 2\}$, jsou dva neomezené nezáporné celočíselné registry.

Ekvivalence přechodových systémů

V této části se budeme zabývat ekvivalencemi přechodových systémů s návěštími, které jsou indukovány Petriho sítěmi — definujeme několik typů ekvivalencí a ukážeme některé vztahy mezi nimi.

Definice (Stopy stavu, trace-ekvivalence)
Nechť $\mathcal{T} = (S, \mathcal{A}, \rightarrow)$ je přechodový systém. Funkci $\mathrm{Traces} : S \rightarrow \mathcal{A}^*$ definujeme předpisem

$$\mathrm{Traces}(s) = \{w \in \mathcal{A}^* \mid \exists s' : s \xrightarrow{w} s'\}$$

Trace-ekvivalenci $=_{\mathrm{tr}} \subseteq S \times S$ definujeme předpisem

$$s \ =_{\mathrm{tr}} t \stackrel{\mathrm{def}}{\Longleftrightarrow} \mathrm{Traces}(s) = \mathrm{Traces}(q)$$

Definice (Bisimulace, bisimulační ekvivalence)
Nechť $\mathcal{T} = (S, \mathcal{A}, \rightarrow)$ je přechodový systém. Relaci $R \subseteq S \times S$ nazveme (*silnou*) *bisimulací*, jestliže pro všechna $(s, t) \in R$ platí

$$(\forall a \in \mathcal{A})(\forall s', s \xrightarrow{a} s')(\exists t', t \xrightarrow{a} t') : (s', t') \in R$$
$$(\forall a \in \mathcal{A})(\forall t', t \xrightarrow{a} t')(\exists s', s \xrightarrow{a} s') : (s', t') \in R$$

Největší relaci bisimulace $\sim \subseteq S \times S$ (taková zřejmě existuje) nazveme *bisimulační ekvivalencí*. Zřejmě $s \sim t$ právě tehdy, když existuje bisimulace R taková, že $(s, t) \in R$.

Poznámka (Vztah bisimulační ekvivalence a trace-ekvivalence)
Pro každý přechodový systém $\mathcal{T} = (S, \mathcal{A}, \rightarrow)$ a každé dva jeho stavy $s, t \in S$ zřejmě platí

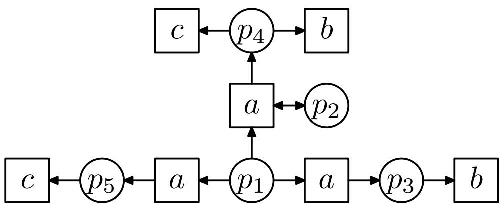
$$s \ \sim t \Rightarrow s \ =_{\text{tr}} t$$

Opačná implikace obecně neplatí. Uvažme například přechodový systém na obrázku, který je složen ze dvou částí. Zřejmě $s_1 =_{\text{tr}} s_1'$, ale $s_2' \neq_{\text{tr}} s_2$ ani $s_2' \neq_{\text{tr}} s_3$, takže trace-ekvivalence není bisimulací.

Takový přechodový systém je součastí přechodového systému generovaného Petriho sítí na následujícím obrázku, kde stavu s_1 odpovídá označkování označkování M_1 a stavu s_1' označkování M_1' dané předpisem

$$M_1(p) = \begin{cases} 1 & p = p_1 \\ 0 & \text{jinak} \end{cases}$$

$$M_1'(p) = \begin{cases} 1 & p = p_1 \vee p = p_2 \\ 0 & \text{jinak} \end{cases}$$



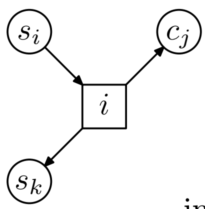
Věta (Nerozhodnutelnost ekvivalencí)
Nechť $\mathcal{T} = (S, \mathcal{A}, \rightarrow)$ je přechodový systém indukovaný Petriho sítí $\mathcal{N}$, $\approx \subseteq S \times S$ relace taková, že $\sim \subseteq \approx \subseteq =_{\text{tr}}$. Problém, zda dvě daná označkování M_1 a M_2 (stavy přechodového systému) splňují $M_1 \approx M_2$ je nerozhodnutelný.

Důkaz: Redukcí (nerozhodnutelného) problému zastavení Minského stroje. Pro daný Minského stroj $\mathcal{M}$ sestrojíme Petriho síť $\mathcal{N}$, její olabelování a dvě označkování M_1 a M_2 tak, že

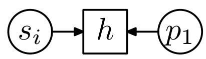
$$\mathcal{M} \text{ nezastaví} \Rightarrow M_1 \sim M_2 \Rightarrow M_1 \approx M_2$$
$$\mathcal{M} \text{ zastaví} \Rightarrow M_1 \neq_{\text{tr}} M_2 \Rightarrow M_1 \not\approx M_2$$

Nechť je tedy dán Minského stroj $\mathcal{M}$. Petriho síť definujeme po instrukcích následovně.

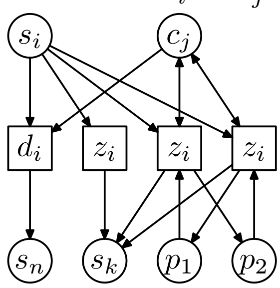
instrukce l_i: inc c_j; goto l_k



instrukce l_i: halt



instrukce l_i: if $c_j = 0$ then goto l_k else dec c_j ; goto l_n



Položme

$$M_1(p) = \begin{cases} 1 & p = s_1 \vee p = p_1 \\ 0 & \text{jinak} \end{cases}$$

$$M_2(p) = \begin{cases} 1 & p = s_1 \vee p = p_2 \\ 0 & \text{jinak} \end{cases}$$

V takto definované síti odpovídá korektnímu výpočtu právě jeden běh. Ostatní běhy jsou nekorektní v tom smyslu, že některý přechod z_i byl proveden v okamžiku, kdy příslušný c_j nebyl nulový.

Nechť $\mathcal{M}$ nezastaví, nikdy se tedy neprovede instrukce halt. Ani při jednom iniciálním označkování se tedy v korektním běhu nemůže provést přechod h. Ostatní běhy obsahují alespoň jeden nekorektní krok. Uvažme libovolný nekorektní běh z počátečního označkování M_1 a v něm první nekorektní krok z_i. Z markingu M_2 lze přesně simulovat tento běh až k prvnímu nekorektnímu kroku. Místo něj (protože příslušné $M_1(c_j) = M_2(c_j) \neq 0$) lze provést jiný přechod z_i, kterým se přemístí token z p_2 do p_1 a síť se dostane do identického stavu jako v simulovaném běhu. Symetricky pro simulování běhů z M_2 běhy z M_1.

Nechť $\mathcal{M}$ zastaví. V korektním běhu z počátečního označkování M_1 je posledním přechodem přechod h. Při simulaci tohto běhu z počátečního označkování M_2 musí síť provádět pouze korektní kroky, jinak by provedla přechod z_i místo d_i. Místo p_1 bude tedy stále prázdné a přechod h se proto neprovede. Z toho $\text{Traces}(M_1) \neq \text{Traces}(M_2)$.

Věta (Nerozhodnutelnost inkluze a rovnosti množin dosažitelných označkování)
Problém inkluze a rovnosti množin dosažitelných označkování je nerozhodnutelný.

Důkaz: Redukcí problému zastavení Minského stroje. Pro daný Miského stroj $\mathcal{M}$ sestrojíme Petriho sítě $\mathcal{N}_1$ a $\mathcal{N}_2$ a označkování M_1 a M_2 tak, aby následující podmínky byly ekvivalentní

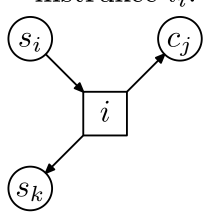
$$\mathcal{M} \text{ nezastaví} \tag{a}$$
$$\text{Reach}(\mathcal{N}_1, M_1) = \text{Reach}(\mathcal{N}_2, M_2) \tag{b}$$
$$\text{Reach}(\mathcal{N}_1, M_1) \subseteq \text{Reach}(\mathcal{N}_2, M_2) \tag{c}$$

Tvrzení dokážeme pomocí tří implikací, přičemž $(b) \Rightarrow (c)$ platí vždy.

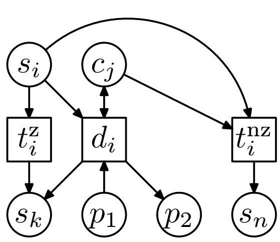
$$(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$$

Pro důkaz $(a) \Rightarrow (b)$ redukujme $\mathcal{M}$ podobně jako v důkazu předchozího tvrzení po instrukcích. Vytvořme tedy sítě $\mathcal{N}_1$ a $\mathcal{N}_2$ a označkování M_1 a M_2. I když v tomto případě není olabelování přechodů podstatné, zavedeme jej pro snazší vyjadřování. Části odpovídající instrukcím typu I a II jsou stejné v obou sítích:

instrukce l_i: inc c_j; goto l_k

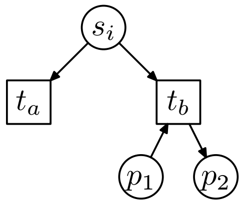


instrukce l_i: if $c_j = 0$ then goto l_k else dec c_j ; goto l_n

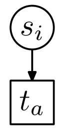


Instrukce l_i: halt se do sítě $\mathcal{N}_1$ zakóduje jinak než do $\mathcal{N}_2$.

instrukce l_i: halt v síti $\mathcal{N}_1$



instrukce l_i: halt v síti $\mathcal{N}_2$



Označkování definujme takto (množiny míst jsou stejné v obou sítích):

$$M_1(p) = M_2(p) = \begin{cases} 1 & p = s_1 \vee p = p_1 \\ 0 & \text{jinak} \end{cases}$$

Jediný rozdíl mezi sítěmi $\mathcal{N}_1$ a $\mathcal{N}_2$ je přechod t_b. Proto

$$\mathrm{Reach}(\mathcal{N}_2, M_2) \subseteq \mathrm{Reach}(\mathcal{N}_1, M_1)$$

zřejmě platí. Nechť $M \in \mathrm{Reach}(\mathcal{N}_1, M_1)$. Ukážeme, že potom také $M \in \mathrm{Reach}(\mathcal{N}_2, M_2)$. Rozlišíme dva pířpady.

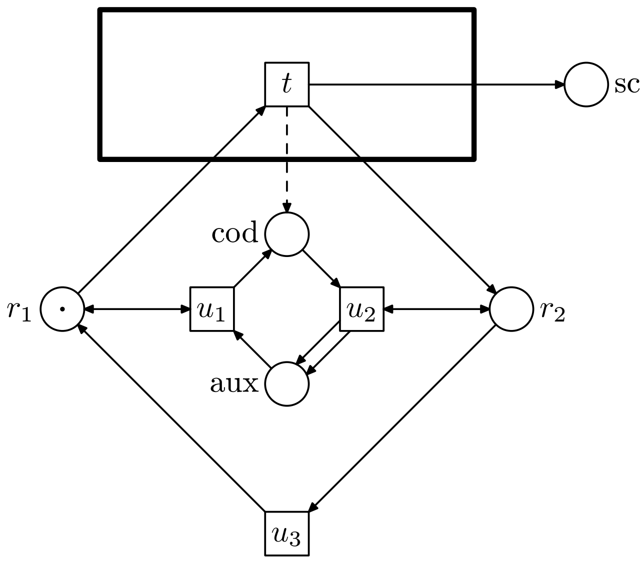
Pokud lze v $\mathcal{N}_1$ dosáhnout M posloupností přechodů, která neobsahuje přechod t_b, lze tutéž posloupnost provést v síti $\mathcal{N}_2$ a dosáhnout téhož označkování.

