State Space Analysis: Properties, Reachability Graph, and Coverability Graph

prof.dr.ir. Wil van der Aalst
Outline

- Motivation
- Formalization
- Basic properties
- Reachability graph
- Coverability graph
Motivation
Design-time analysis vs run-time analysis

- **Design-time analysis**
  - Models are created and analyzed before deployment.
  - Examples: BPMN, BPEL, EPCs, Petri nets, UML AD, etc.
  - Types of models: social networks, organizational networks, decision trees, etc.

- **Run-time analysis**
  - Models are recorded during execution.
  - Event logs store records of events, e.g., messages, transactions, etc.
  - Systems like WebSphere, Oracle, TIBCO/Staffware, SAP, FLOWer, etc.

- **(Software) system**
  - Supports/controls the "world" through models.
  - Analyzes, configures, implements, and extends models.
  - Records events during run-time.

- **Event logs**
  - Store dedicated formats such as IBM's Common Event Infrastructure (CEI) and MXML or proprietary formats stored in flat files or database tables.

- **Validation**
  - Ensures that models meet requirements.

- **Verification**
  - Confirms that models accurately represent the system.

- **Performance analysis**
  - Evaluates system efficiency.

- **Event logs**
  - Extracted from recordings during run-time.
  - Analyzed to validate models and ensure conformance.

- **Discovery**
  - Identifies new models or extensions.

- **Conformance**
  - Validates that models meet specifications.

- **Extension**
  - Adds new functionality to models.

- **People**
  - Engaged in process models.

- **Services**
  - Facilitate interactions in process models.

- **Components**
  - Building blocks of process models.

- **Organizations**
  - Groups of people and services.
Analysis of processes

- Linear algebraic analysis techniques
- Markov chain analysis techniques
- State-space analysis techniques

Petri net
**Generic questions**

**terminating**
it has only finite occurrence sequences

**deadlock-free**
each reachable marking enables a transition

**live**
each reachable marking enables an occurrence sequence containing all transitions

**bounded**
each place has an upper bound that holds for all reachable markings

**1-safe**
1 is a bound for each place s

**reversible**
m0 is reachable from each reachable marking, i.e., the initial marking is a so-called **home marking**.
**Example**

- **terminating**: it has only finite occurrence sequences
- **deadlock-free**: each reachable marking enables a transition
- **live**: each reachable marking enables an occurrence sequence containing all transitions
- **bounded**: each place has an upper bound that holds for all reachable markings
- **1-safe**: 1 is a bound for each place
- **reversible**: m0 is reachable from each reachable marking, i.e., the initial marking is a so-called **home marking**.
Specific questions

Is it possible to have a token in both p2 and p5?
Will t3 always take place?
Will t3 always take place assuming "fairness"?
Is it possible to execute t1 after t4?
Can both p4 and p5 be empty at the same time?
infinite state space
state explosion problem
Concepts

marked net

reachability graph

coverability graph
Relevant material

   http://www.springerlink.com/content/x6hn592l35866lu8/fulltext.pdf


   a) Chapter 1: DOI: 10.1007/978-3-642-19345-3_1
      http://www.springerlink.com/content/p443h219v3u35371/fulltext.pdf
   b) Chapter 5: DOI: 10.1007/978-3-642-19345-3_5
      http://www.springerlink.com/content/u58h17n3167p0x1u/fulltext.pdf
   c) Events logs: http://www.processmining.org/book/

Today's focus is on 1 & 2.
Formalization

Note: refinement of earlier link between Petri net and transitions system (week 2/3) that is closer to standard literature.
Definition 1 (Basic Petri net). A basic Petri net is a triple \((P, T, F)\). \(P\) is a finite set of places, \(T\) is a finite set of transitions \((P \cap T = \emptyset)\), and \(F \subseteq (P \times T) \cup (T \times P)\) is a set of arcs (flow relation).

