Chapter 12: Modeling and Analysis of Distributed Applications

Petri-Nets

- Petri-nets are abstract formal models capturing the flow of information and objects in a way which makes it possible to describe distributed systems and processes at different levels of abstraction in a unified language.

- Petri-nets have the name from their inventor Carl Adam Petri, who introduced this formalism in his PhD-thesis 1962.
Processing of complaints: informal description.

- Customer inquiring
- Complaint registration
- Complaint processing
- Archive
Complaints processing: formal Petri-net orchestration.\(^1\)

---

Complaints processing: more than one complaint
Complaints processing: how to distinguish complaints
Complaints processing: keeping things together
Petri-nets model system dynamics.

- Activities trigger state transitions,
- activities impose control structures,
- applicable for modelling discrete systems.

Benefits

- Uniform language,
- can be used to model sequential, causal independent (concurrent, parallel, nondeterministic) and monitored exclusive activities.
- open for formal analysis, verification and simulation,
- graphical intuitive representation.

The name Petri-net denotes a variety of different versions of nets - we will discuss the special case of System Nets following the naming introduced by W. Reisig.
Petri-nets model system dynamics.

- Activities trigger state transitions,
- activities impose control structures,
- applicable for modelling discrete systems.

Benefits

- Uniform language,
- can be used to model sequential, causal independent (concurrent, parallel, nondeterministic) and monitored exclusive activities.
- open for formal analysis, verification and simulation,
- graphical intuitive representation.

The name Petri-net denotes a variety of different versions of nets - we will discuss the special case of System Nets following the naming introduced by W. Reisig.
Petri-nets

Petri-nets model system dynamics.

- Activities trigger state transitions,
- Activities impose control structures,
- Applicable for modelling discrete systems.

Benefits

- Uniform language,
- Can be used to model sequential, causal independent (concurrent, parallel, nondeterministic) and monitored exclusive activities.
- Open for formal analysis, verification and simulation,
- Graphical intuitive representation.

The name *Petri-net* denotes a variety of different versions of nets - we will discuss the special case of *System Nets* following the naming introduced by W. Reisig.
## Section 12.1 Elementary System Nets

### Basic elements of an elementary System Net (eS-Net)

- **System states** are represented by *places*, graphically circles or ovals.
- A place may be marked by an arbitrary number of *tokens* graphically represented by black dots.
- **System dynamics** is represented by *transitions*, graphically rectangles.
- *Transitions* represent activities (events) and the causalities between such activities (events) are represented by edges.
- *Multiplicities* represent the consumption, respectively creation of resources which are caused by the occurrence of activities.
Section 12.1 Elementary System Nets

Basic elements of an elementary System Net (eS-Net)

- System states are represented by *places*, graphically circles or ovals.
- A place may be marked by an arbitrary number of *tokens* graphically represented by black dots.
- System dynamics is represented by *transitions*, graphically rectangles.
- *Transitions* represent activities (events) and the causalities between such activities (events) are represented by edges.
- *Multiplicities* represent the consumption, respectively creation of resources which are caused by the *occurrence* of activities.
Basic elements of an elementary System Net (eS-Net)

- System states are represented by places, graphically circles or ovals.
- A place may be marked by an arbitrary number of tokens graphically represented by black dots.
- System dynamics is represented by transitions, graphically rectangles.
- Transitions represent activities (events) and the causalities between such activities (events) are represented by edges.
- Multiplicities represent the consumption, respectively creation of resources which are caused by the occurrence of activities.
3-Philosopher-Problem

$b_j$: philosopher starts eating; $e_j$: philosopher stops eating;
$i_j$: philosopher is eating; $g_j$: fork on the desk;
$1 \leq j \leq 3$. 

![Diagram of the 3-Philosopher-Problem with Petri-Nets notation showing transitions between states for philosophers and forks.](image-url)
A transition *may* occur when certain conditions with respect to the markings of its directly connected places are fulfilled; the *occurrence* of a transition - also called its *firing* - effects the markings of its directly connected edges, i.e. has local effects.

The *surrounding* of a transition $t$ is given by $t$ and all its directly connected places:

$s_1, \ldots, s_k$ are called *preconditions* (*pre-places*), $s_{k+1}, \ldots, s_n$ *postconditions* (*post-places*).

A place which is pre- and post-place at the same time is called a *loop*. 
A transition *may* occur when certain conditions with respect to the markings of its directly connected places are fulfilled; the *occurrence* of a transition - also called its *firing* - effects the markings of its directly connected edges, i.e. has local effects.

The *surrounding* of a transition $t$ is given by $t$ and all its directly connected places:

$s_1,\ldots, s_k$ are called *preconditions (pre-places)*, $s_{k+1},\ldots, s_n$ *postconditions (post-places)*.

A place which is pre- and post-place at the same time is called a *loop*. 
A transition may occur when certain conditions with respect to the markings of its directly connected places are fulfilled; the occurrence of a transition - also called its firing - effects the markings of its directly connected edges, i.e. has local effects.

The surrounding of a transition $t$ is given by $t$ and all its directly connected places:

$s_1, \ldots, s_k$ are called preconditions (pre-places), $s_{k+1}, \ldots, s_n$ postconditions (post-places).

A place which is pre- and post-place at the same time is called a loop.
A net is given as a tripel \( N = (P, T, F) \), where

- \( P \), the set of places, and \( T \), the set of transitions, are non-empty disjoint sets,
- \( F \subseteq (P \times T) \cup (T \times P) \), is the set of directed edges, called flow relation, which is a binary relation such that \( \text{dom}(F) \cup \text{cod}(F) = P \cup T \).

