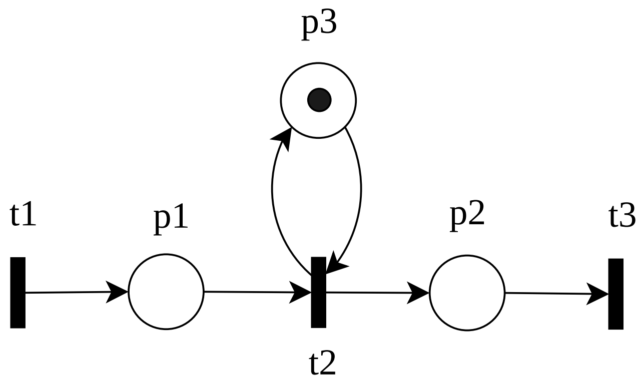
Analýza Petriho sítí

1. Základní pojmy

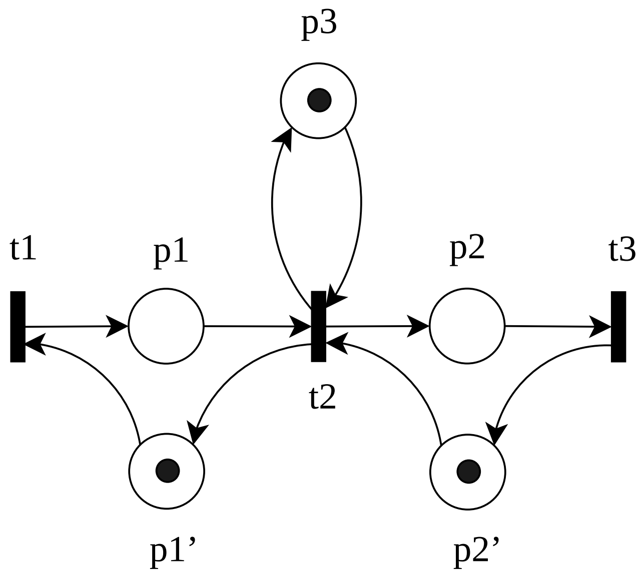
- Základní problémy analýzy
  - bezpečnost (safeness)
  - omezenost (boundness)
  - konzervativnost (conservation)
  - živost (liveness)

- **Definice 1**: Místo $p \in P$ Petriho sítě $N = (P, T, F, W, K, M_0)$ s počátečním značení M_0 je *bezpečné* (safe), jestliže pro všechna značení $M \in [M_0\rangle$ je $M(p) \leq 1$. Petriho síť je *bezpečná*, je-li každé její místo bezpečné.

❖ **Příklad 1**:



síť, která není bezpečná



odpovídající bezpečná síť

Neobsahuje-li graf Petriho sítě násobné hrany, může být transformován na bezpečnou síť následujícím postupem.

Postup:

1. K místu p, které má bý bezpečné přidej komplementární místo p'.
2. Modifikuj incidující přechody podle algoritmu komplementace sítě.

❖ **Definice 2**: Místo $p \in P$ Petriho sítě $N = (P, T, F, W, K, M_0)$ se nazývá *k-bezpečné*, jestliže pro všechna značení $M \in [M_0\rangle$ je $M(p) \leq k$. Je-li místo p' k-bezpečné pro nějaké k, nazývá se *omezené* (bounded). Petriho síť, jejíž všechna místa jsou omezená se nazývá *omezená Petriho síť*.

Omezenost sítě $\Rightarrow$ konečný stavový prostor sítě $\Rightarrow$ ekvivalenci sítě s konečnými automaty

❖ **Definice 3**: Petriho síť $N = (P, T, F, W, K, M_0)$ je *striktně konzervativní*, jestliže platí:

$$\boxed{\forall M \in [M_0\rangle : \sum_{p \in P} M(p) = \sum_{p \in P} M_0(p)}$$

Konzervativnost vzhledem k váhovému vektoru $\underline{w} = (w_1, \ldots, w_n), w_i \geq 0$