- \(P = \{p_1,p_2\}\)
- \(T = \{t_1,t_2\}\)
- \(F = \{(p_1,t_1), (t_1,p_1), (t_1,p_2), (p_1,t_2), (p_2,t_2)\}\)
Definition 2 (Place transition net (PT-net)). An Place transition net (or simply Petri net) is a tuple \((P, T, F, W)\), where:

- \((P, T, F)\) is a basic Petri net,
- \(W \in F \rightarrow \mathbb{N} \setminus \{0\}\) is an (arc) weight function.

- \(P = \{p_1, p_2\}\)
- \(T = \{t_1, t_2\}\)
- \(F = \{(p_1, t_1), (t_1, p_2), (p_2, t_2), (t_2, p_1)\}\)
- \(W(p_1, t_1) = 2, \quad W(t_1, p_2) = 2, \quad W(p_2, t_2) = 1, \quad \text{and} \quad W(t_2, p_1) = 1\)
Multi-sets

Definition 3 (Multi-set). Let \( A \) be a set. \( IB(A) = A \rightarrow \mathbb{N} \) is the set of multi-sets (bags) over \( A \), i.e., \( X \in IB(A) \) is a multi-set where for each \( a \in A \): \( X(a) \) denotes the number of times \( a \) is included in the multi-set.

- \( M_0(p1) = 2 \)
- \( M_0(p2) = 3 \)
Operations on multi-sets

Let $X$ and $Y$ be two multi-sets

- The sum of two multi-sets $(X + Y)$, the difference $(X - Y)$, the presence of an element in a multi-set $(x \in X)$, and the notion of sub-multi-set $(X \leq Y)$ are defined in a straightforward way.
- They can handle a mixture of sets and multi-sets.
- The operators are also robust with respect to the domains of the multi-sets, i.e., even if $X$ and $Y$ are defined on different domains, $X + Y$, $X - Y$, and $X \leq Y$ are defined properly by taking the union of the domains where needed.

- $|X| = \sum_{a \in A} X(a)$ is the size of some multi-set $X$ over $A$.
- $X(A') = \sum_{a \in A'} X(a)$ denotes the number of elements in $X$ with a value in $A' \subseteq A$.
- $\pi_{A'}(X)$ is the projection of $X$ onto $A' \subseteq A$, i.e., $(\pi_{A'}(X))(a) = X(a)$ if $a \in A'$ and $(\pi_{A'}(X))(a) = 0$ if $a \not\in A'$. 
To represent a concrete multi-set we use square brackets, e.g., \([a, a, b, a, b, c]\), \([a^3, b^2, c]\), and \(3[a] + 2[b] + [c]\) all refer to the same multi-set with six elements: 3 \(a\)'s, 2 \(b\)'s, and one \(c\). \([\ ]\) refers to the empty bag, i.e., \(\|\[\]\| = 0\).

- \(M_0 = [p_1, p_1, p_2, p_2, p_2] = [p_1^2, p_2^3] = 2[p_1] + 3[p_2]\)
- also denoted as \((2, 3)\)
Definition 4 (Marking). Let $N = (P, T, F, W)$ be a Petri net. A marking $M$ of $N$ is a multi-set over $P$, i.e., $M \in IB(P)$.


- $\bullet a = \left[ x^W(x,y) \mid (x, y) \in F \land a = y \right]$ is the preset of $a$.
- $a \bullet = \left[ y^W(x,y) \mid (x, y) \in F \land a = x \right]$ is the postset of $a$.
- Moreover, we extend the weight function for the situation that there is not an arc connecting two nodes, i.e., $W(x, y) = 0$ if $(x, y) \notin F$. 