Naopak, nechť M lze v $\mathcal{N}_1$ dosáhnout pouze takovými posloupnostmi přechodů, které obsahují přechod t_b (a tento přechod je tam nejvýše jednou, protože se token přesune z p_1 do p_2). Protože podle (a) stroj $\mathcal{M}$ nezastaví, musela síť $\mathcal{N}_1$ alespoň jednou provést t_i^{z} místo t_i^{nz} (nekorektní krok). Přechod d_i to být nemohl, protože pak by nebylo možné

provést t_b — v p_1 už by nebyl token. Síť $\mathcal{N}_2$ místo jednoho takové přechodu mohla provést přechod d_i a dále se opět chovat jako $\mathcal{N}_1$. Protože je v $\mathcal{N}_2$ již token z p_1 přesunut do p_2, může $\mathcal{N}_2$ provést přechod t_a místo t_b v síti $\mathcal{N}_1$ a dostat se tak do téhož označkování.

Místo implikace $(c) \Rightarrow (a)$ dokážeme její obměnu $\neg(a) \Rightarrow \neg(c)$. Sítě $\mathcal{N}_1$ a $\mathcal{N}_2$ z důkazu implikace $(a) \Rightarrow (b)$ modifikujeme tak, aby síť $\mathcal{N}_1$ po provedení nekorektního kroku výpočtu již nemohla dosáhnout označkování odpovídajícího korektnímu výpočtu. Každý přechod sítí N_1 a N_2 kromě t_a a t_b modifikujeme podle následujícího obrázku. Přitom přechod t dává token do místa cod (přerušovaná šipka) právě tehdy, když $t = t_i^{\mathrm{nz}}$ pro nějaké i. Modifikované sítě označme $\mathcal{N}_1'$ a $\mathcal{N}_2'$. Modifikovaná počáteční označkování M_1' a M_2' jsou totožná s M_1 a M_2 až na přidaný token do místa r_1.

Petriho síť $\mathcal{N}_1$ nebo $\mathcal{N}_2$



V bězích, které maximalizují počet tokenů v cod, dochází v přidané podsíti k následujícím operacím. Pro každý přechod původní sítě, který je různý od t_i^{nz} pro všechna i, je počet tokenů v cod zdvojnásoben. Provede-li se v původní síti přechod t_i^{nz} pro nějaké i, pak je nejprve jeden token do cod přidán a potom je počet zdvojnásoben. Binární zápis počtu tokenů v cod tedy udává, kdy byl v posloupnosti přechodů původní sítě proveden přechod t_i^{nz} pro nějaké i (a to od prvního provedení takového přechodu).

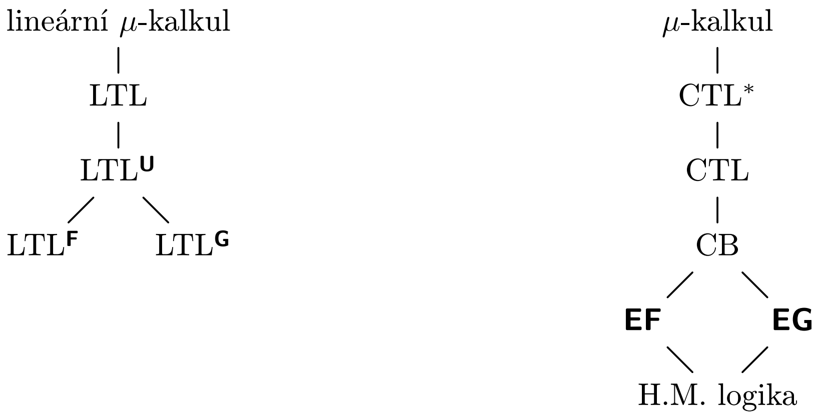
Ukážeme, že existuje označkování M takové, že platí $M \in \mathrm{Reach}(\mathcal{N}_1', M_1)$ a zároveň $M \notin \mathrm{Reach}(\mathcal{N}_2', M_2)$. Nechť označkování M odpovídá korektnímu výpočtu sítě N_1', který maximalizuje počet tokenů v cod, po provedení přechodu t_b. Zejména tedy platí $M(p_1) = 0$ a $M(p_2) = 1$. Aby se síť $\mathcal{N}_2'$ mohla dostat do takového označkování, musela někde provést přechod d_i. Ukážeme, že po provedení takového přechodu se již nikdy nedostane do označkování odpovídajícího korektnímu výpočtu.

Síť $\mathcal{N}_2'$ musela přechod d_i provést místo nějakého přechodu t_i^{nz} sítě $\mathcal{N}_1'$. Místo přechodu t_i^{z} to nebylo možné, protože uvažujeme korektní výpočet sítě $\mathcal{N}_1'$ — přechod t_i^{z} se provádí pouze v případě, že je příslušné místo c_j prázdné. Zatímco se tedy v $\mathcal{N}_1'$ přidá do cod token a potom se jejich počet vynásobí dvěma, v síti $\mathcal{N}_2'$ dojde pouze k vynásobení dvěma.

Pokud toto nenastane při prvním provedení některého z přechodů t_i^{nz} v síti $\mathcal{N}_1'$, počty tokenů v cod se již nikdy nebudou shodovat — zřejmé z významu jejich binárního zápisu. Pokud to ovšem nastane při prvním provedení některého ze všech t_i^{nz}, pak by se ještě počty tokenů shodovat mohly, protože místo cod sítě $\mathcal{N}_2'$ zůstává prázdné. Síť $\mathcal{N}_2'$ tak může provést ještě nějaké výpočty neobsahující žádný přechod t_i^{nz} a potom přesně simulovat výskyty ne nutně stejných přechodů t_i^{nz}. V takovém případě se ovšem budou alespoň o jedna lišit počty v místě sc — síť $\mathcal{N}_2$ musela provést alespoň přechod d_i navíc.

Model-checking Petriho sítí

Následující obrázek znázorňuje hierarchii jednotlivých fragmentů temporálních logik vzhledem k vyjadřovací síle.



Ukážeme nerozhodnutelnost model-checkingu pro LTL$^{\mathsf{F}}$ a EG a EF fragmenty CTL, z čehož bude plynout nerozhodnutelnost všech logik silnějších než některý z těchto fragmentů. Model-checking pro LTL$^{\mathsf{G}}$ a H.M. logiku je rozhodnutelný.

Poznámka (Logiky LTL$^{\mathsf{F}}$ a LTL$^{\mathsf{G}}$)
Fragment LTL$^{\mathsf{F}}$ obsahuje pouze temporální operátor F a negace je omezena pouze na atomické propozice. Fragment LTL$^{\mathsf{G}}$ má podobně omezenou negaci, z operátorů obsahuje pouze G. Temporální operátory F a G jsou duální, negace proto musí být omezena, aby fragment neobsahoval oba tyto operátory.

Poznámka (Sémantika temporálních logik pro Petriho sítě)
Sémantika je definována nad přechodovým systémem indukovaným Petriho sítí $\mathcal{N} = (P, T, F)$ a jejím počátečním označkováním M_0. Protože u *state-based* logik, kterými se budeme zabývat, nezáleží na návěštích přechodů, jsou všechny indukované přechodové systémy z pohledu temporálních logik totožné.

Sémantiku atomických propozic a jejich valuaci je pro model-checking Petriho sítí nutno omezit, jinak by pomocí vhodně zvolené valuace atomických propozic mohl být nerozhodnutelný i model-checking pouze jediné atomické propozice. Přirozené omezení je následující. Ke každému místu s Petriho sítě zvolíme (jedinečnou) atomickou propozici p_s. Valuaci, vzhledem k níž se definuje sémantika logik, definujeme pro atomickou propozici p a stav přechodového systému (označkování) M takto

$$M \in \nu(p) \overset{\text{def}}{\Longleftrightarrow} \exists s \in P : p = p_s \wedge M(s) > 0$$

Připomeňme jen, že platnost atomické propozice p pro běh α (logiky lineárního času), resp. ve stavu M (logiky větvícího se času) je definována vztahy

$$\alpha \models p \overset{\text{def}}{\Longleftrightarrow} \alpha(0) \in \nu(p) \tag{LTL}$$

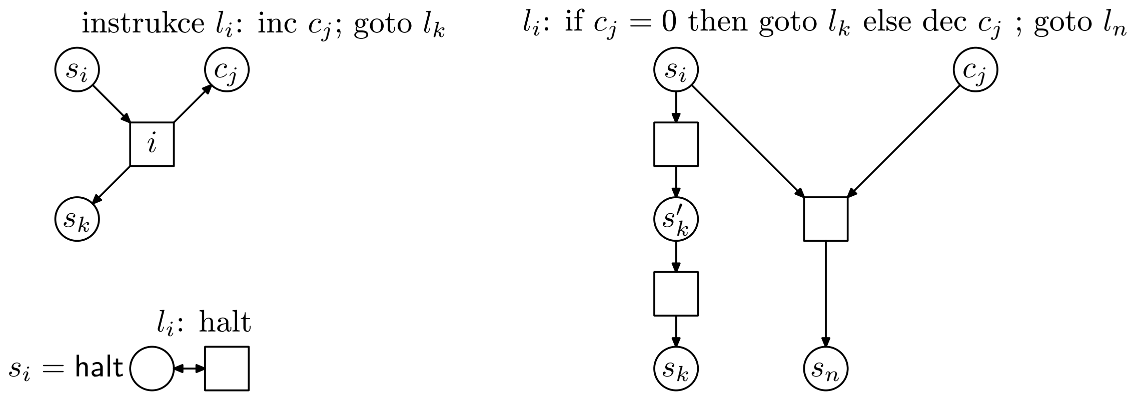
$$M \models p \overset{\text{def}}{\Longleftrightarrow} M \in \nu(p) \tag{CTL}$$

kde $\alpha(0)$ je počáteční stav běhu α a ν je funkce přiřazující atomickým propozicím množinu stavů, v nichž platí.

Je-li sémantika definována uvedeným způsobem a platí-li formule $\neg p_s$ ve stavu M, znamená to, že $M(s) = 0$.

Věta (Nerozhodnutelnost $\mathrm{LTL}^{\mathsf{F}}$)
Model-checking $\mathrm{LTL}^{\mathsf{F}}$ vlastností je pro Petriho sítě nerozhodnutelný.

Důkaz: Redukcí problému zastavení Minského stroje. Konstrukce Petriho sítě $\mathcal{N}$ a jejího počátečního markingu M_0 bude podobná jako v předchozích případech — transformace jednotlivých instrukcí je na následujícím obrázku. Počáteční marking bude mít pouze jeden token v místě s_1.