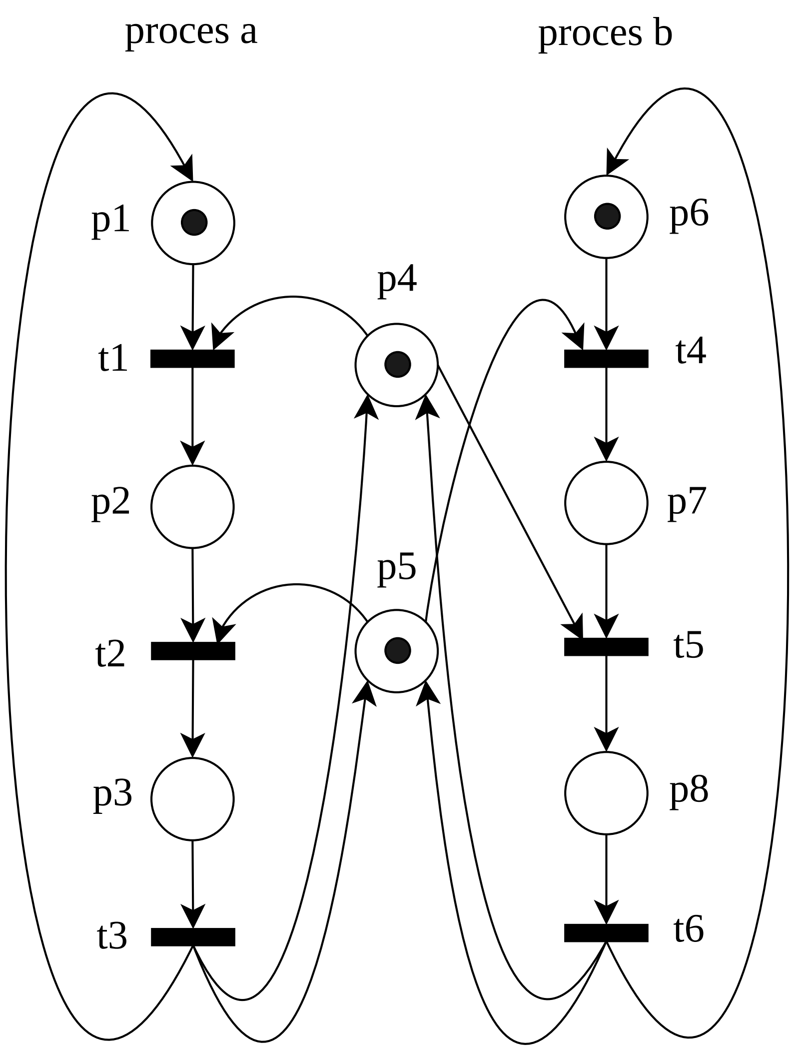
$$\boxed{\forall M \in [M_0\rangle : \sum_{i=1}^{n} w_i.M(p_i) = \sum_{i=1}^{n} w_i.M_0(p_i)}$$

❖ **Definice 4**: Nechť $N = (P, T, F, W, K, M_0)$ je Petriho síť a $t \in T$.

1. t se nazývá *živý přechod*, jestliže pro každé značení $M \in [M_0\rangle$ existuje značení $M' \in [M\rangle$ takové, že t je proveditelný při značení M'.
2. Síť N se nazývá *živou*, je-li každý její přechod živý.

Aplikace: živost x deadlock

❖ **Příklad 2**:



Proveditelné posloupnosti přechodů:

$t_1 t_2 t_3 t_4 t_5 t_6 \ldots$

$t_4 t_5 t_6 t_1 t_2 t_3 \ldots$

Uvažujme však posloupnost přechodů, která začíná $t_1 t_4 \ldots$

- **Definice 5**: Značení M Petriho sítě $N = (P, T, F, W, K, M_0)$ je *živé*, jestliže pro všechna $t \in T$ existuje $M' \in [M\rangle$ takové, že přechod t je proveditelný při značení M'.

- **Věta 1**: Petriho síť je *živá*, právě když všechna značení z $[M_0\rangle$ jsou živá.

- **Definice 6**: (Problém dosažitelnosti - Reachability problem)
Je dána Petriho síť N s počátečním značením M_0 a značení M. Je $M \in [M_0\rangle$?

- **Definice 7**: (Problém pokrytí - Coverability problem)
Je dána Petriho síť N s počátečním značením M_0 a značení M. Existuje $M' \in [M_0\rangle$ takové, že $M' \geq M$?

- **Další problémy analýzy**:
  - posloupnosti přechodů (firing sequences)
  - ekvivalence sítí
  - inkluse sítí

2. Techniky analýzy Petriho sítí

❖ **Strom dosažitelných značení (The Reachability Tree)**:
Strom dosažitelných značení je konečnou reprezentací množiny dosažitelných značení $[M_0\rangle$. Strom dosažitelných značení je kořenový orientovaný strom, jehož kořenem je počáteční značení M_0 a vrcholy tvoří vektory z $(\mathbb{N} \cup \{\omega\})^n, n = |P|$. Kde ω značí supremum množiny $\mathbb{N}$ s vlastnostmi:

1. $\forall n \in \mathbb{N} \colon n < \omega$
2. $\forall m \in \mathbb{N} \cup \{\omega\} \colon m + \omega = \omega + m = \omega - m = \omega$