Let \( N = (P, T, F) \) be a net and \( x \in P \cup T \).

\[
xF := \{ y \mid (x, y) \in F \}
\]

\[
Fx := \{ y \mid (y, x) \in F \}
\]

For \( p \in P \), \( pF \) is the set of post-transitions of \( p \); \( Fp \) is the set of pre-transitions of \( p \). For \( t \in T \), \( tF \) is the set of post-places of \( t \); \( Ft \) is the set of pre-places of \( t \).
A net is given as a triple $N = (P, T, F)$, where

- $P$, the set of places, and $T$, the set of transitionen, are non-empty disjoint sets,
- $F \subseteq (P \times T) \cup (T \times P)$, is the set of directed edges, called flow relation, which is a binary relation such that $\text{dom}(F) \cup \text{cod}(F) = P \cup T$.

Let $N = (P, T, F)$ be a net and $x \in P \cup T$.

$$xF := \{y \mid (x, y) \in F\}$$
$$Fx := \{y \mid (y, x) \in F\}$$

For $p \in P$, $pF$ is the set of post-transitions of $p$; $Fp$ is the set of pre-transitions of $p$. For $t \in T$, $tF$ is the set of post-places of $t$; $Ft$ is the set of pre-places of $t$. 
Let \( N = (P, T, F) \) be a net. Any mapping \( m \) from \( P \) into the set of natural numbers \( \mathbb{NAT} \) is called a marking of \( P \).

A mapping \( P \rightarrow \mathbb{NAT} \cup \{\omega\} \) is called \( \omega \)-marking. \( \omega \) represents an infinitely large number of tokens.

Arithmetic of \( \omega \):

\[
\omega - n = \omega, \omega + n = \omega, n \cdot \omega = \omega, 0 \cdot \omega = 0, \omega > n
\]

where \( n \in \mathbb{NAT}, n > 0 \).

A marking represents a possible system state.
Let $N = (P, T, F)$ be a net. Any mapping $m$ from $P$ into the set of natural numbers $\text{NAT}$ is called a marking of $P$.

A mapping $P \rightarrow \text{NAT} \cup \{\omega\}$ is called $\omega$-marking. $\omega$ represents an infinitely large number of tokens.

Arithmetic of $\omega$:

$\omega - n = \omega, \omega + n = \omega, n \cdot \omega = \omega, 0 \cdot \omega = 0, \omega > n$

where $n \in \text{NAT}, n > 0$.

A marking represents a possible system state.
Let $N = (P, T, F)$ be a net. Any mapping $m$ from $P$ into the set of natural numbers $\text{NAT}$ is called a marking of $P$.

A mapping $P \rightarrow \text{NAT} \cup \{\omega\}$ is called $\omega$-marking. $\omega$ represents an infinitely large number of tokens.

Arithmetic of $\omega$:

\[ \omega - n = \omega, \omega + n = \omega, n \cdot \omega = \omega, 0 \cdot \omega = 0, \omega > n \]

where $n \in \text{NAT}$, $n > 0$.

A marking represents a possible system state.
Let $N = (P, T, F)$ be a net. Any mapping $m$ from $P$ into the set of natural numbers $\text{NAT}$ is called a marking of $P$.

A mapping $P \rightarrow \text{NAT} \cup \{\omega\}$ is called $\omega$-marking. $\omega$ represents an infinitely large number of tokens.

Arithmetic of $\omega$:

\[
\omega - n = \omega, \omega + n = \omega, n \cdot \omega = \omega, 0 \cdot \omega = 0, \omega > n
\]

where $n \in \text{NAT}, n > 0$.

A marking represents a possible system state.
A eS-Net is given as $N = (P, T, F, V, m_0)$, where

- $(P, T, F)$ a net,
- $V : F \rightarrow \mathbb{NAT}^+$ a multiplicity,
- $m_0$ a marking called initial marking.

$N$ is called ordinary eS-Net, whenever $V(f) = 1$, $\forall f \in F$. 
A eS-Net is given as $N = (P, T, F, V, m_0)$, where
- $(P, T, F)$ a net,
- $V : F \rightarrow \mathbb{N}^+$ a multiplicity,
- $m_0$ a marking called initial marking.

$N$ is called ordinary eS-Net, whenever $V(f) = 1$, $\forall f \in F$. 
A transition may fire once it is enabled.

Let \( N = (P, T, F, V, m_0) \) a eS-Net, \( m \) a marking and \( t \in T \) a transition.

- \( t \) is enabled at \( m \), if for all pre-places \( p \in Ft \) there holds:
  \[ m(p) \geq V(p, t). \]

Whenever \( t \) is enabled at \( m \), then \( t \) may fire at \( m \). Firing \( t \) at \( m \) transforms \( m \) to \( m', m[t \succ m'] \), in the following way:

\[
m'(p) := \begin{cases} 
  m(p) - V(p, t) + V(t, p) & \text{if } p \in Ft, p \in tF, \\
  m(p) - V(p, t) & \text{if } p \in Ft, p \notin tF, \\
  m(p) + V(t, p) & \text{if } p \notin Ft, p \in tF, \\
  m(p) & \text{otherwise.}
\end{cases}
\]
A transition may fire once it is enabled.

Let $N = (P, T, F, V, m_0)$ a eS-Net, $m$ a marking and $t \in T$ a transition.

- **t is enabled at $m$**, if for all pre-places $p \in Ft$ there holds:
  
  $$m(p) \geq V(p, t).$$

- Whenever $t$ is enabled at $m$, then $t$ may **fire** at $m$. Firing $t$ at $m$ transforms $m$ to $m'$, $m[t \succ m']$, in the following way:

  $$m'(p) := \begin{cases} 
  m(p) - V(p, t) + V(t, p) & \text{if } p \in Ft, p \in tF, \\
  m(p) - V(p, t) & \text{if } p \in Ft, p \notin tF, \\
  m(p) + V(t, p) & \text{if } p \notin Ft, p \in tF, \\
  m(p) & \text{otherwise.}
  \end{cases}$$
A transition may fire once it is enabled.

Let $N = (P, T, F, V, m_0)$ a eS-Net, $m$ a marking and $t \in T$ a transition.