Instrukce halt byla modifikována tak, aby korektní běh systému byl nekonečný. Do sítě byly přidány stavy s'_k, aby bylo možné LTL formulí rozpoznat běhy, které neodpovídají korektnímu výpočtu simulovaného Minského stroje. Tato formule, označme ji ψ, má tvar

$$\psi \equiv \bigvee_{\text{instrukce typu 2}} (p_{c_j} \wedge p'_{k_i})$$

Definujme nyní formuli φ takto

$$\varphi \equiv \mathbf{F}(p_{\text{halt}} \vee \psi)$$

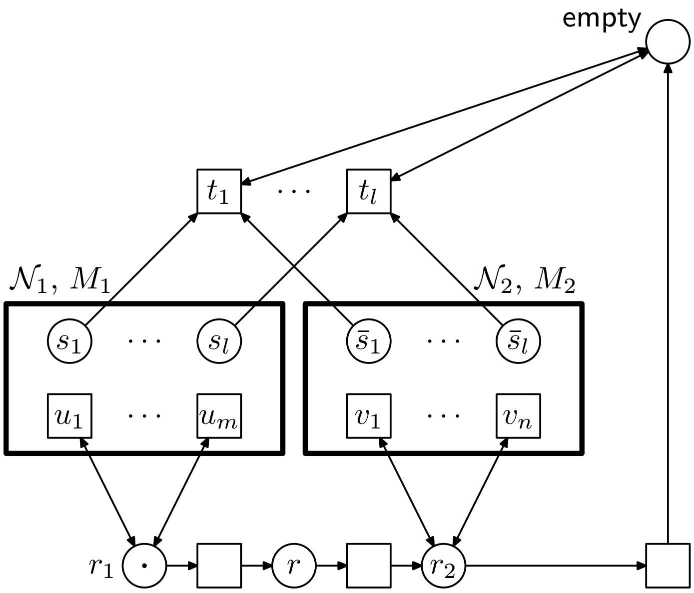
Pro každý běh α začínající v M_0 platí $\alpha \models \varphi$ právě tehdy, když simulovaný Minského stroj zastaví. Model-checking této vlastnosti je tedy nerozhodnutelný.

Věta (Nerozhodnutelnost **EG**-fragmentu CTL)
Model-checking vlastností **EG**-fragmentu CTL je pro Petriho sítě nerozhodnutelný.

Důkaz: **EG**-fragment CTL obsahuje duální operátor **AF**, je tedy nerozhodnutelný ze stejného důvodu jako LTL$^{\mathsf{F}}$.

Věta (Nerozhodnutelnost **EF**-fragmentu CTL)
Model-checking vlastností **EF**-fragmentu CTL je pro Petriho sítě nerozhodnutelný.

Důkaz: Důkaz provedeme redukcí problému inkluze množin dosažitelných označkování. Pro dané sítě $\mathcal{N}_1 = (P, T_1, F_1)$ a $\mathcal{N}_2 = (P, T_2, F_2)$ a jejich počáteční označkování M_1 a M_2 definujeme síť $\mathcal{N}$ s počátečním označkováním M_0 a vlastnost φ **EF**-fragmentu CTL tak, aby $M_0 \models \varphi$ právě tehdy, když $\mathrm{Reach}(\mathcal{N}_1, M_1) \subseteq \mathrm{Reach}(\mathcal{N}_2, M_2)$. Nechť $T_1 = \{u_1, \ldots, u_m\}$, $T_2 = \{v_1, \ldots, v_n\}$ a $P = \{s_1, \ldots, s_l\}$. Konstrukce $\mathcal{N}$ a definice M_0 je znázorněna na následujícím obrázku.



Sítě $\mathcal{N}_1$ a $\mathcal{N}_2$ byly spojeny pomocí čtyř run-place míst r_1, r, r_2 a empty. Dokud je řídící token v r_1, počítá $\mathcal{N}_1$. Jakmile se řídící token přemístí do r, síť $\mathcal{N}_1$ už nebude moci provést žádný přechod. Místo r je přidáno z jediného důvodu — aby bylo možno formulí určit okamžik, kdy přestala počítat $\mathcal{N}_1$ a začne počítat $\mathcal{N}_2$. Z místa r se token musí okamžitě přesunout do r_2, čímž se umožní běh sítě $\mathcal{N}_2$, která se „snaží“ dostat do stejného označkování, v jakém se nachází $\mathcal{N}_1$. Ve vhodném okamžiku se řídící token přesune do empty, v němž se srovnají označkování sítí $\mathcal{N}_1$ a $\mathcal{N}_2$. Protože v logice je k dispozici pouze test na prázdnost místa, umožňuje konstrukce vyprázdnit všechna místa $s_1, \ldots, s_l$ právě tehdy, pokud jsou označkování totožná.

Pro formuli φ,

$$\varphi \equiv \mathsf{AG}\big(p_r \Rightarrow \mathsf{EF}(\bigwedge_{i=1}^{l}(\neg s_i \wedge \neg \bar{s}_i)\big)$$

platí $M_0 \models \varphi$ právě tehdy, když $\text{Reach}(\mathcal{N}_1, M_1) \subseteq \text{Reach}(\mathcal{N}_2, M_2)$.

Poznámka (EF-fragment CTL bez zanoření temporálních operátorů)
Formule φ z předchozího důkazu má zanořené temporální operátory. Vlastnosti EF-fragmentu CTL bez zanořených temporálních operátorů jsou pro Petriho sítě rozhodnutelné.

Poznámka („Action-based“ logiky)
V předchozí části jsme se zabývali tzv. state-based logikami. Pro *action-based logiky*, v nichž sémantika není definována nad stavy, ale nad návěštími přechodů, jsou výsledky podobné s výjimkou LTL, která je pro action-based logiky rozhodnutelná.

Klasické techniky analýzy Petriho sítí

Poznámka (Omezení pro klasické techniky analýzy)
Pro účely této kapitoly se omezíme pouze na sítě bez násobných hran a se slabě souvislým grafem. Ve všech dalších definicích a tvrzeních budeme tedy předpokládat, že Petriho síť $\mathcal{N} = (P, T, F)$ splňuje

$$F : P \times T \cup T \times P \to \{0, 1\}$$

a má slabě, tj. bez ohledu na orientaci hran, souvislý graf.

Definice (Incidenční matice)
Nechť $\mathcal{N} = (P, T, F)$ je Petriho síť. *Incidenční maticí* $\mathsf{N} : P \times T \to \{-1, 0, 1\}$ rozumíme funkci udávající efekt přechodu $t \in T$ na místo $p \in P$, tj. danou vztahem

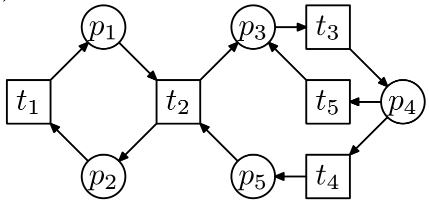
$$\mathsf{N}(p, t) = F(t, p) - F(p, t)$$

Definice (Kroneckerovo delta)
Pro snadnější zápis některých vztahů je vhodné závést tzv. *Kroneckerovo delta*, funkci definovanou vztahem

$$\delta_{ij} = \begin{cases} 1 & \text{pro } i = j \\ 0 & \text{jinak} \end{cases}$$

Poznámka (Notace vektorů, označkování jako vektory)
Tato kapitola využívá aparát lineární algebry. Budeme používat následující konvence. Vektory budeme chápat jako sloupcové matice, které budeme často zapisovat parametrizovaně $\vec{u} = (u_i)_{i=1}^{n}$. Označkování budeme formálně chápat jako vektory $M = (M(p))_{p \in P}$, kde P je množina míst.

Příklad (Incidenční matice)



Pro síť z předchozího obrázku má incidenční matice tvar

	t_1	t_2	t_3	t_4	t_5
s_1	1	−1	0	0	0
s_2	−1	1	0	0	0
s_3	0	1	−1	0	1
s_4	0	0	1	−1	−1
s_5	0	−1	0	1	0

Pokud $\mathsf{N}(p,t) = 0$, neznamená to, že by mezi p a t nevedla žádná hrana, ale že počet hran z místa p do přechodu t je roven počtu hran z t do p. Protože uvažujeme pouze sítě bez násobných hran, může tento počet být buď 0 nebo 1.

Nechť $t_i \in T$ je připraven při označkování M. Všimněme si, že platí

$$M \xrightarrow{t_i} M' \Leftrightarrow M' = M + \mathsf{N} \cdot (\delta_{ij})_{j=1}^{n}$$

Definice (Parikův obraz)
Buď $\mathcal{N} = (P, T, F)$ Petriho síť, kde $T = \{t_1, \dots, t_n\}$. Nechť $\sigma \in T^*$ je posloupnost přechodů. *Parikovým obrazem* posloupnosti σ rozumíme vektor

$$\vec{\sigma} = (\sigma_1, \dots, \sigma_n)^{\mathrm{T}}$$

kde σ_i je počet výskytů t_i v σ.

Věta (Nutná podmínka dosažitelnosti)
Nechť $\mathcal{N} = (P, T, F)$ je Petriho síť s incidenční maticí N. Nechť označkování M' je dosažitelné z M, $M \xrightarrow{\sigma} M'$, kde $\sigma \in T^*$. Potom existuje řešení rovnice

$$M' = M + \mathsf{N}X$$

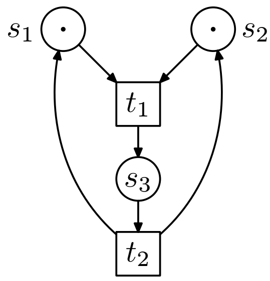
a řešením je i $\vec{\sigma}$.

Důkaz: Nechť $T = \{t_1, \dots, t_n\}$. Ukážeme-li, že $\vec{\sigma}$ je řešením uvedené rovnice, bude tím zároveň dokázána i existence řešení. Indukcí vzhledem k délce posloupnosti přechodů σ. Pro $\sigma = \varepsilon$ je $\vec{\sigma} = 0$, tedy $\mathsf{N}\vec{\sigma} = 0$ a skutečně $M' = M$.

Uvažme nyní $M \xrightarrow{\sigma} M' \xrightarrow{t_i} M''$ a označme $\varrho = \sigma t_i$. Tedy $\vec{\varrho} = \vec{\sigma} + (\delta_{ij})_{j=1}^{n}$. Z indukčního předpokladu platí $M' = M + \mathsf{N}\vec{\sigma}$. Efekt přechodu t_i na označkování M' je určen vektorem $(\mathsf{N}(p, t_i))_{p \in P} = \mathsf{N} \cdot (\delta_{ij})_{j=1}^{n}$. Celkem platí

$$\begin{aligned} M'' &= M' + \mathsf{N} \cdot (\delta_{ij})_{j=1}^{n} \\ &= M + \mathsf{N}\vec{\sigma} + \mathsf{N} \cdot (\delta_{ij})_{j=1}^{n} \\ &= M + \mathsf{N} \cdot \left(\vec{\sigma} + (\delta_{ij})_{j=1}^{n}\right) \\ &= M + \mathsf{N}\vec{\varrho} \end{aligned}$$

Příklad (Motivace pro S-invarianty)
S-invarianty jsou vlastně globální vlastnosti sítí. Neformálně se jedná o vektor určující váhy jednotlivých míst tak, aby vážené součty označkování dosažitelných z daného iniciálního markingu byly stejné. Písmeno „S“ značí, že S-invarianty vypovídají o stavech (z německého *die Stelle*). Pro síť na následujícím obrázku jsou S-invarianty například vektory $(1, 1, 2)^{\mathrm{T}}$, $(1, 0, 1)^{\mathrm{T}}$, $(0, 1, 1)^{\mathrm{T}}$, $(0, 0, 0)^{\mathrm{T}}$.



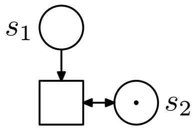
Přitom nulový vektor je S-invariantem pro každou síť. Povolíme-li jako váhy (koeficienty) racionální čísla nebo libovolné jiné pole $\mathbb{P}$, budou S-invarianty sítě s n místy tvořit vektorový podprostor $\mathbb{P}^n$ — jsou uzavřeny na násobení skalárem i součet.

Uvedená intuitivní definice nevypovídá nic o tom, jak S-invarianty vytvořit pro danou síť. Proto se definují jinak.