❖ **Algoritmus konstrukce stromu dosažitelných značení**:
Nechť x je vrchol (uzel) stromu. $M_x : P \rightarrow \mathbb{N} \cup \{\omega\}$ bude ohodnocení vrcholu x;
$M_{\text{kořen}} = M_0$

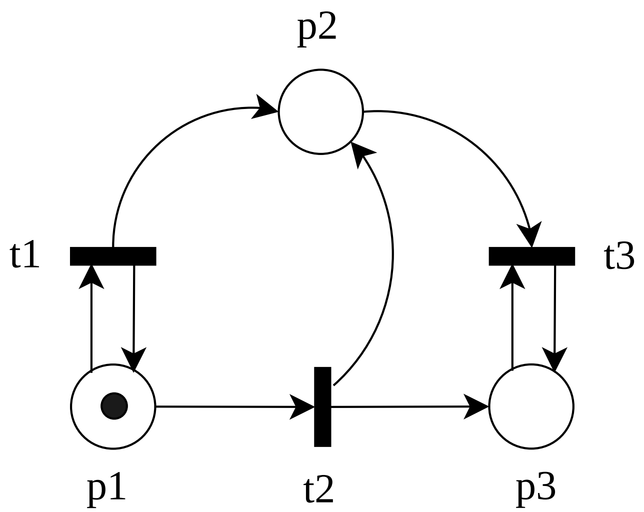
Rozlišíme 4 typy vrcholů: *čelní* , *koncový*, *duplikovaný*, *vnitřní*

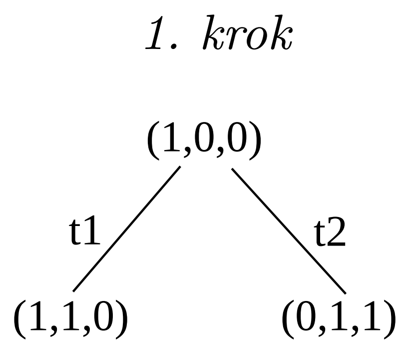
Nechť x je právě zpracovávaný čelní vrchol.

1. Jestliže $\exists y, y \neq x$, y není čelní a $M_x = M_y$, pak x se stává *duplikovaným vrcholem*
2. Jestliže $\delta(M_x, t)$ není definováno pro žádné $t \in T$, pak x se stává *koncovým vrcholem*
3. Je-li jistý přechod $t \in T$ M_x-proveditelný, vytvoříme nový vrchol z s ohodnocením M_z:
   $\forall p \in P$:
   (a) Je-li $M_x(p) = \omega$, pak $M_z(p) = \omega$
   (b) Existuje-li na cestě z kořene do vrcholu x vrchol y takový, že $M_y \leq \delta(M_x, t)$ a jestliže $M_y(p) < \delta(M_x, t)(p)$, pak $M_z(p) = \omega$
   (c) Jinak $M_z(p) = \delta(M_x, t)(p)$

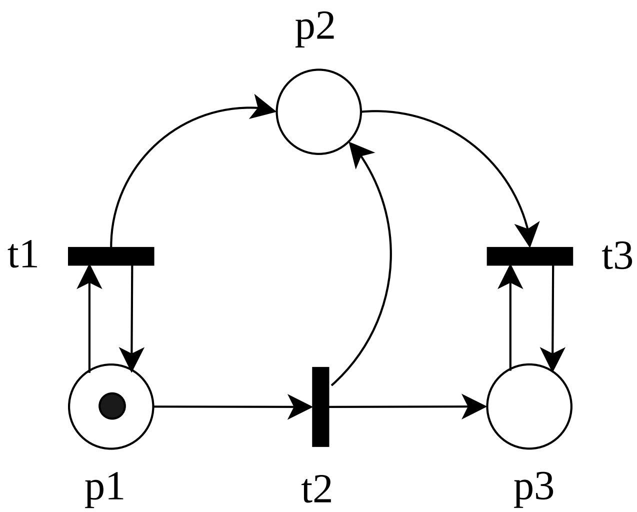
   Hrana $< x, z >$ je označena přechodem t a vrchol z se stává čelním vrcholem.