- **t is enabled at m**, if for all pre-places $p \in Ft$ there holds:

  $$m(p) \geq V(p, t).$$

- Whenever $t$ is enabled at $m$, then $t$ may fire at $m$. Firing $t$ at $m$ transforms $m$ to $m'$, $m[t \triangleright m']$, in the following way:

  $$
m'(p) := \begin{cases} 
  m(p) - V(p, t) + V(t, p) & \text{if } p \in Ft, p \in tF, \\
  m(p) - V(p, t) & \text{if } p \in Ft, p \notin tF, \\
  m(p) + V(t, p) & \text{if } p \notin Ft, p \in tF, \\
  m(p) & \text{otherwise}.
  \end{cases}$$
Transitions and markings in terms of vectors

Let places in $P$ be linearly ordered.

- Markings of a net can be considered as vectors of nonnegative integers of dimension $|P|$, called *place-vectors*.

- Transitions $t$ can be characterized as vectors of nonnegative integers of dimension $|P|$, called *transition vectors* $\Delta t$, $t^+$, $t^-$:

Let $N = (P, T, F, V, m_0)$ a eS-Net, $p \in P$ and $t \in T$.

$$
t^+(p) := \begin{cases} V(t, p) & \text{if } p \in tF, \\
0 & \text{otherwise.} \end{cases}
$$

$$
t^-(p) := \begin{cases} V(p, t) & \text{if } p \in Ft, \\
0 & \text{otherwise.} \end{cases}
$$

$$
\Delta t(p) := t^+(p) - t^-(p).
$$
Transitions and markings in terms of vectors

Let places in \( P \) be linearly ordered.

- Markings of a net can be considered as vectors of nonnegative integers of dimension \(| P |\), called \textit{place-vectors}.

- Transitions \( t \) can be characterized as vectors of nonnegative integers of dimension \(| P |\), called \textit{transition vectors} \( \Delta t, t^+, t^- \):

Let \( N = (P, T, F, V, m_0) \) a eS-Net, \( p \in P \) and \( t \in T \).

\[
t^+(p) := \begin{cases} 
V(t, p) & \text{if } p \in tF, \\
0 & \text{otherwise.}
\end{cases}
\]

\[
t^-(p) := \begin{cases} 
V(p, t) & \text{if } p \in Ft, \\
0 & \text{otherwise.}
\end{cases}
\]

\[
\Delta t(p) := t^+(p) - t^-(p).
\]
Transitions and markings in terms of vectors

Let places in \( P \) be linearly ordered.

- Markings of a net can be considered as vectors of nonnegative integers of dimension \( |P| \), called *place-vectors*.

- Transitions \( t \) can be characterized as vectors of nonnegative integers of dimension \( |P| \), called *transition vectors* \( \Delta t, t^+, t^- \):

Let \( N = (P, T, F, V, m_0) \) a eS-Net, \( p \in P \) and \( t \in T \).

\[
\begin{align*}
t^+(p) & := \begin{cases} 
V(t, p) & \text{if } p \in tF, \\
0 & \text{otherwise.}
\end{cases} \\
t^-(p) & := \begin{cases} 
V(p, t) & \text{if } p \in Ft, \\
0 & \text{otherwise.}
\end{cases} \\
\Delta t(p) & := t^+(p) - t^-(p).
\end{align*}
\]
Transitions and markings in terms of vectors

Let places in $P$ be linearly ordered.

- Markings of a net can be considered as vectors of nonnegative integers of dimension $|P|$, called *place-vectors*.

- Transitions $t$ can be characterized as vectors of nonnegative integers of dimension $|P|$, called *transition vectors* $\Delta t, t^+, t^-$:

Let $N = (P, T, F, V, m_0)$ a eS-Net, $p \in P$ and $t \in T$.

\[
\begin{align*}
    t^+(p) & := \begin{cases} 
        V(t, p) & \text{if } p \in tF, \\
        0 & \text{otherwise.}
    \end{cases} \\
    t^-(p) & := \begin{cases} 
        V(p, t) & \text{if } p \in Ft, \\
        0 & \text{otherwise.}
    \end{cases} \\
    \Delta t(p) & := t^+(p) - t^-(p).
\end{align*}
\]
Place and transition vectors at work:

- $m \leq m'$, if $m(p) \leq m'(p)$ for $\forall p \in P$,
- $m < m'$, if $m \leq m'$, however $m \neq m'$.
- $t$ is enabled at $m$ iff $t^- \leq m$,
- $m[t > m'$ iff $t^- \leq m$ and $m' = m + \Delta t$. 
Place and transition vectors at work:

- \( m \leq m' \), if \( m(p) \leq m'(p) \) for \( \forall p \in P \),
- \( m < m' \), if \( m \leq m' \), however \( m \neq m' \).
- \( t \) is enabled at \( m \) iff \( t^- \leq m \),
- \( m \uparrow t \) iff \( t^- \leq m \) and \( m' = m + \Delta t \).
Reachability

Let $N = (S, T, F, V, m_0)$ a eS-Net.

We denote $W(T)$ the set of words with finite length over $T$; $\epsilon \in W(T)$ is called the empty word.

The length of a word $w \in W(T)$ is given by $l(w)$. We have $l(\epsilon) = 0$.

Let $m, m'$ be markings of $P$ and $w \in W(T)$. We define a relation $m[w \succ m']$ inductively:

- $m[\epsilon \succ m'$ iff $m = m'$,
- Let $t \in T, w \in W(T)$. $m[wt \succ m'$ iff $\exists m'': m[w \succ m'', m''[t \succ m']$.

The reachability relation $[\cdot \succ\cdot]$ of $N$ is defined by

$$m[\ast \succ m' \iff \exists w : w \in W(T), m[w \succ m';$$

$m'$ is reachable from $m$ in $N$. 
Reachability

Let $N = (S, T, F, V, m_0)$ a eS-Net.

We denote $W(T)$ the set of words with finite length over $T$; $\epsilon \in W(T)$ is called the \textit{empty word}.

The length of a word $w \in W(T)$ is given by $l(w)$. We have $l(\epsilon) = 0$.