Examples

- \( \bullet p_1 = [t_1] \)
- \( p_1 \bullet = [t_1, t_2] \)
- \( \bullet p_2 = [t_1] \)
- \( p_2 \bullet = [t_2] \)
- \( \bullet t_1 = [p_1] \)
- \( t_1 \bullet = [p_1, p_2] \)
- \( \bullet t_2 = [p_1, p_2] \)
- \( t_2 \bullet = [\ ] \)

- \( \bullet p_1 = [t_2] \)
- \( p_1 \bullet = [t_1^2] \)
- \( \bullet p_2 = [t_1^2] \)
- \( p_2 \bullet = [t_2] \)
- \( \bullet t_1 = [p_1^2] \)
- \( t_1 \bullet = [p_2^2] \)
- \( \bullet t_2 = [p_2] \)
- \( t_2 \bullet = [p_1] \)
Firing rule

Definition 6 (Firing rule). Let $N = (P, T, F, W)$ be a Petri net and $M \in IB(P)$ be a marking.

- A transition $t \in T$ is enabled, notation $(N, M)[t]$, if and only if, $M \geq \bullet t$.
- An enabled transition $t$ can fire while changing the state to $M'$, notation $(N, M)[t](N, M')$, if and only if, $M' = (M - \bullet t) + t\bullet$. 
### Table 2  Formal Definition of a Petri Net

A Petri net is a 5-tuple, $PN = (P, T, F, W, M_0)$ where:

- $P = \{p_1, p_2, \ldots, p_m\}$ is a finite set of places,
- $T = \{t_1, t_2, \ldots, t_n\}$ is a finite set of transitions,
- $F \subseteq (P \times T) \cup (T \times P)$ is a set of arcs (flow relation),
- $W: F \rightarrow \{1, 2, 3, \ldots\}$ is a weight function,
- $M_0: P \rightarrow \{0, 1, 2, 3, \ldots\}$ is the initial marking,
- $P \cap T = \emptyset$ and $P \cup T \neq \emptyset$.

A Petri net structure $N = (P, T, F, W)$ without any specific initial marking is denoted by $N$.

A Petri net with the given initial marking is denoted by $(N, M_0)$.

---

A net $N$ is constituted by

- a set $S$ of places,
- a set $T$ of transitions such that $S \cap T = \emptyset$, and
- a set $F$ of directed arcs (flow relation), $F \subseteq (S \cup T) \times (S \cup T)$, satisfying

$$F \cap (S \times S) = F \cap (T \times T) = \emptyset.$$
The behavior of many systems can be described in terms of system states and their changes. In order to simulate the dynamic behavior of a system, a state or marking in a Petri nets is changed according to the following transition (firing) rule:

1) A transition $t$ is said to be enabled if each input place $p$ of $t$ is marked with at least $w(p, t)$ tokens, where $w(p, t)$ is the weight of the arc from $p$ to $t$.

2) An enabled transition may or may not fire (depending on whether or not the event actually takes place).

3) A firing of an enabled transition $t$ removes $w(p, t)$ tokens from each input place $p$ of $t$, and adds $w(t, p)$ tokens to each output place $p$ of $t$, where $w(t, p)$ is the weight of the arc from $t$ to $p$.

A marking of a net $N$ is a mapping $m: S_N \rightarrow \mathbb{N}$ where $\mathbb{N} = \{0, 1, 2, \ldots\}$. A place $s$ is marked by a marking $m$ if $m(s) > 0$. The null marking is the marking which maps every place to 0.

A transition $t$ is enabled by a marking $m$ if $m$ marks all places in $t^*$. In this case $t$ can occur. Its occurrence transforms $m$ into the marking $m'$, defined for each place $s$ by

$$m'(s) = \begin{cases} 
    m(s) - 1 & \text{if } s \in t^* - t^*, \\
    m(s) + 1 & \text{if } s \in t^* - t, \\
    m(s) & \text{otherwise}.
\end{cases}$$
Basic Properties
Basic properties of a marked Petri net

Definition 9 (Basic properties). Let $N = (P, T, F, W)$ be a Petri net and $M \in MB(P)$ be a marking.