- **Příklad 3**: Konstrukce stromu dosažitelných značení

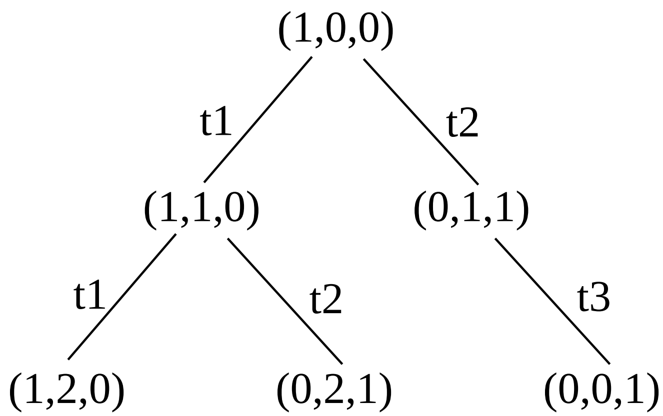




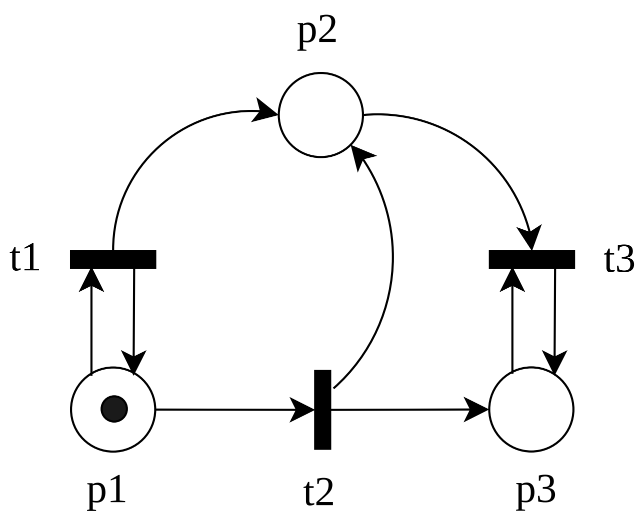
❖ **Příklad 3**: (pokračování)



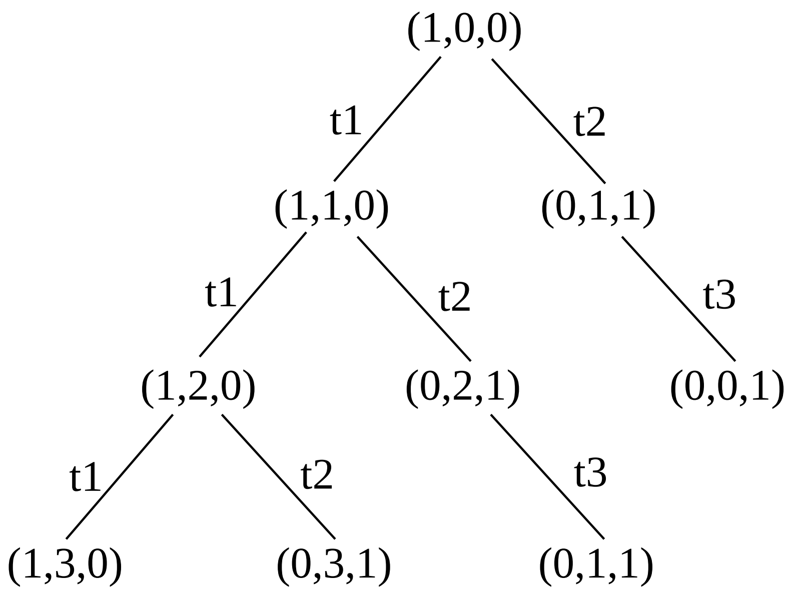
2. krok



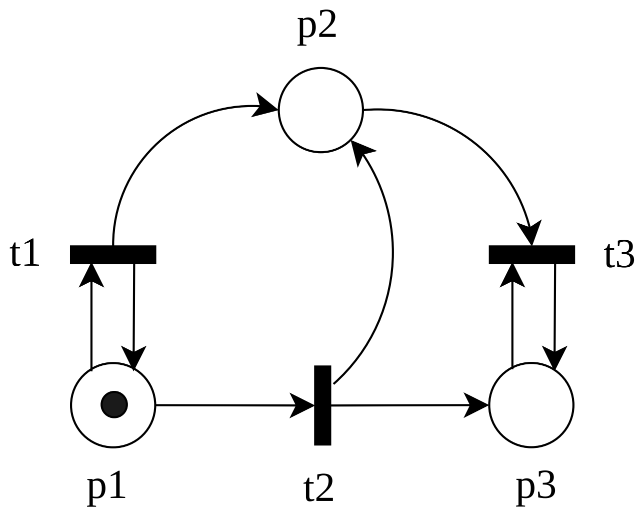
❖ **Příklad 3**: (pokračování)