Definice (S-invariant)
Nechť $\mathcal{N} = (P, T, F)$ je Petriho síť s incidenční maticí N. Vektor $I \in \mathbb{Q}^{|P|}$ nazveme *S-invariant*, jestliže I je řešením rovnice

$$X^{\mathrm{T}} \cdot \mathsf{N} = 0^{\mathrm{T}}$$

Příklad (Určení S-invariantů)
Mějme (mrtvou) síť danou následujícím obrázkem



Incidenční matice této sítě je $\mathsf{N} = (0, -1)^{\mathrm{T}}$. S-invarianty jsou tedy řešením rovnice

$$\begin{aligned} (x_1, x_2)\begin{pmatrix} 0 \\ -1 \end{pmatrix} &= (0, 0) \\ -x_2 &= 0 \\ x_2 &= 0 \\ I \ &\in \{(k, 0)^{\mathrm{T}} \mid k \in \mathbb{Q}\} \end{aligned}$$

Vzhledem k intuitivní definici S-invariantů by však každý vektor $I \in \mathbb{Q}^2$ měl být S-invariantem, protože síť je mrtvá — má pouze jediné dosažitelné označkování. Formální definice nepokrývá všechny S-invarianty podle intuitivní definice. Řešení rovnice z formální definice totiž nejsou na rozdíl od intuitivní definice závislá na iniciálním markingu — jsou to S-invarianty pro každé počáteční označkování. Omezením se na konkrétní iniciální označkování a markingy z něj dosažitelné, se množina uvažovaných označkování zmenší a proto se může zvětšit množina S-invariantů.

Věta (Alternativní definice S-invariantů)
Nechť $\mathcal{N} = (P, T, F)$ je Petriho síť. Vektor $I \in \mathbb{Q}^{|P|}$ je S-invariant sítě $\mathcal{N}$ právě tehdy, když $\forall t \in T$ platí

$$\sum_{s \in {}^\bullet t} I(s) = \sum_{s \in t^\bullet} I(s)$$

kde $I(s)$ je složka vektoru I pro místo s, tj. žádný přechod nezmění vážený součet označkování.

Důkaz: Nechť I je řešením rovnice $X^{\mathrm{T}}\mathsf{N} = 0^{\mathrm{T}}$, kde N je incidenční matice sítě $\mathcal{N}$. Označme $\vec{t_j}$ j-tý sloupec N. Vektor I je S-invariant právě tehdy, když $I^{\mathrm{T}}\vec{t_j} = 0$ pro každé j. Rozepišme levou stranu rovnosti. Nechť $|P| = m$.

$$\begin{aligned} I^{\mathrm{T}}\vec{t_j} &= \sum_{i=1}^{m} I(s_i)\mathsf{N}(s_i, t_j) = \sum_{i=1}^{m} I(s_i)\big(F(t_j, s_i) - F(s_i, t_j)\big) \\ &= \sum_{i=1}^{m} I(s_i)F(t_j, s_i) - \sum_{i=1}^{m} I(s_i)F(s_i, t_j) \end{aligned}$$

Protože síť podle předpokladů neobsahuje násobné hrany, pro všechna i platí $F(t_j, s_i) \in \{0, 1\}$ a $F(s_i, t_j) \in \{0, 1\}$, přičemž

$$\begin{aligned} F(t_j, s_i) = 1 &\Leftrightarrow s_i \in t^\bullet \\ F(s_i, t_j) = 1 &\Leftrightarrow s_i \in {}^\bullet t \end{aligned}$$

odkud

$$\sum_{i=1}^{m} I(s_i)F(t_j, s_i) = \sum_{s \in t_j^\bullet} I(s)$$

$$\sum_{i=1}^{m} I(s_i)F(s_i, t_j) = \sum_{s \in {}^\bullet t_j} I(s)$$

Celkem dostáváme pro každé $t_j \in T$

$$0 = I^{\mathrm{T}}\vec{t_j} = \sum_{s \in t_j^\bullet} I(s) - \sum_{s \in {}^\bullet t_j} I(s)$$

Vektor I je tedy S-invariant právě tehdy, když pro všechna $t_j \in T$ platí

$$\sum_{s \in {}^\bullet t_j} I(s) = \sum_{s \in t_j^\bullet} I(s)$$

Věta (Alternativní nutná podmínka dosažitelnosti)
Pro Petriho síť $\mathcal{N} = (P, T, F)$ s iniciálním markingem M_0 a incidenční maticí N jsou následující podmínky ekvivalentní

$$\text{pro každý S-invariant } I \text{ platí } I^{\mathrm{T}}M_0 = I^{\mathrm{T}}M \qquad (a)$$
$$\text{rovnice } M_0 + \mathsf{N}X = M \text{ má řešení v } \mathbb{Q} \qquad (b)$$

Důkaz: $(b) \Rightarrow (a)$ Nechť I je libovolný S-invariant sítě $\mathcal{N}$, tedy platí $I^{\mathrm{T}}N = 0^{\mathrm{T}}$. Tedy

$$\begin{aligned} M &= M_0 + \mathsf{N}X \\ I^{\mathrm{T}}M &= I^{\mathrm{T}}(M_0 + \mathsf{N}X) = I^{\mathrm{T}}M_0 + I^{\mathrm{T}}\mathsf{N}X = I^{\mathrm{T}}M_0 + 0^{\mathrm{T}}X \\ I^{\mathrm{T}}M &= I^{\mathrm{T}}M_0 \end{aligned}$$

$(a) \Rightarrow (b)$ S-invarianty jsou řešením rovnice $X^{\mathrm{T}}\mathsf{N} = 0^{\mathrm{T}}$. Nechť $I_1, \ldots, I_n$ je báze prostoru řešení této rovnice. Pokud $n = 0$, neexistuje žádný S-invariant a implikace platí triviálně. Nechť tedy $n > 0$.

Označme $\mathsf{A} = (I_i^{\mathrm{T}})_{i=1}^{n}$ matici, jejíž řádky tvoří jednotlivé bázové S-invarianty. Tedy platí $\mathsf{A} \cdot \mathsf{N} = 0$ a sloupce matice N generují prostor řešení rovnice

$$\mathsf{A}X = 0$$

Je-li totiž m velikost největší lineárně nezávislé množiny tvořené sloupci N, potom $n = |P| - m$. Protože řádky matice A jsou tvořeny bází, jsou lineárně nezávislé a dimenze prostoru řešení rovnice $\mathsf{A}X = 0$ je $|P| - n = m$. Přitom každý sloupec N je řešením a je mezi nimi m lineárně nezávislých — báze prostoru řešení.

Podle (a) pro všechna i, $1 \leq i \leq n$, platí

$$\begin{aligned} I_i^{\mathrm{T}} M_0 &= I_i^{\mathrm{T}} M \\ I_i^{\mathrm{T}}(M_0 - M) &= 0 \\ \mathsf{A}(M - M_0) &= 0 \end{aligned}$$

Vektor $M - M_0$ je tedy řešením rovnice $\mathsf{A}X = 0$ a lze jej proto vyjádřit jako lineární kombinace sloupců N, které tento prostor generují. Pro vhodné R tedy platí

$$M - M_0 = \mathsf{N}R \qquad \Rightarrow \qquad M = M_0 + \mathsf{N}R$$

Poslední rovnost lze chápat i tak, že R je řešením rovnice

$$M = M_0 + \mathsf{N}X$$

Definice (Semipozitivní a pozitivní S-invarianty)
S-invariant I sítě $\mathcal{N} = (P, T, F)$ se nazývá *semipozitivní*, jestliže $I(s) \geq 0$ pro všechna $s \in P$ a existuje $s_0 \in P$ takové, že $I(s_0) > 0$. S-invariant I se nazývá *pozitivní*, jestliže $I(s) > 0$ pro všechna $s \in P$.

Věta (Nutná podmínka živosti sítě)
Nechť $\mathcal{N} = (P, T, F)$ je Petriho síť s počátečním označkováním M_0. Je-li $(\mathcal{N}, M_0)$ živá, pak pro každý semipozitivní S-invariant I platí

$$I^{\mathrm{T}} M_0 > 0$$

Důkaz: Síť $\mathcal{N}$ je živá, jestliže pro každý dosažitelný marking M a každý přechod $t \in T$ existuje marking M' dosažitelný z M, v němž je t uschopněný. Předpokládejme nyní sporem, že $I^{\mathrm{T}} M_0 = 0$. Případ $I^{\mathrm{T}} M_0 < 0$ nemůže nastat, protože pro všechna $s \in P$ platí $I(s) \geq 0$ z předpokladu a $M_0(s) \geq 0$ z definice.

Protože I je semipozitivní, existuje $s_0 \in P$ takové, že $I(s_0) > 0$. Neboť uvažujeme pouze sítě se slabě souvislým grafem, existuje přechod $t \in T$ takový, že $t \in {}^{\bullet}s_0$ nebo $t \in s_0{}^{\bullet}$. Síť $\mathcal{N}$ je živá, tedy existuje označkování M dosažitelné z M_0, v němž je přechod t uschopněn. Označíme-li M' označkování, do nějž se síť dostane z označkování M provedením přechodu t, potom $I^{\mathrm{T}} M > 0$ nebo $I^{\mathrm{T}} M' > 0$, protože $M(s_0) > 0$ nebo $M'(s_0) > 0$. Tedy I není S-invariant — spor.

Věta (Postačující podmínka ohraničenosti sítě)
Nechť $\mathcal{N} = (P, T, F)$ je Petriho síť. Má-li $\mathcal{N}$ pozitivní S-invariant, pak je ohraničená pro všechna počáteční označkování.

Důkaz: Sporem. Nechť má síť pozitivní S-invariant I, ale není ohraničená, tj. existuje neohraničené místo $p \in P$. Nechť M je označkování sítě. Protože p není ohraničené, existuje dosažitelný marking M' takový, že

$$M'(p) > \frac{I^{\mathrm{T}} M}{I(p)}$$

Potom, protože I je pozitivní, a místa nemohou obsahovat záporný počet tokenů, platí

$$I^{\mathrm{T}} M' \geq I(p) M'(p) > I^{\mathrm{T}} M$$

Tedy I není S-invariant — spor.

Poznámka (Motivace pro T-invarianty)
S-invarianty jsou definovány jako řešení rovnice $X^{\mathrm{T}}\mathsf{N} = 0^{\mathrm{T}}$. Je přirozené zajímat se o vlastnosti řešení duální rovnice $\mathsf{N}X = 0$ a pokusit se je interpretovat.

Definice (T-invariant, semipozitivní a pozitivní T-invariant)
T-invariantem Petriho sítě $\mathcal{N}$ s incidenční maticí N nazveme každé řešení v $\mathbb{Q}$ rovnice

$$\mathsf{N}X = 0$$

T-invariant J se nazývá *semipozitivní*, jestliže $J(t) \geq 0$ pro všechna $t \in T$ a existuje $t_0 \in T$, pro nějž $J(t_0) > 0$. T-ivariant J se nazývá *pozitivní*, jestliže $J(t) > 0$ pro všechna $t \in T$.

Věta (Alternativní definice T-invariantu)
Nechť $\mathcal{N} = (P, T, F)$ je Petriho síť. Funkce $J : T \to \mathbb{Q}$ je T-invariant právě tehdy, když pro každé místo $p \in P$ platí

$$\sum_{t \in {}^{\bullet}p} J(t) = \sum_{t \in p^{\bullet}} J(t)$$

Důkaz: Důkaz je analogický důkazu alternativní definice S-invariantu.

Věta (Parikův obraz posloupnosti přechodů jako T-invariant)
Nechť je posloupnost přechodů $\sigma \in T^*$ proveditelná v síti $\mathcal{N} = (P, T, F)$ z označkování M. Pak $\vec{\sigma}$ je T-invariant právě tehdy, když $M \xrightarrow{\sigma} M$.