- $(N, M)$ is **terminating** if and only if there is a $k \in \mathbb{N}$ such that $|\sigma| \leq k$ for any firing sequence $\sigma$ (i.e., $(N, M)[\sigma]$).
- $(N, M)$ is **deadlock-free** if and only if for any $M' \in R(N, M)$ there exists a transition $t$ such that $(N, M')[t]$.
- $(N, M)$ is **live** if and only if for any $t \in T$ and any $M' \in R(N, M)$ there exists a $M'' \in R(N, M')$ such that $(N, M'')[t]$.
- $(N, M)$ is **bounded** if and only if there is a $k \in \mathbb{N}$ such that for any $M' \in R(N, M)$ and any $p \in P$: $M'(p) \leq k$.
- $(N, M)$ is **safe** if and only if for any $M' \in R(N, M)$ and any $p \in P$: $M'(p) \leq 1$.
- $(N, M)$ is **reversible** if and only if for any $M' \in R(N, M)$: $M \in R(N, M')$. 
\((N, M)\) is terminating if and only if there is a \(k \in \mathbb{N}\) such that 
\(|\sigma| \leq k\) for any firing sequence \(\sigma\) (i.e., \((N, M)[\sigma]\)).
Deadlock-free

\((N, M)\) is *deadlock-free* if and only if for any \(M' \in \mathcal{R}(N, M)\) there exists a transition \(t\) such that \((N, M')[t]\).
Liveness

Transition $t \in T$ is live in $(N, M)$ if and only if for any $M' \in \mathcal{R}(N, M)$ there exists a $M'' \in \mathcal{R}(N, M')$ such that $(N, M'')[t]$.

$(N, M)$ is live if all of its transitions are live.
Basic idea of liveness

- All reachable markings
- Markings where t is enabled
Boundedness

Place $p \in P$ is $k$-bounded in $(N, M)$ if and only if for any $M' \in R(N, M)$: $M'(p) \leq k$.

Place $p \in P$ is bounded in $(N, M)$ if and only if there is a $k \in \mathbb{N}$ such that $p$ is $k$-bounded.

$(N, M)$ is bounded if and only if all of its places are bounded.
Place $p \in P$ is *safe* in $(N, M)$ if and only if $p$ is 1-bounded.

$(N, M)$ is *safe* if and only if all of its places are safe.
(\(N, M\)) is \textit{reversible} if and only if for any \(M' \in R(N, M)\): \(M \in R(N, M')\).

Marking \(M'\) is a \textit{home marking} in \((N, M)\) if it is reachable from any reachable marking, i.e., for any \(M'' \in R(N, M)\): \(M' \in R(N, M'')\).

\((N, M)\) is \textit{reversible} if and only if \(M\) is a home marking.
Reachability Graph
Definition 10 (Reachability graph). Let $N = (P, T, F, W)$ be a Petri net and $M \in IB(P)$ be a marking. The reachability graph of $(N, M)$ is the graph $(V, E)$ with as vertices $V = R(N, M)$ the set of all reachable markings and as edges $E = \{(M', t, M'') \in V \times T \times V \mid ((N, M')[t](N, M''))\}$ the set of all possible state changes. Note that $(M', t, M'') \in E$ denotes that $M''$ is reachable from $M'$ by firing $t$. 

\[
(N, M')[t](N, M'')
\]
Reachability graph algorithm

1) Label the initial marking $M_0$ as the root and tag it "new".

2) While "new" markings exists, do the following:
   a) Select a new marking $M$.
   b) If no transitions are enabled at $M$, tag $M$ "dead-end".
   c) While there exist enabled transitions at $M$, do the following for each enabled transition $t$ at $M$:
      i. Obtain the marking $M'$ that results from firing $t$ at $M$.
      ii. If $M'$ does not appear in the graph, add $M'$ and tag it "new".
      iii. Draw an arc with label $t$ from $M$ to $M'$ (if not already present).