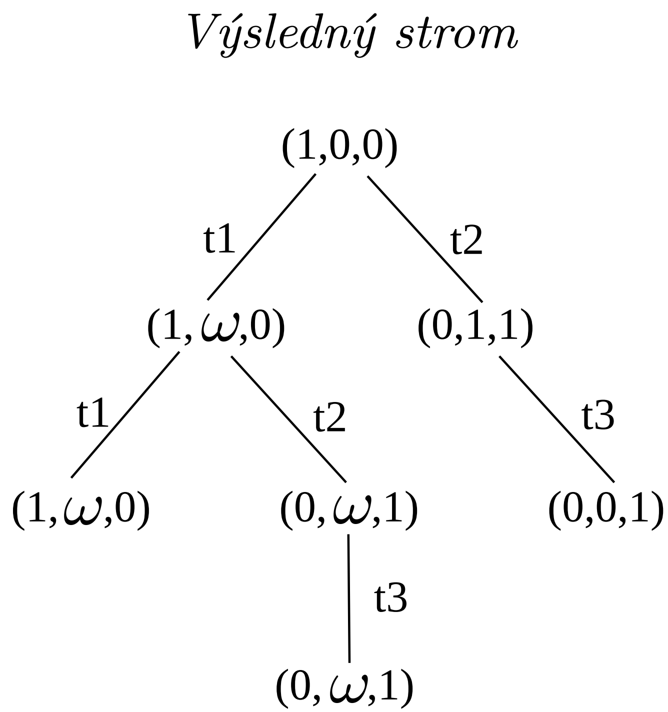


3. krok



❖ **Příklad 3**: (pokračování)





❖ **Využití stromu dosažitelných značení pro analýzu Petriho sítí**:

- bezpečnost
- omezenost
- konzervativnost
- pokrytí
- živost
- dosažitelnost

Poznámka:
Alternativní reprezentace stavového prostoru Petriho sítí: Graf pokrytí.

3. Invarianty

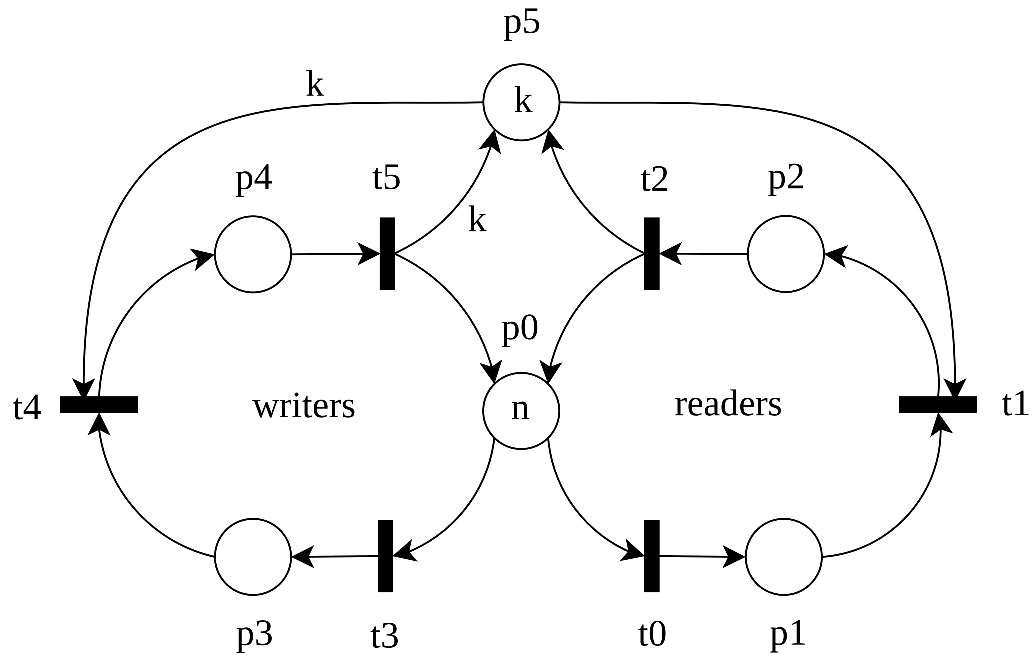
Nyní se budeme zabývat metodami analýzy, které jsou založeny na lineární algebraické reprezentaci Petriho sítě. Budou nás zajímat množiny míst, které nemění svoje značky v průběhu provádění přechodů. Množiny takových míst se nazývají P-invarianty.
T-invarianty udávají kolikrát je třeba, počínaje určitým značením, provést každý přechod sítě, abychom získali nazpět toto značení (reprodukovali dané značení sítě).

❖ **Příklad aplikace P-invariantů Petriho sítě**:
Uvažujme model kooperace procesů nazývaný termínem *Readers-Writers*:
n procesů (například v operačním systému) má přístup ke společné vyrovnávací paměti (bufferu), aby do ní určitá data zapsal nebo z ní data přečetl.