Let $m, m'$ be markings of $P$ and $w \in W(T)$. We define a relation $m \succ w \succ m'$ inductively:

- $m[\epsilon \succ m' \text{ iff } m = m']$,
- Let $t \in T, w \in W(T)$. $m[wt \succ m' \text{ iff } \exists m'': m \succ m'', m'' [t \succ m']$.

The \textit{reachability relation} $[\succ]$ of $N$ is defined by

$m[\succ m' \text{ iff } \exists w : w \in W(T), m \succ w \succ m';$

$m'$ is \textit{reachable} from $m$ in $N$. 
Reachability

Let \( N = (S, T, F, V, m_0) \) a eS-Net.

We denote \( W(T) \) the set of words with finite length over \( T \); \( \epsilon \in W(T) \) is called the empty word.

The length of a word \( w \in W(T) \) is given by \( l(w) \). We have \( l(\epsilon) = 0 \).

Let \( m, m' \) be markings of \( P \) and \( w \in W(T) \). We define a relation \( m \left[ w \succ m' \right] \) inductively:

- \( m[\epsilon \succ m' \text{ iff } m = m'] \),
- Let \( t \in T, w \in W(T) \). \( m[wt \succ m' \text{ iff } \exists m'' : m[w \succ m'', m''[t \succ m'] \).

The reachability relation \( [\succ] \) of \( N \) is defined by

\[
m \succ m' \text{ iff } \exists w : w \in W(T), m[w \succ m'];
\]

\( m' \) is reachable from \( m \) in \( N \).
Reachability

Let $$N = (S, T, F, V, m_0)$$ a eS-Net.

We denote $$W(T)$$ the set of words with finite length over $$T$$; $$\epsilon \in W(T)$$ is called the empty word.

The length of a word $$w \in W(T)$$ is given by $$l(w)$$. We have $$l(\epsilon) = 0$$.

Let $$m, m'$$ be markings of $$P$$ and $$w \in W(T)$$. We define a relation $$m[w \succ m']$$ inductively:

- $$m[\epsilon \succ m']$$ iff $$m = m'$$,
- Let $$t \in T$$, $$w \in W(T)$$. $$m[wt \succ m']$$ iff $$\exists m'' : m[w \succ m'']$$, $$m''[t \succ m']$$.

The reachability relation $$[\succ]$$ of $$N$$ is defined by

$$m[\ast \succ m']$$ iff $$\exists w : w \in W(T)$$, $$m[w \succ m']$$;

$$m'$$ is reachable from $$m$$ in $$N$$. 
12. Petri-Nets

12.1. Elementary System Nets

- $R_N(m) := \{m' | m[* \succ m']\}$, the set of markings reachable from $m$ by $N$,
- $L_N(m) := \{w | \exists m' : m[w \succ m']\}$, the set of all words representing firing sequences of transitions of $N$ starting at $m$,
- $\Delta w := \sum_{i=1}^{n} \Delta t_i$, wobei $w = t_1 t_2 \ldots t_n$.

Results

- $[* \succ$ is reflexiv and transitiv.
- $m[w \succ m'] \Rightarrow (m + m^*)[w \succ (m' + m^*)]$, $\forall m^* \in NAT^{|S|}$. (Monotonie)
- $m[w \succ m'] \Rightarrow m' = m + \Delta w$. 
\( R_N(m) := \{ m' \mid m[\ast \succ m'] \} \), the set of markings reachable from \( m \) by \( N \),

\( L_N(m) := \{ w \mid \exists m' : m[w \succ m'] \} \), the set of all words representing firing sequences of transitions of \( N \) starting at \( m \),

\[ \Delta w := \sum_{i=1}^{n} \Delta t_i, \text{ wobei } w = t_1 t_2 \ldots t_n. \]

**Results**

- \( [\ast \succ] \) is reflexiv and transitiv.
- \( m[w \succ m'] \Rightarrow (m + m^*)[w \succ (m' + m^*)], \forall m^* \in NAT^{|S|}. \) (Monotonie)
- \( m[w \succ m'] \Rightarrow m' = m + \Delta w. \)
$R_N(m) := \{ m' | m[* \succ] m' \}$, the set of markings reachable from $m$ by $N$,

$L_N(m) := \{ w | \exists m' : m[w \succ] m' \}$, the set of all words representing firing sequences of transitions of $N$ starting at $m$,

$\Delta w := \sum_{i=1}^{n} \Delta t_i$, wobei $w = t_1 t_2 \ldots t_n$.

Results

- $[* \succ]$ is reflexiv and transitiv.
- $m[w \succ] m' \Rightarrow (m + m^*)[w \succ] (m' + m^*)$, $\forall m^* \in NAT^{|S|}$. (Monotonie)
- $m[w \succ] m' \Rightarrow m' = m + \Delta w$. 
\[ R_N(m) := \{ m' \mid m[* \succ m'] \}, \text{ the set of markings reachable from } m \text{ by } N, \]

\[ L_N(m) := \{ w \mid \exists m' : m[w \succ m'] \}, \text{ the set of all words representing firing sequences of transitions of } N \text{ starting at } m, \]

\[ \Delta w := \sum_{i=1}^{n} \Delta t_i, \text{ wobei } w = t_1 t_2 \ldots t_n. \]

**Results**

- \([* \succ] \text{ is reflexiv and transitiv.} \]
- \(m[w \succ m'] \Rightarrow (m + m^*)[w \succ (m' + m^*), \forall m^* \in \text{NAT}^{\|S\|}. \text{ (Monotonie)} \]
- \(m[w \succ m'] \Rightarrow m' = m + \Delta w. \]
Reachability graph