3) Output the graph.
Step 1: Label the initial marking $M_0$ as the root and tag it "new" (indicated by green color).

Example

[p1,free,p4]
Example (continued)

[p1,free,p4]

[p2,free,p4]  [p1,free,p4]  [p2,free,p4]

[p1,free,p5]
Example (continued)
Example (continued)
Example (continued)
Example (continued)
Example (continued)

[Diagram of a Petri net with transitions t1, t2, t3, t4 and places p1, p2, p3, p4, p5, and tokens representing [p1, free, p4], [p2, free, p4], [p1, free, p5], [p2, free, p5], [p1, p3, p4], [p2, p3, p4], [p1, p3, p5], [p2, p3, p5].]
Example (continued)
Example (complete)

- The marked Petri net is:
  - deadlock free
  - live
  - bounded
  - safe
  - reversible
  - all markings are home markings
Coverability Graph
Problem

ps. \((n,m)\) is a shorthand for \([p_1^n, p_2^m]\)
Coverability tree algorithm

1) Label the initial marking $M_0$ as the root and tag it "new".

2) While "new" markings exists, do the following:
   a) Select a new marking $M$ and remove the "new" tag.
   b) If $M$ is identical to a marking on the path from the root to $M$, then tag $M$ "old" and go to another new marking.
   c) If no transitions are enabled at $M$, tag $M$ "dead-end".
   d) While there exist enabled transitions at $M$, do the following for each enabled transition $t$ at $M$:
      i. Obtain the marking $M'$ that results from firing $t$ at $M$.
      ii. If, on the path from the root to $M$, there exists a marking $M''$ such that $M'(p) \geq M''(p)$ for each $p$ and $M' \neq M''$ (i.e., $M''$ is coverable), then replace $M'(p)$ by $\omega$ for each $p$ such that $M'(p) > M''(p)$.
      iii. Introduce $M'$ as a node, draw an arc with label $t$ from $M$ to $M'$, and tag $M'$ "new".

3) Output the tree.
Example

Step 1: Label the initial marking $M_0$ as the root and tag it "new" (indicated by green color).
Example (continued)

Step 2: While "new" markings exists, do the following:

- **Select a new marking** $M$ **and remove the "new" tag.**
- **If** $M$ **is identical to a marking on the path from the root to** $M$, **then tag** $M$ **"old" and go to another new marking.**
- **If no transitions are enabled at** $M$, **tag** $M$ **"dead-end".**
- **While there exist enabled transitions at** $M$, **do the following for each enabled transition** $t$ **at** $M$:
  - **Obtain the marking** $M'$ **that results from firing** $t$ **at** $M$.
  - **If**, on the path from the root to $M$, **there exists a marking** $M''$ **such that** $M'(p) \geq M''(p)$ **for each** $p$ **and** $M' \neq M''$ **(i.e.,** $M''$ **is coverable)**, **then replace** $M'(p)$ **by** $\omega$ **for each** $p$ **such that** $M'(p) > M''(p)$.
  - **Introduce** $M'$ **as a node, draw an arc with label** $t$ **from** $M$ **to** $M'$, **and tag** $M'$ **"new"**
Example (continued)

Step 2: While "new" markings exist, do the following:

- Select a new marking $M$ and remove the "new" tag.
- If $M$ is identical to a marking on the path from the root to $M$, then tag $M$ "old" and go to another new marking.
- If no transitions are enabled at $M$, tag $M$ "dead-end".
- While there exist enabled transitions at $M$, do the following for each enabled transition $t$ at $M$:
  - Obtain the marking $M'$ that results from firing $t$ at $M$.
  - If, on the path from the root to $M$, there exists a marking $M''$ such that $M'(p) \geq M''(p)$ for each $p$ and $M' \neq M''$ (i.e., $M''$ is coverable), then replace $M'(p)$ by $\omega$ for each $p$ such that $M'(p) > M''(p)$.
  - Introduce $M'$ as a node, draw an arc with label $t$ from $M$ to $M'$, and tag $M'$ "new"
Example (continued)