Důkaz: Přímý důsledek nutné podmínky dosažitelnosti.

Věta (Nutná podmínka živosti a ohraničenosti — pozitivní T-invariant)
Nechť je Petriho síť $\mathcal{N} = (P, T, F)$ s iniciálním markingem M_0 živá a ohraničená. Potom existuje pozitivní T-invariant sítě $\mathcal{N}$.

Důkaz: Protože $(\mathcal{N}, M_0)$ je živá, lze z každého označkování připravit libovolný přechod. Z každého označkování tedy existuje proveditelná posloupnost přechodů, která obsahuje každý přechod alespoň jednou. Definujme rekurzívně označkování M_i, $0 \leq i$. Označkování M_0 je počáteční označkování sítě. Označkování M_{i+1} vznikne posloupností přechodů σ_i z označkování M_i, kde σ_i obsahuje každý přechod alespoň jednou.

Protože $(\mathcal{N}, M_0)$ je ohraničená, existuje pouze konečně mnoho různých označkování, označme jejich počet n. Mezi výše definovanými označkováními M_i, $0 \leq i \leq n$, tedy musí být alespoň dvě totožná. Nechť $M_{i_1} = M_{i_2}$, $i_1 < i_2$. Potom

$$\vec{\sigma} = \vec{\sigma}_{i_1} + \cdots + \vec{\sigma}_{i_2-1}$$

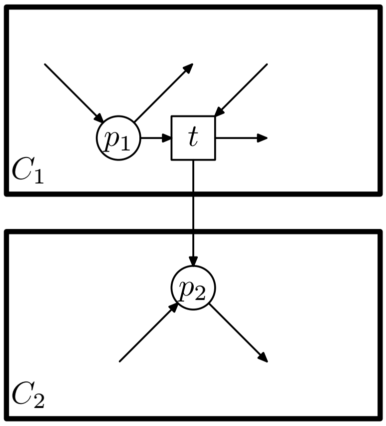
je pozitivní T-invariant.

Věta (Nutná podmínka živosti a ohraničenosti — silná souvislost)
Nechť je Petriho síť $\mathcal{N} = (P, T, F)$ s iniciálním markingem M_0 živá a ohraničená. Pak graf $\mathcal{N}$ je silně souvislý.

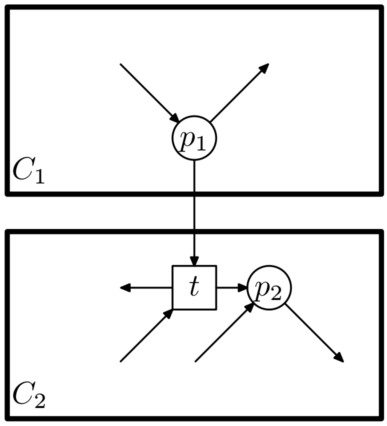
Důkaz: Připomeňme, že uvažujeme pouze sítě se slabě souvislým grafem. Jedná se tedy o zesílení charakteristiky. Sporem předpokládejme, že se graf skládá alespoň ze dvou silně souvislých komponent. Kvůli slabé souvislosti tedy existuje alespoň jedna terminální komponenta $\mathcal{C}_2$ a její předchůdce $\mathcal{C}_1$. Konkrétně, existuje přechod t, který bere z $p_1 \in \mathcal{C}_1$ a dává do $p_2 \in \mathcal{C}_2$. Rozlišíme dvě možnosti podle toho, kde se nachází t.

Nechť $t \in \mathcal{C}_1$. Protože $\mathcal{N}$ je živá a $\mathcal{C}_2$ nemůže dávat tokeny do $\mathcal{C}_1$, musí být C_1 schopna libovolněkrát připravit a odpálit přechod t. Tím dochází ke kumulaci tokenů v p_2 — spor s ohraničeností.

Nechť $t \in \mathcal{C}_2$. Protože místo p_1 dává do t, musí mít libovolněkrát k dispozici token, aby bylo možné libovolněkrát provést přechod t. Uvážíme-li takovou posloupnost, která opakovaně připravuje přechod t a vynecháme-li z ní přechod $t \in \mathcal{C}_2$, dojde ke kumulaci tokenů v p_1 — spor s ohraničeností.



$t \in C_1$



$t \in C_2$

Definice (S-systém)
Petriho síť $\mathcal{N} = (P, T, F)$ nazveme *S-systém* (*S-síť*), jestliže pro všechny přechody $t \in T$ platí

$$|{}^{\bullet}t| = |t^{\bullet}| = 1$$

Věta (Nutná podmínka dosažitelnosti v S-systému — zachování počtu tokenů)
Nechť je označkování M' dosažitelné z M v S-systému $\mathcal{N} = (P, T, F)$. Potom platí

$$\sum_{p \in P} M(p) = \sum_{p \in P} M'(p)$$

Důkaz: Zřejmé — žádný přechod nemění počet tokenů.

Lemma (Nutná podmínka silné souvislosti grafu S-systému)
Nechť $\mathcal{N} = (P, T, F)$ je S-systém se silně souvislým grafem. Pro každá dvě místa $p_1, p_2 \in P$ a označkování M, $M(p_1) > 0$, existují $\sigma \in T^*$ a označkování M', $M \xrightarrow{\sigma} M'$ takové, že

$$M'(p) = \begin{cases} M(p_1) - 1 & \text{pro } p = p_1 \\ M(p_2) + 1 & \text{pro } p = p_2 \\ M(p) & \text{jinak} \end{cases}$$

Důkaz: Ze silné souvislosti grafu $\mathcal{N}$ plyne existence cesty σ mezi p_1 a p_2. Označme ji $\varrho = s_0 t_0 s_1 t_1 \dots t_{n-1} s_n$, $s_i \in P$, $t_i \in T$, $s_0 = p_1$ a $s_n = p_2$. Každý přechod t_i, $0 \leq i < n$ odebere token z s_i a vloží jej do s_{i+1}. Protože $s_0 = p_1$ obsahuje při M alespoň jeden token, je posloupnost přechodů $\sigma = t_0 \dots t_{n-1}$ proveditelná v M a označkování se změní předepsaným způsobem.

Věta (Živost S-systémů)
S-systém $\mathcal{N} = (P, T, F)$ s počátečním označkováním M_0 je živý právě tehdy, když graf $\mathcal{N}$ je silně souvislý a existuje $p \in P : M_0(p) > 0$.

Důkaz: „$\Rightarrow$" Přímým důsledkem nutné podmínky dosažitelnosti je skutečnost, že každý S-systém je ohraničený. Živý S-systém je tedy živá a ohraničená Petriho síť. Graf $\mathcal{N}$ je proto silně souvislý. Aby byla jakákoliv síť živá, musí jistě obsahovat nenulový počet tokenů. Proto $\exists p \in P : M_0(p) > 0$.

„$\Leftarrow$" Nechť M je libovolné označkování dosažitelné z M_0. Protože v S-systému se zachovává počet tokenů, existuje $s \in P : M(s) > 0$. Nechť $t \in T$ je libovolný. Nechť ${}^{\bullet}t = \{s'\}$. Ze silné souvislosti grafu $\mathcal{N}$ existuje posloupnost přechodů $\sigma \in T^*$, která přesune token z s do s' — uschopní přechod t.

Lemma (Postačující podmínka dosažitelnosti v S-systému)
Nechť $\mathcal{N} = (P, T, F)$ je S-systém se silně souvislým grafem a nechť pro dvě označkování M, M' platí

$$\sum_{p \in P} M(p) = \sum_{p \in P} M'(p)$$

Potom existuje $\sigma \in T^*$ takové, že $M \xrightarrow{\sigma} M'$.

Důkaz: Pro každé $p \in P$, pro nějž $M(p) > M'(p)$ lze kvůli silné souvislosti grafu N přebytečné tokeny přesunout do míst $s \in P$, pro něž $M(s) < M'(s)$.

Věta (Ohraničenost živých S-systémů)
Nechť je S-systém $\mathcal{N} = (P, T, F)$ s počátečním označkováním M_0 živý. Potom $(\mathcal{N}, M_0)$ je b-ohraničený právě tehdy, když platí

$$\sum_{p \in P} M_0(p) \leq b$$

Důkaz: „⇒“ Živý S-systém má silně souvislý graf. Všechny tokeny v něm lze tedy přemístit do jediného místa $p_0 \in P$. Označme tomu odpovídající marking M. Platí $M(p_0) \leq b$ z b-ohraničenosti sítě a $M(p) = 0$ pro $p \neq p_0$. Protože S-systém zachovává počet tokenů v sítí, platí

$$\sum_{p \in P} M_0(p) = \sum_{p \in P} M(p) = M(p_0) \leq b$$

„⇐“ Protože S-systém zachovává počet tokenů, nemůže žádné místo obsahovat více než $\sum_{p \in P} M_0(p) \leq b$ tokenů. Tedy síť je b-ohraničená.

Věta (Dosažitelnost v živém S-systému I)
Nechť $\mathcal{N} = (P, T, F)$ je živý S-systém. Marking M je dosažitelný z M_0 právě tehdy, když

$$\sum_{p \in P} M_0(p) = \sum_{p \in P} M(p)$$

Důkaz: Směr „⇒“ vyjadřuje nutnou podmínku dosažitelnosti. Pro opačný směr si uvědomme, že živý S-systém je ohraničený a má tedy silně souvislý graf. Je tedy splněna postačující podmínka pro dosažitelnosti v S-systému.

Věta (Charakterizace S-invariantů)
Nechť $\mathcal{N} = (P, T, F)$ je S-systém. Vektor I je S-invariant právě tehdy, když $I = (x)_{i=1}^{|P|}$ pro nějaké $x \in \mathbb{Q}$.

Důkaz: „⇐“ Pro každé $t \in T$ platí

$$\sum_{p \in {}^\bullet t} I(p) = x = \sum_{p \in t^\bullet} I(p)$$

což je alternativní definice S-invariantů.

„⇒“ Nechť $|P| = n$ a $p \in P$ je libovolné místo. Definujme induktivně množiny P_i, $0 \leq i \leq n$, takto

$$\begin{aligned} P_0 &= \{p\} \\ P_{i+1} &= \{p \in t^\bullet \mid (\exists s \in P_i)(\exists t \in T) : s \in {}^\bullet t\} \cup \\ &\cup \{p \in {}^\bullet t \mid (\exists s \in P_i)(\exists t \in T) : s \in t^\bullet\} \end{aligned}$$

Jistě pro všechna i platí $P_i \subseteq P_{i+1}$ a kvůli slabé souvislosti grafu $\mathcal{N}$ platí $P_n = P$. Nechť I je libovolný S-invariant. Indukcí vzhledem k i ukážeme, že $(\forall i)(\forall s \in P_i) : I(s) = I(p)$. Pro $i = 0$ tvrzení platí. Nechť $s \in P_{i+1}$ je libovolné. Pak existuje $s' \in P_i$ a přechod $t \in T$ tak, že $\{s'\} = {}^\bullet t$ a $\{s\} = t^\bullet$, nebo $\{s'\} = t^\bullet$ a $\{s\} = {}^\bullet t$. Protože $I(s') = I(p)$ z indukčního předpokladu, v obou případech dostáváme z alternativní definice S-invariantu

$$I(p) = I(s') = I(s)$$

Věta (Dosažitelnost v živém S-systému II)
Nechť $\mathcal{N} = (P, T, F)$ je živý S-systém při označkování M_0. Označkování M je dosažitelné z M_0 právě tehdy, když pro každý S-invariant I platí

$$I^{\mathrm{T}} M_0 = I^{\mathrm{T}} M$$

Důkaz: Implikace „⇒“ platí obecně — alternativní nutná podmínka dosažitelnosti. Zbývá tedy ukázat „⇐“. Podle charakterizace S-invariantů S-systémů je $I = (1)_{i=1}^{|P|}$ S-invariant, tedy platí

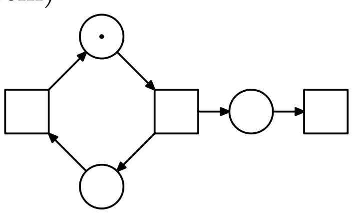
$$\sum_{p \in P} M_0(p) = \sum_{p \in P} M(p)$$

Podle přechozí věty o dosažitelnosti je M dosažitelné z M_0.