Předpokládejme, že se tyto procesy mají chovat podle následujících pravidel:

1. Jestliže žádný z procesů nezapisuje do vyrovnávací paměti, pak nejvýše k procesů, $k \leq n$, může simultánně číst z vyrovnávací paměti.
2. Přístup libovolného procesu, který chce zapisovat do vyrovnávací paměti lze povolit pouze tehdy, jestliže žádný z procesů ani nečte, ani nezapisuje.

❖ **Příklad 4**: Readers-Writers



$$\underline{N} = \begin{array}{c|cccccc|cc|c}
 & t_0 & t_1 & t_2 & t_3 & t_4 & t_5 & i_1 & i_2 & M_0 \\
\hline
p_0 & -1 & & 1 & -1 & & 1 & 1 & 0 & n \\
p_1 & 1 & -1 & & & & & 1 & 0 & \\
p_2 & & 1 & -1 & & & & 1 & 1 & \\
p_3 & & & & 1 & -1 & & 1 & 0 & \\
p_4 & & & & & 1 & -1 & 1 & k & \\
p_5 & & -1 & 1 & & -k & k & 0 & 1 & k
\end{array}$$

$$\underline{N}^T.i = \mathbf{0}$$

❖ **Interpretace invariantů**:

$\underline{i_1}$:

$$\forall M \in [M_0\rangle : \quad \sum_{i=0}^{4} M(p_i) = \sum_{i=0}^{4} M_0(p_i) = n$$

tj. počet procesů je konstantní (žádné procesy se neztrácejí, ani nepřibývají) a každý proces je v jednom ze stavů $p_0, \ldots, p_4$

$\underline{i_2}$:

$$\forall M \in [M_0\rangle : \quad M(p_2) + k.M(p_4) + M(p_5) = M_0(p_2) + k.M_0(p_4) + M_0(p_5) = k$$

- p_4 obsahuje nejvýše jednu značku (existuje nejvýše jeden zapisující proces)
- obsahuje-li p_4 značku, pak $M(p_2) = M(p_5) = 0$ (jakmile některý proces zapisuje, pak žádný nečte)
- p_2 může obsahovat maximálně k značek (maximálně k procesů může číst simultánně z vyrovnávací paměti)
- jestliže $M(p_4) = 0$ (žádný z procesů nezapisuje), pak p_2 může obsahovat k značek a pak je synchronizační místo p_5 prázdné

❖ **S využitím invariantů i_1 a i_2 lze dokázat následující tvrzení**:
Petriho síť modelu Readers-Writers s uvedeným počátečním značením a s kapacitami míst

$$K(p_i) = n \quad \text{pro} \quad i \in \{0, 1, 3\}$$
$$K(p_4) = 1 \;\text{ a }\; K(p_2) = K(p_5) = k$$

je živá.

4. P-invarianty

P-invarianty získáme řešením soustavy algebraických rovnic tvaru $\underline{N}^T.x = \mathbf{0}$ ($\underline{N}^T$ je transponovaná matice Petriho sítě N).

❖ **Definice 8**: Nechť $N = (P, T, F, W, K, M_0)$ je Petriho síť. Vektor míst $i\colon P \to \mathbb{Z}$ nazýváme *P-invariantem* Petriho sítě N, jestliže platí $\underline{N}^T.i = \mathbf{0}$. Jestliže $i(p) \in \{0, 1\}$ pro všechna $p \in P$, pak i nazýváme *binárním P-invariantem* sítě N.

❖ **Lemma 1**: Nechť i_1 a i_2 jsou P-invarianty sítě N a nechť $z \in \mathbb{Z}$. Pak $i_1 + i_2$ a $z.i_1$ jsou také P-invarianty sítě N.

❖ **Věta 2**: Nechť N je Petriho síť s počátečním značením M_0. Pak pro každý P-invariant i sítě N a pro každé dosažitelné značení $M \in [M_0\rangle$ platí $M.i = M_0.i$.

Důkaz:
Nechť $M_1, M_2 \in [M_0\rangle$ a nechť $t \in T$ tak, že $M_1[t\rangle M_2$. Pak platí $M_2 = M_1 + \underline{t}$ a $\underline{t}.i = \mathbf{0}$ (protože i je invariant). Proto $M_2.i = (M_1 + \underline{t}).i = M_1.i + \underline{t}.i = M_1.i$.

❖ **Věta 3**: Nechť N je živá Petriho síť a nechť $i\colon P \rightarrow \mathbb{Z}$ je vektor míst, pro který platí $\forall M \in [M_0\rangle\colon M.i = M_0.i$. Pak i je P-invariant.

Důkaz:
Stačí dokázat, že pro každý přechod $t \in T$ platí $\underline{t}.i = \mathbf{0}$. Nechť tedy $t \in T$ a $M \in [M_0\rangle$ a nechť t je M-proveditelný. Pak $M[t\rangle M'$, $M.i = M'.i = (M + \underline{t}).i = M.i + \underline{t}.i$. Tudíž $\underline{t}.i = \mathbf{0}$.