Step 2: While "new" markings exists, do the following:

- Select a new marking $M$ and remove the "new" tag.
- If $M$ is identical to a marking on the path from the root to $M$, then tag $M$ "old" and go to another new marking.
- If no transitions are enabled at $M$, tag $M$ "dead-end".
- While there exist enabled transitions at $M$, do the following for each enabled transition $t$ at $M$:
  - Obtain the marking $M'$ that results from firing $t$ at $M$.
  - If, on the path from the root to $M$, there exists a marking $M''$ such that $M'(p) \geq M''(p)$ for each $p$ and $M' \neq M''$ (i.e., $M''$ is coverable), then replace $M'(p)$ by $\omega$ for each $p$ such that $M'(p) > M''(p)$.
  - Introduce $M'$ as a node, draw an arc with label $t$ from $M$ to $M'$, and tag $M'$ "new"
Example (complete)

Step 3: Output the tree.

Coverability graph:
Another example

Step 1: Label the initial marking $M_0$ as the root and tag it "new" (indicated by green color).

Step 2 ...
Example (continued)
Example (continued)
Example (continued)
Example (continued)

Step 3: Output the tree.

[p1,p3]  [p1,p2^ω,p3]  [p1,p2^ω,p3]
  \[\omega\]  \[\omega\]  \[\omega\]
t1 \[p1,p2^ω,p3]  \[p1,p2^ω,p3]  \[p1,p2^ω,p3]
t1 \[\omega\]  \[\omega\]  \[\omega\]
[p1,p2^ω,p3,p4^ω]  [p1,p2^ω,p3,p4^ω]  [p1,p2^ω,p3,p4^ω]
  \[\omega\]  \[\omega\]  \[\omega\]
t2 \[p1,p2^ω,p3,p4^ω]  \[p1,p2^ω,p3,p4^ω]  \[p1,p2^ω,p3,p4^ω]
t2 \[\omega\]  \[\omega\]  \[\omega\]
[p1,p2^ω,p3,p4^ω]  [p1,p2^ω,p3,p4^ω]  [p1,p2^ω,p3,p4^ω]
  \[\omega\]  \[\omega\]  \[\omega\]
t1 \[p1,p2^ω,p3,p4^ω]  \[p1,p2^ω,p3,p4^ω]  \[p1,p2^ω,p3,p4^ω]
t2 \[\omega\]  \[\omega\]  \[\omega\]
[p1,p2^ω,p3,p4^ω]  [p1,p2^ω,p3,p4^ω]  [p1,p2^ω,p3,p4^ω]
  \[\omega\]  \[\omega\]  \[\omega\]
t1 \[p1,p2^ω,p3,p4^ω]  \[p1,p2^ω,p3,p4^ω]  \[p1,p2^ω,p3,p4^ω]
t2 \[\omega\]  \[\omega\]  \[\omega\]
[p1,p2^ω,p3,p4^ω]  [p1,p2^ω,p3,p4^ω]  [p1,p2^ω,p3,p4^ω]
  \[\omega\]  \[\omega\]  \[\omega\]
t1 \[p1,p2^ω,p3,p4^ω]  \[p1,p2^ω,p3,p4^ω]  \[p1,p2^ω,p3,p4^ω]
t2 \[\omega\]  \[\omega\]  \[\omega\]
[p1,p2^ω,p3,p4^ω]  [p1,p2^ω,p3,p4^ω]  [p1,p2^ω,p3,p4^ω]
  \[\omega\]  \[\omega\]  \[\omega\]
t1 \[p1,p2^ω,p3,p4^ω]  \[p1,p2^ω,p3,p4^ω]  \[p1,p2^ω,p3,p4^ω]
t2 \[\omega\]  \[\omega\]  \[\omega\]
[p1,p2^ω,p3,p4^ω]  [p1,p2^ω,p3,p4^ω]  [p1,p2^ω,p3,p4^ω]
  \[\omega\]  \[\omega\]  \[\omega\]
Example (complete)