Let $N = (P, T, F, V, m_0)$ a eS-Net. The *Reachability graph* of $N$ is a directed graph $EG(N) := (R_N(m_0), B_N)$; $R_N(m_0)$ is the set of nodes and $B_N$ is the set of annotated edges as follows:

$$B_N = \{(m, t, m') \mid m, m' \in R_N(m_0), t \in T, m[t \succ m']\}.$$
Exercise: Give the reachability graph of the following eS-Net:

\[ R_N(m_0) = \{ (1, 0, 0, 0), (1, 1, 0, 0), (1, 2, 0, 0), (1, 3, 0, 0), \ldots, \\
                    (0, 0, 1, 0), (0, 1, 1, 0), (0, 2, 1, 0), (0, 3, 1, 0), \ldots, \\
                    (0, 0, 1, 1), (0, 1, 1, 1), (0, 0, 1, 2), (0, 1, 1, 2), (0, 0, 1, 3), \ldots \} \]

\[ L_N(m_0) = \{ \epsilon, t_1, t_1 t_1, t_1 t_1 t_1, \ldots, \\
                  t_2, t_1 t_2, t_1 t_1 t_2, t_1 t_1 t_1 t_2, \ldots, \\
                  t_1 t_2 t_3, t_1 t_1 t_2 t_3, t_1 t_1 t_2 t_3 t_3, t_1 t_1 t_1 t_2 t_3, t_1 t_1 t_1 t_2 t_3 t_3 t_3, \ldots \} \]
Section 12.2 Control Patterns

- eS-nets can be used to model *causal dependencies*; for modelling temporal aspects extensions of the formalism are required.

- Whenever between some transitions there are no causal dependencies, the transitions are called *concurrent*; concurrency is a prerequisite for parallelism.
Some typical causalities

Sequence

Iteration
AND-join, OR-join, AND-split, OR-split

- AND-join
- OR-join
- AND-split
- OR-split
OR-Split with regulation
OR-Join with regulation
A eS-Net with concurrency
Section 12.3 Analysis

Boundedness

Let $N = (P, T, F, V, m_0)$ be a eS-Net, $m$ a marking, $p \in P$.

- Let $k \in \mathbb{N}^+$. $p$ is called $k$-bounded, if for each marking $m'$ there holds:
  \[ m' \in R_N(m_0) \Rightarrow m'(p) \leq k. \]

- $p$ is called bounded, if $p$ $k$-bounded for some $k \in \mathbb{N}^+$.

- $N$ is called bounded ($k$-bounded), if each place is bounded ($k$-bounded).

- A eS-net is called safe, if it is 1-bounded. Places of a bounded net may be interpreted as boolean conditions.
Section 12.3 Analysis

Boundedness

Let $N = (P, T, F, V, m_0)$ be an eS-Net, $m$ a marking, $p \in P$.

- Let $k \in \mathbb{N}^+$. $p$ is called $k$-bounded, if for each marking $m'$ there holds:

  $$m' \in R_N(m_0) \Rightarrow m'(p) \leq k.$$ 

- $p$ is called bounded, if $p$ is $k$-bounded for some $k \in \mathbb{N}^+$.

- $N$ is called bounded ($k$-bounded), if each place is bounded ($k$-bounded).

- A eS-net is called safe, if it is 1-bounded. Places of a bounded net may be interpreted as boolean conditions.
Section 12.3 Analysis

**Boundedness**

Let $N = (P, T, F, V, m_0)$ be a eS-Net, $m$ a marking, $p \in P$.

- Let $k \in \mathbb{N}^+$. $p$ is called $k$-bounded, if for each marking $m'$ there holds:

  $$m' \in R_N(m_0) \Rightarrow m'(p) \leq k.$$

- $p$ is called bounded, if $p$ $k$-bounded for some $k \in \mathbb{N}^+$.

- $N$ is called bounded ($k$-bounded), if each place is bounded ($k$-bounded).

- A eS-net is called safe, if it is 1-bounded. Places of a bounded net may be interpreted as boolean conditions.
**Theorem**

Let $N = (P, T, F, V, m_0)$ be an eS-Net. $N$ is *unbounded*, i.e. not bounded, iff there exist $w \in W(T)$, $m, m' \in R_N(m_0)$, such that $m[w \triangleright m'$ and $m' > m$.

**Proof $\Leftarrow$**

Let $w \in W(T)$, $m, m' \in R_N(m_0)$, such that $m[w \triangleright m'$ and $m' > m$. It holds

$$m[w \triangleright m'[w \triangleright m''[w \triangleright m''' \ldots,$$

where $m < m' < m'' < m''' < \ldots$.

Thus there must exist at least one unbounded place.
Theorem

Let $N = (P, T, F, V, m_0)$ be a eS-Net. $N$ is unbounded, i.e. not bounded, iff there exist $w \in W(T)$, $m, m' \in R_N(m_0)$, such that $m[w \succ m'$ and $m' > m$.

Proof $\Leftarrow$

Let $w \in W(T)$, $m, m' \in R_N(m_0)$, such that $m[w \succ m'$ and $m' > m$. It holds

$$m[w \succ m'[w \succ m''[w \succ m''' \ldots,$$

where $m < m' < m'' < m''' < \ldots$.

Thus there must exist at least one unbounded place.
To prove \( \Rightarrow \) we first prove:

**Lemma**

For each infinite sequence of markings \((m_i)\) of markings there exists an infinite subsequence \((m'_j)\), which is weakly monotonic, i.e. \( l < k \) implies \( m'_l \leq m'_k \).

To prove the Lemma, first extract an infinite subsequence for which weak monotonicity holds for the first components of its markings. Then extract from that subsequence an infinite subsequence for which weak monotonicity holds for the second components of its markings, etc.
To proof ⇒ we first proof:

**Lemma**

For each infinite sequence of markings \((m_i)\) of markings there exists an infinite subsequence \((m'_j)\), which is weakly monotonic, i.e. \(l < k\) implies \(m'_l \leq m'_k\).

To prove the Lemma, first extract an infinite subsequence for which weak monotonicity holds for the first components of its markings. Then extract from that subsequence an infinite subsequence for which weak monotonicity holds for the second components of its markings, etc.
Proof ⇒

- Consider the reachability graph $EG(N)$, which has an infinite number of nodes. Starting from $m_0$ there exist a directed path to each node of the graph. Because of the finite number of transitions, each node has only a finite number of direct successors.