❖ **Definice 9**: Petriho síť N je *pokryta P-invarianty*, jestliže pro každé místo $p \in P$ existuje kladný P-invariant i sítě N takový, že jeho složka $i(p) > 0$.

❖ **Věta 4**: Je-li Petriho síť N pokryta P-invarianty, pak existuje P-invariant i sítě N, pro který $i(p) > 0$ pro všechna $p \in P$.

Důkaz:
Podle předpokladu, pro každé $p \in P$ existuje invariant i_p sítě N, pro který $i(p) > 0$. Podle Lemmy 1 je invariant

$$i = \sum_{p \in P} i_p$$

Tento invariant splňuje podmínku $i(p) > 0$ pro všechna $p \in P$.

❖ **Věta 5**: Nechť N je Petriho síť s konečným počátečním značením M_0. Je-li N pokryta P-invarianty, pak je *omezená*.

Důkaz:
Nechť $q \in P$ je libovolné místo sítě N a i je P-invariant, pro který $i(q) > 0$ a nechť $M \in [M_0\rangle$. Poněvadž (podle Věty 2)

$$M(q).i(q) \leq \sum_{p \in P} M(p).i(p) = M.i = M_0.i$$

dostáváme

$$M(q) \leq M_0 \frac{i}{i(q)}$$

Poznámka:
Opačné tvrzení k Větě 5, tj. je-li síť omezená, pak je pokryta P-invarianty, obecně neplatí.

5. T-invarianty

Nyní se budeme zabývat řešením soustavy rovnic tvaru $\underline{N}.x = \mathbf{0}$. Předpokládejme, že vektor $u\colon T \rightarrow \mathbb{N}$ je takovým řešením. Jestliže je možné, počínaje určitým značením M, provést každý přechod t přesně $u(t)$-krát, pak opět získáme značení M.

❖ **Věta 6**: Nechť $N = (P, T, F, W, K, M_0)$ je Petriho síť a nechť $M_0, M_1, \ldots, M_k \in [M_0\rangle$ a $t_1, t_2, \ldots, t_k \in T$, přičemž

$$M_0[t_1\rangle M_1[t_2\rangle \ldots [t_k\rangle M_k$$

Nechť vektor $u\colon T \rightarrow \mathbb{N}$ je definován takto:

$$u(t) = |\{i\colon t_i = t \ \wedge \ 1 \leq i \leq k\}|$$

Pak $M_0 + \underline{N}.u = M_k$.

Poznámka:
Opak Věty 6 obecně neplatí, protože pro provedení výpočetní posloupnosti odpovídající vektoru u je třeba dostatečného počtu značek a dostatečné volné kapacity míst.

❖ **Věta 7**: Nechť N je Petriho síť $N = (P, T, F, W, K, M_0)$, pro kterou $K(p) = \omega$ pro všechna $p \in P$. Nechť $M, M' \colon P \rightarrow \mathbb{Z}$ jsou dvě značení a nechť $u \colon T \rightarrow \mathbb{N}$ je vektor. Pak $M + \underline{N}.u = M'$ tehdy a jen tehdy, jestliže existuje $M'' \colon P \rightarrow \mathbb{N}$ a přechody $t_1, \ldots, t_k \in T$ takové, že $(M + M'')[t_1\rangle \ldots [t_k\rangle(M' + M'')$ a pro všechna $t \in T$ je $u(t) = |\{i \colon t_i = t \ \wedge \ 1 \leq i \leq k\}|$.

❖ **Definice 10**: Značení M Petriho sítě N se nazývá *reprodukovatelné*, jestliže existuje $M' \neq M$ tak, že $M' \in [M\rangle$ a zároveň $M \in [M'\rangle$.

❖ **Lemma 2**: Nechť $N = (P, T, F, W, K, M_0)$ je Petriho síť, pro kterou $\forall p \in P\colon K(p) = \omega$. Je-li značení M sítě N reprodukovatelné, pak je rovněž reprodukovatelné značení $M + M'$ pro libovolné značení M' sítě N.

❖ **Definice 11**: Nechť $N = (P, T, F, W, K, M_0)$ je Petriho síť. Vektor $i\colon T \rightarrow \mathbb{Z}$ se nazývá *T-invariant* sítě N, jestliže $\underline{N}.i = \mathbf{0}$.

❖ **Lemma 3**: Jestliže i_1 a i_2 jsou T-invarianty Petriho sítě N a $z \in \mathbb{Z}$, pak $i_1 + i_2$ a $z.i_1$ jsou také T-invarianty sítě N.