Definice (T-systém)
Petriho síť $\mathcal{N} = (P, T, F)$ nazveme *T-systémem*, jestliže pro všechna místa $p \in P$ platí

$$|p^{\bullet}| = |{}^{\bullet}p| = 1$$

Příklad (Neohraničený T-systém)



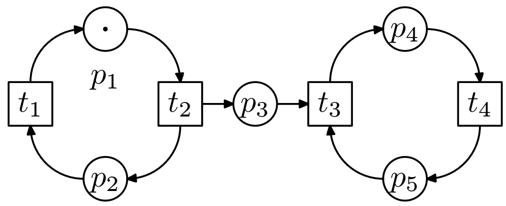
Definice (Cyklus)
Cyklem v síti $\mathcal{N} = (P, T, F)$ rozumíme cestu z uzlu x grafu $\mathcal{N}$ do uzlu y takovou, že $F(y, x) = 1$ a žádný uzel se na této cestě nevyskytuje více než jednou.

Nechť M je marking $\mathcal{N}$, γ je cyklus v M a R je množina míst v γ. Definujeme

$$M(\gamma) = \sum_{p \in R} M(p)$$

Řekneme, že cyklus γ je *označkován* v markingu M, jestliže $M(\gamma) \geq 1$.

Příklad (T-systém s cykly)
Síť s markingem na následujícím obrázku obsahuje dva cykly, $\gamma_1 = p_1 t_2 p_2 t_1$ a $\gamma_2 = p_4 t_4 p_5 t_3$, z nichž první je označkovaný a druhý není.



Věta (Nutná podmínka dosažitelnosti v T-systému)
Nechť γ je cyklus T-systému $\mathcal{N} = (P, T, F)$ a M_0 jeho iniciální marking. Pak pro každé označkování M dosažitelné z M_0 platí

$$M_0(\gamma) = M(\gamma)$$

Důkaz: Protože M je dosažitelné z M_0, existuje posloupnost přechodů $\sigma \in T^*$, $M_0 \xrightarrow{\sigma} M$. Indukcí k délce σ. Základní krok je zřejmý. Uvažme tedy M' dosažitelné z M_0, $M' \xrightarrow{t} M''$, $M_0(\gamma) = M'(\gamma)$ pro libovolné pevné $t \in T$. Rozlišíme dvě možnosti.

Nechť γ obsahuje t. Potom t bere z jednoho místa cyklu — z každého místa vede právě jedna hrana, hrany z ostatních míst cyklu musí tvořit tento cyklus, vedou tedy do jiných přechodů. Ze stejného důvody t dává do právě jednoho místa cyklu. Počet tokenů v cyklu se tedy odpálením přechodu t nezmění.

Nechť γ neobsahuje t. Všechny hrany, které vedou z míst cyklu a do míst cyklu, tvoří tento cyklus. Proto t nebere z žádného místa cyklu ani do žádného nedává. Odpálením takového přechodu se distribuce tokenů v cyklu nezmění.

Důsledek (Nutná podmínka neohraničenosti místa v T-systému)
Neohraničená místa v T-systémech neleží na žádném cyklu.

Věta (Živost T-systémů)
T-systém $(\mathcal{N}, M_0)$, $\mathcal{N} = (P, T, F)$, je živý právě tehdy, když každý cyklus γ splňuje $M_0(\gamma) \geq 1$.

Důkaz: Implikace „$\Rightarrow$“ se snadno dokáže ze své obměny.

Pro důkaz „$\Leftarrow$“ uvažme libovolný marking M dosažitelný z M_0 a libovolný přechod $t \in T$. Ukážeme, že existuje označkování M', $M \rightarrow^* M'$ a t je uschopněn v M'. Pro každé označkování M definujme množinu S_M předpisem

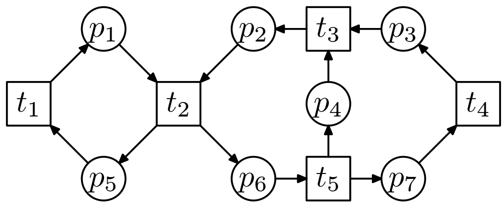
$$S_M = \{s \in P \mid \text{existuje cesta z } s \text{ do } t\text{, na níž jsou všechna místa prázdná v } M\}$$

Indukcí k $|S_M|$ dokážeme, že pro libovolnou S_M lze připravit přechod t. Je-li $|S_M| = 0$, pak t je připraven v M. Nechť tedy $|S_M| = n + 1$. Označme π cestu v $(\mathcal{N}, M)$ maximální délky, na níž jsou všechna místa prázdná, a která končí v t. Cesta π je nutně konečná, jinak by obsahovala neoznačkovaný cyklus, což z předpokladů není možné. Z maximality π potom plyne, že první uzel je přechod, označme jej u, a tento je připraven v M. Uvažme marking M', $M \xrightarrow{u} M'$. Ukážeme, že $S_{M'} \subset S_M$, z indukčního předpokladu bude tedy možné uzavřít, že z M lze připravit t.

Nechť je tedy $s \in S_{M'}$. Pak existuje cesta z s do t, na níž jsou všechna místa při označkování M' prázdná. Uvědomme si, že M' vzniklo z M provedením přechodu u. Označkování se tedy liší pouze v místech z ${}^\bullet u$ a $u^\bullet$ a uvažovaná cesta z s do t neobsahuje přechod u, protože pak by obsahovala neprázdné místo z $u^\bullet$ — všechna místa z $u^\bullet$ jsou bezprostředně po provedení přechodu u neprázdná. Tato cesta neobsahuje ani místa z ${}^\bullet u$, protože $\mathcal{N}$ je T-systém, takže z každého takového místa vede jediná hrana — do přechodu u. Na všech místech uvažované cesty z s do t jsou M a M' totožné, tedy $s \in S_M$.

Zbývá ukázat, že existuje $s \in S_M$ takové, že $s \notin S_{M'}$. Při označkování M existuje prázdné místo $s \in u^\bullet$, $s \in S_M$, druhý uzel maximální cesty uvažované na začátku důkazu. V označkování M' — po provedení přechodu u — je toto místo neprázdné, tedy $s \notin S_{M'}$.

Příklad (Ilustrace k důkazu charakteristické podmínky živosti T-systémů)



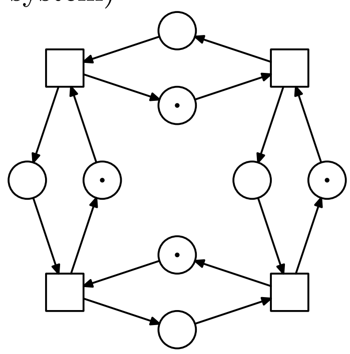
Důsledek (Složitost problému živosti T-systémů)
Problém živosti sítě je pro T-systémy rozhodnutelný v polynomiálním čase. Na základě předchozí věty lze totiž problém živosti T-systémů rozhodovat následujícím algoritmem.

while existuje prázdné nenavštívené místo **do**
  prohledáváním do šířky hledej cyklus složený ...
  ... pouze z přechodů a prázdných nenavštívených míst
  místa, kterými prohledávání prošlo, se stávají navštívená
  if nalezen cyklus **then**
    return síť není živá
  fi
done
return síť je živá

Věta (Charakterizace T-invariantů)
Nechť $\mathcal{N} = (P, T, F)$ je T-systém. Vektor I je T-invariant $\mathcal{N}$ právě tehdy, když $I = (x)_{i=1}^{|T|}$ pro nějaké $x \in \mathbb{Q}$.

Důkaz: Důkaz je duální důkazu charakterizace S-invariantů pro S-systémy.

Příklad (Živý 1-ohraničený T-systém)



Věta (Ohraničenost živých T-systémů)
Živý T-systém $\mathcal{N} = (P, T, F)$ s iniciálním markingem M_0 je b-ohraničený právě tehdy, když každé místo $s \in P$ leží na nějakém cyklu γ takovém, že $M_0(\gamma) \leq b$.

Důkaz: „$\Leftarrow$“ Tento směr plyne přímo z nutné podmínky dosažitelnosti v T-systému — počet tokenů v cyklech se zachovává. V každém místě tedy může být nejvýše tolik tokenů, kolik tokenů je v cyklu s nejméně tokeny, na němž místo leží. Dle předpokladů implikace je to pro každé místo nejvýše b.

„$\Rightarrow$“ Nechť $s \in P$ je libovolné pevné místo. Musíme ukázat, že existuje cyklus γ obsahující s, pro nějž $M(\gamma) \leq b$. Uvažme dosažitelné označkování M, kde $M(s)$ je maximální možné. Z b-ohraničenosti sítě v předpokladech je jisté, že $M(s) \leq b$. Definujme označkování L předpisem

$$L(r) = \begin{cases} 0 & \text{pro } r = s \\ M(r) & \text{jinak} \end{cases}$$

Potom systém $(\mathcal{N}, L)$ není živý. Kdyby byl, potom by z L existovala proveditelná posloupnost přechodů σ, která by připravila a provedla přechod $t \in {}^\bullet s$. Tím by se síť dostala do označkování L', $L'(s) = 1$. Poslopnost přechodů σ by však jistě bylo možné provést i z označkování M, čímž by se síť dostala do označkování M', $M'(s) = M(s) + 1$, což je spor s předpokladem maximality.

Protože systém $(\mathcal{N}, L)$ není živý, z obměny charakteristiky živých T-systémů plyne, že existuje cyklus γ, $L(\gamma) = 0$. Ovšem systém $(\mathcal{N}, M)$ živý je, tedy $M(\gamma) > 0$. Protože označkování M a L se liší pouze hodnotou pro místo s, musí s ležet na γ. V označkování M je to navíc jediné neprázdné místo tohoto cyklu. Pro cyklus γ proto platí

$$M(\gamma) = M(s) \leq b$$

Protože M je dosažitelné z M_0, z nutné podmínky dosažitelnosti plyne $M_0(\gamma) = M(\gamma)$. Tedy γ je cyklus požadované vlastnosti.

Lemma (Vlastnosti řešení nutné podmínky dosažitelnosti pro T-systémy)
Nechť N je incidenční matice T-systému $\mathcal{N} = (P, T, F)$ a nechť je označkování M dosažitelné z M_0. Potom existuje takové řešení rovnice

$$M_0 + \mathsf{N}X = M \qquad (*)$$

které má všechny složky kladné.

Důkaz: Z nutné podmínky dosažitelnosti pro obecné Petriho sítě je zaručena existence nějakého řešení X_0. Nechť $I = \lambda(1)_{i=1}^{|T|}$ je T-invariant T-systému. Potom i $X + I$ je řešení rovnice $(*)$. Protože I je T-invariant, platí $NI = 0$, takže

$$N(X + I) = NX + NI = NX$$

Protože složky X_0 jsou konečné a složky I lze zvolit libovolně velké, existuje řešení $X_1 = X_0 + I$, jehož všechny složky jsou kladné.