- Thus, at $m_0$ there start an infinite number of paths without cycles, however only a finite number of edges. Therefore, one of these edges must be part of infinitely many paths. Let $m_0 \rightarrow m_1$ be one such edge.

- The same argument can be applied w.r.t. $m_1$ such that we get $m_0 \rightarrow m_1 \rightarrow m_2$, where $m_1 \rightarrow m_2$ is part of an infinite number of paths.

- The above construction can be repeated infinitely many times. Therefore there exists an infinite sequence of markings $(m_i)$ of pairwise distinct markings, such that $m_k, m_l$, $0 \leq k \leq l$ implies:

$\quad m_0[*\succ m_k[*\succ m_l].$

because of the Lemma there exists an infinite weakly monotonic subsequence $(m'_j)$ von $(m_i)$. Let $m'_1, m'_2$ two successive elements. From construction we have $m_0[*\succ m'_1[*\succ m'_2,$ $m'_1 \leq m'_2$ and even $m'_1 < m'_2$. 
Proof

- Consider the reachability graph $EG(N)$, which has an infinite number of nodes. Starting from $m_0$ there exist a directed path to each node of the graph. Because of the finite number of transitions, each node has only a finite number of direct successors.

- Thus, at $m_0$ there start an infinite number of paths without cycles, however only a finite number of edges. Therefore, one of these edges must be part of infinitely many paths. Let $m_0 \rightarrow m_1$ be one such edge.

- The same argument can be applied w.r.t. $m_1$ such that we get $m_0 \rightarrow m_1 \rightarrow m_2$, where $m_1 \rightarrow m_2$ is part of an infinite number of paths.

- The above construction can be repeated infinitely many times. Therefore there exists an infinite sequence of markings $(m_i)$ of pairwise distinct markings, such that $m_k, m_l$, $0 \leq k \leq l$ implies:

  $$m_0 \star \succ m_k \star \succ m_l.$$

  because of the Lemma there exists an infinite weakly monotonic subsequence $(m'_i)$ von $(m_i)$. Let $m'_1, m'_2$ two successive elements. From construction we have $m_0 \star \succ m'_1 \star \succ m'_2$, $m'_1 \leq m'_2$ and even $m'_1 < m'_2$. 
Proof ⇒

- Consider the reachability graph $EG(N)$, which has an infinite number of nodes. Starting from $m_0$ there exist a directed path to each node of the graph. Because of the finite number of transitions, each node has only a finite number of direct successors.

- Thus, at $m_0$ there start an infinite number of paths without cycles, however only a finite number of edges. Therefore, one of these edges must be part of infinitely many paths. Let $m_0 \rightarrow m_1$ be one such edge.

- The same argument can be applied w.r.t. $m_1$ such that we get $m_0 \rightarrow m_1 \rightarrow m_2$, where $m_1 \rightarrow m_2$ is part of an infinite number of paths.

- The above construction can be repeated infinitely many times. Therefore there exists an infinite sequence of markings $(m_i)$ of pairwise distinct markings, such that $m_k, m_l, 0 \leq k \leq l$ implies:

  $$m_0[*\succ m_k[*\succ m_l.$$  

  because of the Lemma there exists an infinite weakly monotonic subsequence $(m'_j)$ von $(m_i)$. Let $m'_1, m'_2$ two successive elements. From construction we have $m_0[*\succ m'_1[*\succ m'_2$, $m'_1 \leq m'_2$ and even $m'_1 < m'_2$. 
Proof ⇒

- Consider the reachability graph $EG(N)$, which has an infinite number of nodes. Starting from $m_0$ there exist a directed path to each node of the graph. Because of the finite number of transitions, each node has only a finite number of direct successors.

- Thus, at $m_0$ there start an infinite number of paths without cycles, however only a finite number of edges. Therefore, one of these edges must be part of infinitely many paths. Let $m_0 \rightarrow m_1$ be one such edge.

- The same argument can be applied w.r.t. $m_1$ such that we get $m_0 \rightarrow m_1 \rightarrow m_2$, where $m_1 \rightarrow m_2$ is part of an infinite number of paths.

- The above construction can be repeated infinitely many times. Therefore there exists an infinite sequence of markings $(m_i)$ of pairwise distinct markings, such that $m_k, m_l, 0 \leq k \leq l$ implies:

$$m_0 \succ m_k \succ m_l.$$  

because of the Lemma there exists an infinite weakly monotonic subsequence $(m'_j)$ von $(m_i)$. Let $m'_1, m'_2$ two successive elements. From construction we have $m_0 \succ m'_1 \succ m'_2$, $m'_1 \leq m'_2$ and even $m'_1 < m'_2$. 
Reachability

Let $N = (P, T, F, V, m_0)$ be a eS-Net, $m \in NAT^{|P|}$ a marking. The decision problem:

$$m \in R_N(m_0)?$$

is called reachability-problem.

The reachability problem is decidable, however even for bounded nets hyperexponential.
Reachability

Let $N = (P, T, F, V, m_0)$ be a eS-Net, $m \in \mathbb{N}^{P}$ a marking. The decision problem:

$$m \in R_N(m_0)?$$

is called \textit{reachability-problem}.

The reachability problem is decidable, however even for bounded nets hyperexponential.
**Coverability**

Let $N = (P, T, F, V, m_0)$ be a eS-Net and let $m, m'$ be markings of $N$.

- If $m \leq m'$, then $m'$ covers $m$, respectively, $m$ is covered by $m'$.
- $m$ is called *coverable* in $N$, if there exists a reachable marking $m'$ which covers $m$.

Consequence: Whenever a marking is not coverable w.r.t. some eS-Net $N$, it is not reachable in $N$.

Give examples.
Coverability

Let $N = (P, T, F, V, m_0)$ be a eS-Net and let $m, m'$ be markings of $N$.

- If $m \leq m'$, then $m'$ covers $m$, respectively, $m$ is covered by $m'$.
- $m$ is called coverable in $N$, if there exists a reachable marking $m'$ which covers $m$.