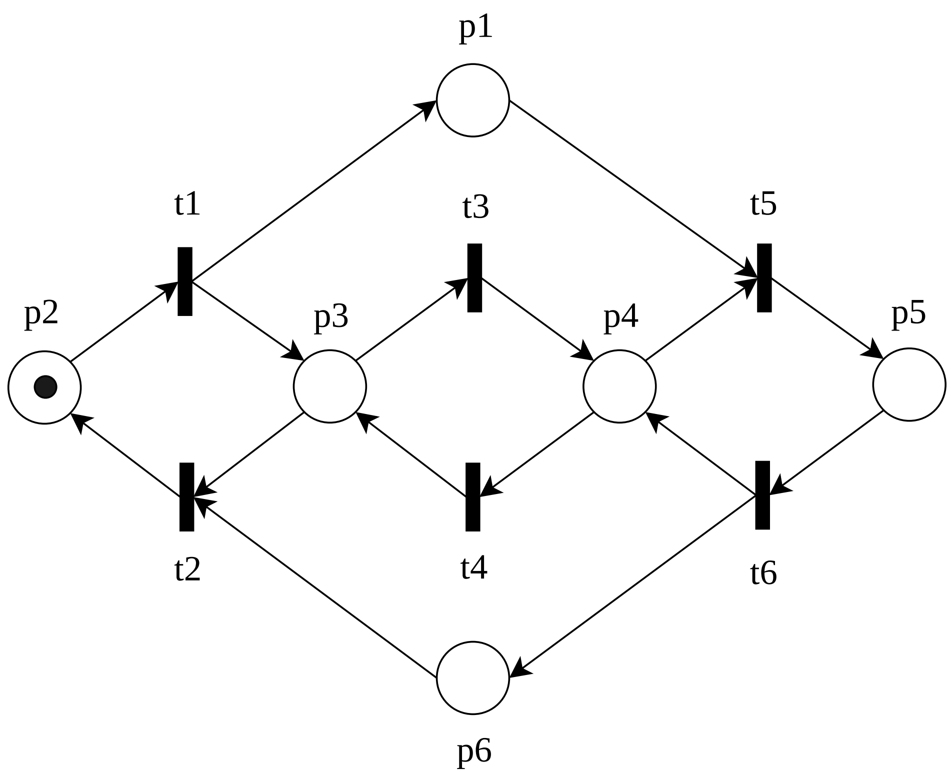
❖ **Věta 8**: Nechť N je Petriho síť s neomezenými kapacitami všech míst. Síti N přísluší nenulový T-invariant i právě tehdy, má-li reprodukovatelné značení.

Důkaz:
$\underline{N}.i = \mathbf{0} \Leftrightarrow \mathbf{0} + \underline{N}.i = \mathbf{0} \Leftrightarrow \exists t_1, t_2, \ldots, t_k \in T$ a M'' takové, že
$(\mathbf{0} + M'')[t_1\rangle \ldots [t_k\rangle(\mathbf{0} + M'')$ a $\forall t \in T : i(t) = |\{i : t_i = t \ \wedge \ 1 \leq i \leq k\}|$ (Věta 7)

❖ **Definice 12**: T-invariant i Petriho sítě N se nazývá *realizovatelný*, jestliže existuje $M \in [M_0\rangle$ a výpočetní posloupnost $M[t_1\rangle \ldots [t_k\rangle M_k$ taková, že
$\forall t \in T : i(t) = |\{i : t_i = t \ \wedge \ 1 \leq i \leq k\}|$.

❖ **Příklad 5**: Petriho síť s nerealizovatelným invariantem

Ne každý kladný T-invariant i je realizovatelný. Dokonce ani nepostačuje, aby N byla živá a omezená a každé značení bylo reprodukovatelné a invariant i nebyl součtem jiných kladných T-invariantů.



T-invariant i definovaný zobrazením $i(t_1) = i(t_2) = i(t_5) = i(t_6) = 1$ a $i(t_3) = i(t_4) = 0$ není realizovatelný.

❖ **Definice 13**: Petriho síť N je pokryta T-invarianty, jestliže pro každý přechod t sítě N existuje kladný T-invariant i sítě N takový, že $i(t) > 0$.

❖ **Věta 9**: Je-li Petriho síť N pokryta T-invarianty, pak existuje invariant i sítě N takový, že $i(t) > 0$ pro všechny přechody $t \in T$.

❖ **Věta 10**: Každá živá a omezená Petriho síť je pokryta T-invarianty.

Poznámka:
Věta 10 představuje pouze nutnou podmínku pro živost omezené Petriho sítě. Není-li daná Petriho síť pokryta T-invarianty, pak není živá nebo není omezená.