Lemma (Celočíselné řešení nutné podmínky dosažitelnosti pro T-systémy)
Jestliže pro označkování M dosažitelné z M_0 v T-systému $\mathcal{N} = (P, T, F)$ s incidenční maticí N existuje řešení rovnice

$$M_0 + \mathsf{N}X = M \qquad (*)$$

potom má tato rovnice i celočíselné řešení, jehož všechny složky jsou kladné.

Důkaz: Na základě předchozího lemmatu existuje řešení $X \in \mathbb{Q}^{|T|}$, jehož všechny složky jsou kladné. Definujme $Y : T \to \mathbb{N}$ předpisem

$$Y(t) = \lceil X(t) \rceil$$

Ukážeme, že Y je také řešením rovnice $(*)$. Nechť $s \in P$ je libovolné. Protože $\mathcal{N}$ je T-systém, platí $|{}^\bullet s| = |s^\bullet| = 1$. Označme $t_1 \in s^\bullet$ a $t_2 \in {}^\bullet s$ jediné přechody vedoucí z s a do s. Protože X je řešením rovnice $(*)$, platí

$$M(s) = M_0(s) + X(t_2) - X(t_1)$$

Přitom jistě $M_0(s) \in \mathbb{Z}$ a $M(s) \in \mathbb{Z}$, tedy $X(t_2) - X(t_1) \in \mathbb{Z}$ a existují $x_1, x_2 \in \mathbb{Z}$, $r \in \langle 0, 1)$ takové, že

$$X(t_1) = x_1 + r$$
$$X(t_2) = x_2 + r$$

Proto platí

$$X(t_2) - X(t_1) = x_2 - x_1 = (x_2+1) - (x_1+1) = Y(t_2) - Y(t_1)$$
$$M(s) = M_0(s) + Y(t_2) - Y(t_1) \text{ pro všechna } s \in P,\ t_1 \in s^\bullet \text{ a } t_2 \in {}^\bullet s$$
$$M = M_0 + \mathsf{N}Y$$

Věta (Dosažitelnost v živém T-systému)
Nechť $\mathcal{N} = (P, T, F)$ je živý T-systém s iniciálním markingem M_0 a incidenční maticí N. Marking M je dosažitelný z M_0 právě tehdy, když pro každý S-invariant I platí $I^{\mathrm{T}} M_0 = I^{\mathrm{T}} M$.

Důkaz: „$\Rightarrow$“ Platí obecně — alternativní nutná podmínka dosažitelnosti.

„$\Leftarrow$“ Protože $I^{\mathrm{T}} M_0 = I^{\mathrm{T}} M$ pro každý S-invariant I, má podle alternativní nutné podmínky dosažitelnosti soustava

$$M_0 + \mathsf{N}X = M$$

řešení v $\mathbb{Q}$. Podle předchozího lemmatu navíc existuje řešení Y, jehož všechny složky jsou přirozená čísla. Ukážeme, že existuje posloupnost $\sigma \in T^*$ proveditelná z M_0, $\vec{\sigma} = Y$ jejímž výsledkem je marking M. Indukcí k $n = \sum_{t \in T} Y(t)$. Je-li $n = 0$, potom $M = M_0$ z $(*)$.

Uvažme případ pro $n + 1$. Ukážeme, že existuje $t \in T$ proveditelný v M_0, $Y(t) > 0$. Položme

$$\langle Y \rangle = \{t \in T \mid Y(t) > 0\}$$
$$S_Y = \{s \in P \mid s \in {}^\bullet\langle Y \rangle \wedge M_0(s) = 0\}$$

Nechť $s \in S_Y$, tedy $M_0(s) = 0$. Pak existuje takový přechod $t \in \langle Y \rangle$, že $s \in t^\bullet$. Uvědomme si totiž, že pro Y platí $M = M_0 + \mathsf{N}Y$. Kdyby zmíněný přechod neexistoval, bylo by

$M(s) < 0$, což pro označkování není možné. Protože $\mathcal{N}$ je T-systém, je tento přechod jediný, pro nějž platí $s \in t^\bullet$.

Uvažme nyní cestu přes místa z S_Y. Taková cesta je nutně konečná, jinak by T-systém obsahoval cyklus prázdných míst — spor s živostí. Podle předchozího odstavce musí tato cesta začínat přechodem $t \in \langle Y \rangle$. Pokud by nezačínala přechodem, bylo by možné ji prodloužit. Pokud začíná přechodem, musí to být přechod z $\langle Y \rangle$.

Přechod t je v M_0 připraven. V opačném případě by existovalo místo $s \in {}^\bullet t$, $t \in \langle Y \rangle$, $M_0(s) = 0$, tedy $s \in S_Y$, a cestu by bylo možné prodloužit.

Označme M' označkování, pro nějž $M_0 \xrightarrow{t} M'$. Pro označkování M' a řešení Y' rovnice $(*)$ definované pro každé $u \in T$ předpisem

$$Y'(u) = \begin{cases} Y(u) - 1 & \text{pro } u = t \\ Y(u) & \text{jinak} \end{cases}$$

podle indukčního předkpokladu existuje taková posloupnost přechodů $\sigma' \in T^*$ proveditelná z M', že $\vec{\sigma}' = Y'$. Potom $\sigma = t\sigma'$ je hledaná posloupnost.

Definice (Free-choice systém)
Petriho síť $\mathcal{N} = (P, T, F)$ nazveme *free-choice systémem*, jestliže platí

$$F(s,t) = 1 \Rightarrow (\forall s' \in {}^\bullet t)(\forall t' \in s^\bullet) : F(s',t') = 1$$

Věta (Alternativní definice free-choice systémů)
Nechť $\mathcal{N} = (P, T, F)$ je Petriho síť. Následující podmínky jsou ekvivalentní

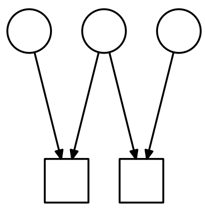
$$\mathcal{N} \text{ je free-choice systém} \tag{a}$$
$$\forall s, r \in P : s^\bullet \cap r^\bullet = \emptyset \vee s^\bullet = r^\bullet \tag{b}$$
$$\forall t, u \in T : {}^\bullet t \cap {}^\bullet u = \emptyset \vee {}^\bullet t = {}^\bullet u \tag{c}$$

Důkaz: Zřejmé.

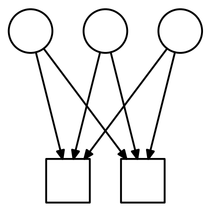
Definice (Cluster uzlu)
Nechť $\mathcal{N} = (P, T, F)$ je Petriho síť a x uzel jejího grafu. *Cluster* uzlu x je nejmenší množina $[x]$ uzlů grafu $\mathcal{N}$, která splňuje

$$x \in [x]$$
$$s \in P, s \in [x] \Rightarrow s^\bullet \subseteq [x]$$
$$t \in T, t \in [x] \Rightarrow {}^\bullet t \subseteq [x]$$

Poznámka (Clustery v obecné Petriho sítí a ve free-choice systému)
U free-choice systémů je kladeno omezení na hrany mezi místy a přechody, které z těchto míst berou — na hrany v clusterech. Rozdíl je znázorněn na následujícím obrázku.



cluster v obecné Petriho síti může vypadat například takto

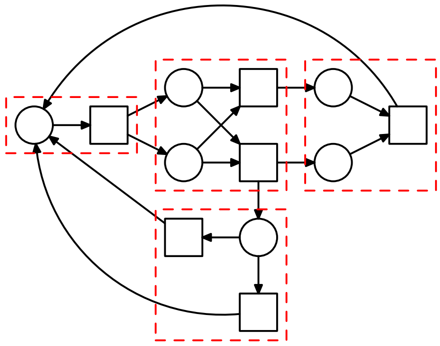


ve free-choice systému musí cluster se stejnými místy a přechody vypadat vždy takto

Věta (Rozklad na clustery)
Nechť $\mathcal{N} = (P, T, F)$ je Petriho síť. Množina všech clusterů tvoří rozklad na množině uzlů grafu $\mathcal{N}$.

Důkaz: Zřejmé.

Příklad (Rozklad na clustery)
Na následujícím obrázku je znázorněn free-choice systém a rozklad jeho grafu na clustery. Rozklad grafu na clustery lze ovšem provést i pro obecnou Petriho síť, i když tam není tento pojem tak důležitý.



Definice (Stabilní predikáty — sifony a pasti)
Nechť $\mathcal{N} = (P, T, F)$ je Petriho síť, $R \subseteq P$ množina míst. Množinu R nazveme *sifon*, jestliže ${}^\bullet R \subseteq R^\bullet$. Množinu R nazveme *past*, jestliže $R^\bullet \subseteq {}^\bullet R$.

Poznámka (Význam pojmů sifon a past vzhledem k označkování)
Z definic pojmů lze snadno dokázat následující tvrzení. Je-li sifon prázdný, prázdný již zůstane. Obsahuje-li past alespoň jeden token, již nikdy nebude prázdná.

Věta (Sifon v uváznuté síti)
Nechť $(\mathcal{N}, M_0)$ je uváznutá Petriho síť, tj. žádný přechod není připraven. Potom množina prázdných míst sítě $\mathcal{N}$ při označkování M_0 tvoří množinově neprázdný sifon.

Důkaz: Množinu prázdných míst v uváznuté síti $(\mathcal{N}, M_0)$ označme R. Protože je síť uváznutá a existuje $t \in T \neq \emptyset$, musí existovat prázdné místo $p \in P$, $t \in p^\bullet$. Tedy $R \neq \emptyset$. Ukážeme, že R je sifon. Nechť $t \in {}^\bullet R$. Protože síť je uváznutá, existuje místo $p \in P$, $t \in p^\bullet$, které je prázdné, tedy $p \in R$. Proto také $t \in R^\bullet$.

Věta (Postačující podmínka neuváznutí)
Jestliže každý neprázdný sifon sítě $(\mathcal{N}, M_0)$ obsahuje past, která je při M_0 označkovaná, pak v systému nemůže dojít k uváznutí.

Důkaz: Sporem předpokládejme, že $M_0 \xrightarrow{\sigma} M$, kde $\sigma \in T^*$ je proveditelná posloupnost přechodů z M_0, a síť $(\mathcal{N}, M)$ je uváznutá. Dle předchozí věty existuje množinově neprázdný sifon $R \subseteq P$, který není označkovaný. Pak R obsahuje past, která byla při M_0 označkovaná, ale při M již označkovaná není — spor.

Lemma (Nutná podmínka pro existenci mrtvého přechodu free-choice systému)
Nechť $\mathcal{N} = (P, T, F)$ je free-choice systém. Je-li $t \in T$ mrtvý v markingu M, pak existuje místo $s \in {}^\bullet t$ a označkování M' dosažitelné z M tak, že s je mrtvý v M'.

Důkaz: Mějme mrtvý přechod $t \in T$. Protože $\mathcal{N}$ je free-choice systém, jsou mrtvé i všechny přechody z množiny $({}^\bullet t)^\bullet$, protože berou tokeny ze stejné množiny míst. Sporem předpokládejme, že žádné místo z ${}^\bullet t$ není mrtvé. Protože všechny přechody, které berou tokeny z těchto míst jsou mrtvé, tokeny v těchto místech se mohou pouze kumulovat. Postupně lze tedy dosáhnout označkování, v němž jsou všechna tato místa neprázdná, což je spor — potom by byly mrtvé přechody připraveny.

Lemma (Nutná podmínka neživých free-choice systémů)
Každý neživý free-choice systém $(\mathcal{N}, M_0)$, $\mathcal{N} = (P, T, F)$, má takový neprázdný sifon $R \subseteq P$ a dosažitelný marking M, že R není označkovaný v M.