Consequence: Whenever a marking is not coverable w.r.t. some eS-Net $N$, it is not reachable in $N$.

Give examples.
**Coverability**

Let \( N = (P, T, F, V, m_0) \) be a eS-Net and let \( m, m' \) be markings of \( N \).
  - If \( m \leq m' \), then \( m' \) covers \( m \), respectively, \( m \) is covered by \( m' \).
  - \( m \) is called *coverable* in \( N \), if there exists a reachable marking \( m' \) which covers \( m \).

Consequence: Whenever a marking is not coverable w.r.t. some eS-Net \( N \), it is not reachable in \( N \).

**Give examples.**
Coverability Graph

Let $N = (P, T, F, V, m_0)$ a eS-Net. The Coverability Graph of $N$ is given by $CG(N) := (R, B)$ as follows:

- **inductive definition of an auxiliary tree $T(N)$:**
  
  The values of the nodes in $T(N)$ are $\omega$-markings of $N$. The value of the root node $r$ is $m_0$. Let $m$ be the value of some node $n$ of $T(N)$, $t \in T$, and $m[t \succ m']$.

  - Whenever on the path from the root $r$ to $n$ there exists a node $n''$ with value $m''$ such that $m'' < m'$, then update $m'$ by $m'(s) := \omega$ for all places $p$ with $m''(p) < m'(p)$.
  - Introduce a new successor node $n'$ of $n$ with value $m'$ and mark the edge from $n$ to $n'$ by $t$.
  - If there already exists another node in the tree with the same value $m'$, node $n'$ is not considered any further.

- A coverability graph is derived from a coverability tree by taking the values of the nodes in the tree as nodes in the graph.
Coverability Graph

Let $N = (P, T, F, V, m_0)$ a eS-Net. The Coverability Graph of $N$ is given by $CG(N) := (R, B)$ as follows:

- **inductive definition of an auxiliary tree $T(N)$:**
  
  The values of the nodes in $T(N)$ are $\omega$-markings of $N$. The value of the root node $r$ is $m_0$. Let $m$ be the value of some node $n$ of $T(N)$, $t \in T$, and $m[t > m']$.

- Whenever on the path from the root $r$ to $n$ there exists a node $n''$ with value $m''$ such that $m'' < m'$, then update $m'$ by $m'(s) := \omega$ for all places $p$ with $m''(p) < m'(p)$.

- Introduce a new successor node $n'$ of $n$ with value $m'$ and mark the edge from $n$ to $n'$ by $t$.

- If there already exists another node in the tree with the same value $m'$, node $n'$ is not considered any further.

- A coverability graph is derived from a coverability tree by taking the values of the nodes in the tree as nodes in the graph.
Coverability Graph

Let $N = (P, T, F, V, m_0)$ a eS-Net. The Coverability Graph of $N$ is given by $CG(N) := (R, B)$ as follows:

- **Inductive definition of an auxiliary tree $T(N)$:**
  
  The values of the nodes in $T(N)$ are $\omega$-markings of $N$. The value of the root node $r$ is $m_0$. Let $m$ be the value of some node $n$ of $T(N)$, $t \in T$, and $m[t > m']$.
  
  - Whenever on the path from the root $r$ to $n$ there exists a node $n''$ with value $m''$ such that $m'' < m'$, then update $m'$ by $m'(s) := \omega$ for all places $p$ with $m''(p) < m'(p)$.
  
  - Introduce a new successor node $n'$ of $n$ with value $m'$ and mark the edge from $n$ to $n'$ by $t$.
  
  - If there already exists another node in the tree with the same value $m'$, node $n'$ is not considered any further.

- A coverability graph is derived from a coverability tree by taking the values of the nodes in the tree as nodes in the graph.
Slide 1: Coverability Graph

Let $N = (P, T, F, V, m_0)$ a eS-Net. The Coverability Graph of $N$ is given by $CG(N) := (R, B)$ as follows:

- **Inductive definition of an auxiliary tree $T(N)$:**
  - The values of the nodes in $T(N)$ are $\omega$-markings of $N$. The value of the root node $r$ is $m_0$. Let $m$ be the value of some node $n$ of $T(N)$, $t \in T$, and $m[t > m']$.
  - Whenever on the path from the root $r$ to $n$ there exists a node $n''$ with value $m''$ such that $m'' < m'$, then update $m'$ by $m'(s) := \omega$ for all places $p$ with $m''(p) < m'(p)$.
  - Introduce a new successor node $n'$ of $n$ with value $m'$ and mark the edge from $n$ to $n'$ by $t$.
  - If there already exists another node in the tree with the same value $m'$, node $n'$ is not considered any further.

A coverability graph is derived from a coverability tree by taking the values of the nodes in the tree as nodes in the graph.
Coverability Graph

Let $N = (P, T, F, V, m_0)$ a eS-Net. The Coverability Graph of $N$ is given by $CG(N) := (R, B)$ as follows:

- **inductive definition of an auxiliary tree $T(N)$:**
  - The values of the nodes in $T(N)$ are $\omega$-markings of $N$. The value of the root node $r$ is $m_0$. Let $m$ be the value of some node $n$ of $T(N)$, $t \in T$, and $m[t \succ m']$.
    - Whenever on the path from the root $r$ to $n$ there exists a node $n''$ with value $m''$ such that $m'' < m'$, then update $m'$ by $m'(s) := \omega$ for all places $p$ with $m''(p) < m'(p)$.
    - Introduce a new successor node $n'$ of $n$ with value $m'$ and mark the edge from $n$ to $n'$ by $t$.
    - If there already exists another node in the tree with the same value $m'$, node $n'$ is not considered any further.

- A coverability graph is derived from a coverability tree by taking the values of the nodes in the tree as nodes in the graph.
Coverability Graph

Let $N = (P, T, F, V, m_0)$ a eS-Net. The *Coverability Graph* of $N$ is given by $CG(N) := (R, B)$ as follows:

- **inductive definition of an auxiliary tree $T(N)$:**
  The values of the nodes in $T(N)$ are $\omega$-markings of $N$. The value of the root node $r$ is $m_0$. Let $m$ be the value of some node $n$ of $T(N)$, $t \in T$, and $m[t \succ m']$.

  - Whenever on the path from the root $r$ to $n$ there exists a node $n''$ with value $m''$ such that $m'' < m'$, then update $m'$ by $m'(s) := \omega$ for all places $p$ with $m''(p) < m'(p)$.
  - Introduce a new successor node $n'$ of $n$ with value $m'$ and mark the edge from $n$ to $n'$ by $t$.
  - If there already exists another node in the tree with the same value $m'$, node $n'$ is not considered any further.

- A coverability graph is derived from a coverability tree by taking the values of the nodes in the tree as nodes in the graph.
Give a coverability tree.
A eS-net with two different coverability graphs.
Two eS-Nets with identical coverability graphs.
Theorem

The coverability graph \( CG(N) = (R, B) \) of a eS-net \( N \) is finite.

Proof:
Assume \( CG(N) \) is not finite. Then it contains an infinite number of nodes. Thus there exists an infinite, weakly monotonic sequence of \( \omega \)-markings, i.e. values of the nodes in the tree. Because of the construction of the auxiliary tree \( T(N) \), such an infinite sequence cannot exist, as we can introduce \( \omega \) only a finite number of times.
To test the reachability of a certain marking we may first test its coverability and then try to find a firing sequence which confirms its reachability.

Is marking $m = (0, 3, 1, 3)$ reachable?

Yes, using the word $w = t_1^6 t_2 t_3^3$. 
To test the reachability of a certain marking we may first test its coverability and then try to find a firing sequence which confirms its reachability.

Is marking \( m = (0, 3, 1, 3) \) reachable?

Yes, using the word \( w = t_1^6 t_2 t_3^3 \).
To test the reachability of a certain marking we may first test its coverability and then try to find a firing sequence which confirms its reachability.

Is marking \( m = (0, 3, 1, 3) \) reachable?

Yes, using the word \( w = t_1^6 t_2 t_3^3 \).
**Live, dead and deadlockfree**

Let $N = (P, T, F, V, m_0)$ a eS-Net.

- A marking $m$ is called *dead* in $N$, if there is no $t \in T$ which is enabled at $m$.
- A transition $t$ is called *dead* at marking $m$, if there is no marking reachable from $m$, such that $t$ is enabled.
  
  If $t$ dead at $m_0$, then $t$ is called dead in $N$.

- A transition $t$ is called *live* at marking $m$, if for any reachable marking from $m$ it holds that $t$ is not dead.
  
  If $m = m_0$, then $t$ is called live in $N$.

- A marking $m$ is called *live* in $N$ if all transitions $t \in T$ are live in $m$. If $m = m_0$ then $N$ is called live.

- $N$ is called *deadlockfree*, if no dead marking is reachable.

**Note:** whenever a transition is dead at some $m$, then it is not live at $m$.

However, the other direction does not hold.
Live, dead and deadlockfree

Let $N = (P, T, F, V, m_0)$ a eS-Net.

- A marking $m$ is called **dead** in $N$, if there is no $t \in T$ which is enabled at $m$.

- A transition $t$ is called **dead** at marking $m$, if there is no marking reachable from $m$, such that $t$ is enabled.

  If $t$ dead at $m_0$, then $t$ is called dead in $N$.

- A transition $t$ is called **live** at marking $m$, if for any reachable marking from $m$ it holds that $t$ is not dead.

  If $m = m_0$, then $t$ is called **live** in $N$.

- A marking $m$ is called **live** in $N$ if all transitions $t \in T$ are **live** in $m$. If $m = m_0$ then $N$ is called **live**.

- $N$ is called **deadlockfree**, if no dead marking is reachable.

Note: whenever a transition is dead at some $m$, then it is not live at $m$.
However, the other direction does not hold.
Live, dead and deadlockfree

Let $N = (P, T, F, V, m_0)$ a eS-Net.

- A marking $m$ is called *dead* in $N$, if there is no $t \in T$ which is enabled at $m$.
- A transition $t$ is called *dead* at marking $m$, if there is no marking reachable from $m$, such that $t$ is enabled.

If $t$ dead at $m_0$, then $t$ is called dead in $N$.

- A transition $t$ is called *live* at marking $m$, if for any reachable marking from $m$ it holds that $t$ is not dead.
  If $m = m_0$, then $t$ is called *live* in $N$.

- A marking $m$ is called *live* in $N$ if all transitions $t \in T$ are *live* in $m$. If $m = m_0$ then $N$ is called *live*.

- $N$ is called *deadlockfree*, if no dead marking is reachable.

Note: whenever a transition is dead at some $m$, then it is not live at $m$.
However, the other direction does not hold.
Live, dead and deadlockfree

Let \( N = (P, T, F, V, m_0) \) a eS-Net.

- A marking \( m \) is called dead in \( N \), if there is no \( t \in T \) which is enabled at \( m \).
- A transition \( t \) is called dead at marking \( m \), if there is no marking reachable from \( m \), such that \( t \) is enabled.

If \( t \) dead at \( m_0 \), then \( t \) is called dead in \( N \).

- A transition \( t \) is called live at marking \( m \), if for any reachable marking from \( m \) it holds that \( t \) is not dead.
  If \( m = m_0 \), then \( t \) is called live in \( N \).

- A marking \( m \) is called live in \( N \) if all transitions \( t \in T \) are live in \( m \). If \( m = m_0 \) then \( N \) is called live.
- \( N \) is called deadlockfree, if no dead marking is reachable.

Note: whenever a transition is dead at some \( m \), then it is not live at \( m \).
However, the other direction does not hold.
Firing the word $t_3 t_1 t_2$ results in a dead marking $(0, 0)$. The coverability graph does not indicate this!

Liveness cannot be tested by inspection of the coverability graph.

Do there exist other techniques for analysis?