Důkaz: Protože $(\mathcal{N}, M_0)$ není živý, existuje $t \in T$ a dosažitelný marking M' tak, že t je mrtvý v M'. Podle předchozího lemmatu existuje marking M'' dosažitelný z M' a místo $p \in {}^\bullet t$, které je mrtvé v M''. Označme M marking dosažitelný z M'', který maximalizuje množinu mrtvých míst a tuto množinu označme $R \subseteq P$.

Množina R je neprázdná, protože $p \in R$. Nechť $t \in {}^\bullet R$. Potom t je mrtvý v M, jinak by množina R obsahovala i místa, která v M nejsou mrtvá. Podle předchozího lemmatu tedy $t \in p^\bullet$ pro nějaké místo $p \in P$ mrtvé v M. Protože p je mrtvé v M, platí $p \in R$ a tedy $t \in R^\bullet$ — množina R je sifon. Protože sifon R obsahuje pouze místa mrtvá v M, není R označkován v M. Je to tedy sifon požadovaných vlastností.

Věta (Postačující podmínka živosti free-choice systému)
Nechť $(\mathcal{N}, M_0)$ je free-choice systém. Jestliže každý neprázdný sifon R obsahuje past označkovanou v M_0, pak $(\mathcal{N}, M_0)$ je živá síť.

Důkaz: Obměna předchozího lemmatu.

Poznámka (Existence největšího sifonu a největší pasti)
Protože sjednocením sifonů je sifon a sjednocením pastí je past, je korektní hovořit o největším sifonu a největší pasti, protože oba existují.

Definice (Alokace, doména)
Nechť C je nějaká množina clusterů Petriho sítě $\mathcal{N} = (P, T, F)$ taková, že každý cluster z C obsahuje alespoň jeden přechod. *Alokací* rozumíme funkci $\alpha : C \to T$ takovou, že

$$\forall c \in C : \alpha(c) \in C$$

Potom C nazýváme *doménou* α.

Řekneme, že posloupnost přechodů σ *souhlasí s alokací* $\alpha : C \to T$, pokud pro všechny přechody $t \in T$ vyskytující se v σ platí $[t] \in C \Leftrightarrow \alpha([t]) = t$.

Lemma (Nekonečná posloupnost přechodů k alokaci)
Nechť α je alokace živého free-choice systému $\mathcal{N}$ s neprázdnou doménou C a počátečním označkováním M_0. Potom existuje nekonečná posloupnost přechodů proveditelná z M_0 taková, že σ souhlasí s α a alespoň jeden prvek z $\alpha(C)$ se v σ vyskytuje nekonečněkrát.

Důkaz: Nechť t je přechod připravený v nějakém označkování M free-choice systému. Potom jsou připraveny i všechny přechody $u \in [t]$, protože berou ze stejné množiny míst jako přechod t. Proto lze hovořit o připravenosti clusteru — je-li cluster připraven, lze provést libovolný jeho přechod.

Definujme posloupnost přechodů proveditelnou z M_0 v $\mathcal{N}$ induktivně takto:

$$\sigma_0 = \varepsilon$$
$$\sigma_{i+1} = \sigma_i \pi_i \alpha([t_i])$$
$$\sigma = \lim_{i \to \infty} \sigma_i$$

kde π_i je nejkratší posloupnost přechodů, která připraví nějaký cluster $[t_i] \in C$. Posloupnost σ souhlasí s alokací α, protože přechody z žádného π_i nenáleží kvůli minimalitě do žádného clusteru z C. Z každého připraveného clusteru $[t_i] \in C$ je proveden právě přechod $\alpha([t_i])$. Množina $\alpha(C)$ je konečná, ale posloupnost σ obsahuje nekonečně mnoho výskytů jejích prvků, nutně se tedy alespoň jeden z nich musí v σ vyskytovat nekonečněkrát.

Definice (Alokace bez cyklů vzhledem k množině míst)
Nechť R je nějaká množina míst Petriho sítě $\mathcal{N}$. Označme

$$C = \{[t] \mid t \in R^\bullet\}$$

Množina C je množina clusterů generovaná množinou míst R, z nichž každý obsahuje alespoň jeden přechod. Řekneme, že *alokace* α s doménou C *je bez cyklů* pro R, jestliže síť $\mathcal{N}$ neobsahuje cyklus tvořený pouze místy z R a přechody z $\alpha(C)$.

Lemma (Existence alokace bez cyklů v Petriho síti pro danou množinu míst)
Nechť $\mathcal{N} = (P, T, F)$ je free-choice systém, $R \subseteq P$ nějaká množina míst a nechť $Q \subseteq P$ je maximální past obsažená v R. Není vyloučeno, že $Q = \emptyset$. Označme

$$D = R \setminus Q$$
$$C = \{[t] \mid t \in D^\bullet\}$$

Pak existuje alokace s doménou C, která je bez cyklů pro D taková, že alokované přechody nedávají do pasti Q, tj.

$$\alpha(C) \cap {}^\bullet Q = \emptyset$$

Důkaz: Indukcí k $|R|$. Je-li $R = \emptyset$, potom i $D = Q = C = \emptyset$. Jediná alokace s doménou $C = \emptyset$ je prázdná alokace, která je jistě bez cyklů pro D a jistě platí $\alpha(C) \cap {}^\bullet Q = \emptyset$.

Nechť $|R| > 0$. Je-li R past, potom $Q = R$ a $D = C = \emptyset$. Zbytek je totožný se základním krokem indukce.

Nechť tedy R není past. Potom existuje přechod $t \in T$ takový, že $t \in R^\bullet$ a $t \notin {}^\bullet R$. Označme $R' = R \setminus {}^\bullet t$. Jistě platí $R' \subset R$, $|R'| < |R|$. Nechť Q' je maximální past v R' a označme

$$D' = R' \setminus Q'$$
$$C' = \{[u] \mid u \in D'^\bullet\}$$

Podle indukčního předpokladu existuje alokace $\alpha' : C' \to T$, která je bez cyklů pro D' taková, že $\alpha'(C') \cap Q' = \emptyset$.

Protože přechod t porušuje vlastnost pasti pro množinu R, nemůže žádné místo z ${}^\bullet t$ patřit do pasti Q a tedy $Q = Q'$. Potom $D = D' \cup {}^\bullet t$ a $C = \cup\{[t]\}$. Definujme $\alpha : C \to T$

předpisem

$$\alpha(c) = \begin{cases} \alpha'(c) & \text{pro } c \in C' \\ t & \text{pro } c = [t] \end{cases}$$

Pokud by v D existoval přechod přes alokované přechody, musel by obsahovat přechod t. V D' totiž takový cyklus nebyl a D obsahuje navíc pouze místa z ${}^\bullet t$ a t je jediný alokovaný přechod, který vede z míst z ${}^\bullet t$. Jenže t nevede ani do R, jistě tedy nevede ani do D. Uvažovaný cyklus tedy neexistuje. Přechod t navíc jistě nevede ani do Q, tj. $t \notin {}^\bullet Q = {}^\bullet Q'$, přitom je to jediný přechod, který je v $\alpha(C)$ navíc oproti $\alpha'(C')$. Proto $\alpha(C) \cap {}^\bullet Q = \emptyset$.

Věta (Nutná podmínka živosti free-choice systému)
Každý neprázdný sifon živého free-choice systému obsahuje iniciálně označkovanou past.

Důkaz: Nechť $(\mathcal{N}, M_0)$ je živý free-choice systém. Nechť $R \neq \emptyset$ je sifon a nechť Q je maximální past obsažená v R. Musíme ukázat, že $M_0(Q) > 0$. Předně si uvědomme, že z obměny nutné podmínky neživosti free-choice systémů plyne, že $M_0(R) > 0$. Označme $D = R \setminus Q$.

Pokud $D^\bullet = \emptyset$, potom je D past obsažená v R. Protože $R = D \cup Q$ a D i Q jsou pasti, je i R past. Z maximality Q potom plyne, že $Q = R$ a $D = \emptyset$. Potom z výše uvedeného $M_0(Q) = M_0(R) > 0$.

Nechť tedy $D^\bullet \neq \emptyset$. Položme $C = \{[t] \mid t \in D^\bullet\}$. Podle předchozího lemmatu existuje alokace $\alpha : C \to T$, která je bez cyklů pro D a splňuje $\alpha(C) \cap {}^\bullet Q = \emptyset$. Podle lemmatu o nekonečné posloupnosti přechodů k alokaci existuje k alokaci α nekonečná posloupnost přechodů $\sigma \in T^*$, která souhlasí s α a alespoň jeden přechod z $\alpha(C)$ je v ní vyskytuje nekonečněkrát. Dokážeme, že platí

$$\mathcal{A}(\sigma) \cap {}^\bullet Q \subseteq Q^\bullet \qquad (i)$$

$$Q^\bullet \cap \mathcal{A}(\sigma) \neq \emptyset \qquad (ii)$$

Z podmínky (i) plyne, že se Q nemůže označkovat během posloupnosti přechodů σ. Z podmínky (ii) plyne, že nějaký přechod z posloupnosti σ bere z Q. Aby to bylo možné, musí být $M_0(Q) > 0$.

Důkaz (i) sporem. Nechť existuje $t \in \mathcal{A}(\sigma)$ takový, že $t \in {}^\bullet Q$, ale $t \notin Q^\bullet$. Protože R je sifon a $Q \subseteq R$, přechod t bere z nějakého místa $s \in R$. Protože $t \notin Q^\bullet$, musí být $s \in D$, tedy $[t] \in C$. Přechod t se navíc vyskytuje v σ, takže to musí být alokovaný přechod. Alokace byla ovšem zvolena tak, že $\alpha(C) \cap {}^\bullet Q = \emptyset$, takže musí platit $t \notin {}^\bullet Q$ — spor.

Důkaz (ii). Definujme relaci $\prec$ na $\alpha(C)$ takto: $t \prec t'$, jestliže existuje cesta z t do t' přes uzly z $D \cup \alpha(C)$. Cesta může být tvořena pouze jediným uzlem $t = t'$, relace je tedy reflexivní. Protože graf $D \cup \alpha(C)$ neobsahuje cykly, je relace $\prec$ uspořádání. Nechť u je některý minimální prvek v tomto uspořádání takový, že u se vyskytuje v σ nekonečněkrát.

Přechod u bere z nějakého místa $s \in D$, protože podle definice C je $u = \alpha([t])$ pro nějaké $t \in D^\bullet$. Proto se v σ musí nekonečněkrát vyskytovat přechod v, který dává do s, aby byl uschopněn přechod u (přechodů je konečně mnoho). Protože v dává do sifonu R, musí z něj také brát.

Tedy v bere z $Q \cup D = R$. Kdyby v bral z D, dostaneme spor s minimalitou u v uspořádání $\prec$. Proto v bere z Q. Máme tedy přechod vyskytující se v σ, $v \in \mathcal{A}(\sigma)$, který bere z Q, $v \in Q^\bullet$. To je hledaný přechod pro důkaz (ii).

Věta (Commonerova věta)
Free-choice systém je živý právě tehdy, když každý jeho neprázdný sifon obsahuje iniciálně označkovanou past.

Důkaz: Viz nutná a postačující podmínka živosti free-choice systému.

Důsledek (Složitost problému živosti a neživosti)
Problém neživosti free-choice systémů je NP-úplný. Z toho plyne, že problém živosti je co-NP-úplný.

Důkaz: Redukcí ze SAT. Pro danou formuli φ sestrojíme free-choice systém tak, aby φ měla splňující valuaci právě tehdy, když free-choice systém bude neživý.

Rejstřík