Coverability graph
Coverability graph

• Take the coverability tree and simply merge nodes with identical labels
Another example

marked net

reachability graph

coverability tree

coverability graph

ps. \((n,m)\) is a shorthand for \([p_1^n, p_2^m]\)
\omega\text{-markings}

**Definition 11 (\omega\text{-marking}).** Let \( N = (P, T, F, W) \) be a Petri net with initial marking \( M' \).

An \( \omega \)-marking \( M \) of \( N \) is an extended multi-set over \( P \), i.e., \( M \in A \rightarrow (IN \cup \{\omega\}) \).

If \( M(p) = \omega \), then place \( p \in P \) is said to be unbounded in \( M \).
If \( M(p) \neq \omega \) for all \( p \in P \), then \( M \) is said to be \( \omega \)-free.

\( M \) is a reachable \( \omega \)-marking of \( (N, M') \) if and only if it appears in the coverability graph of \( (N, M') \).
Properties

• The coverability tree/graph is always finite.
• The marked Petri net is bounded if and only if the corresponding coverability tree/graph contains only $\omega$-free markings.
• The coverability tree/graph gives an over-approximation.
• Different Petri nets may have the same coverability tree/graph.
Theorem 1 (Relation). Let $N = (P, T, F, W)$ be a Petri net and $M \in IB(P)$ be a marking. Let $M'$ be an $\omega$-marking appearing in the coverability graph of $(N, M)$ and $n \in \mathbb{N}$ an arbitrary number.

There exists an $M'' \in R(N, M)$ such that for all $p \in P$:

- If $M'(p) \neq \omega$, then $M''(p) = M'(p)$.
- If $M'(p) = \omega$, then $M''(p) \geq n$.

Let $n=180$. There is a reachable marking with 0 tokens in $p1$ and at least 180 tokens in $p2$. 
Example (readers and writers)

construct coverability graph ...
Coverability tree
Coverability graph
Coverability graph (vector notation)

\[
\begin{align*}
&\quad (1,0,0,1,0) \\
&\quad \quad t1 \rightarrow (0,1,0,1,0) \\
&\quad \quad \quad t4 \rightarrow (0,1,0,0,1) \\
&\quad \quad \quad \quad t4 \rightarrow (0,1,0,0,1) \\
&\quad \quad \quad \quad \quad t1 \rightarrow (0,1,0,0,1) \\
&\quad \quad \quad \quad \quad \quad t2 \rightarrow (1,0,1,0,1) \\
&\quad \quad \quad \quad \quad \quad \quad t2 \rightarrow (1,0,1,0,1) \\
&\quad \quad \quad \quad \quad \quad \quad \quad t2 \rightarrow (1,0,1,0,1) \\
&\quad \quad \quad \quad \quad \quad \quad \quad \quad t1 \rightarrow (1,0,\omega,1,0) \\
&\quad \quad \quad \quad \quad \quad \quad \quad \quad \quad t4 \rightarrow (0,1,\omega,1,0) \\
&\quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad t3 \rightarrow (0,1,\omega,0,1) \\
&\quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad t2 \rightarrow (1,0,\omega,0,1)
\end{align*}
\]
Analysis results

- \( p_1, p_2, p_4, p_5 \) are safe
- \( p_3 \) is unbounded
- \([p_2,p_5]\) is reachable
- \([p_1,p_2]\) is not reachable
- \([p_1,p_3^{180},p_5]\) is coverable
Additional properties

• A transition $t$ is dead if and only if it does not appear in the coverability graph.
• The coverability graph and reachability graph are identical if the marked Petri net is bounded (i.e., only $\omega$-free markings).
• The marked Petri net is safe if only 0's and 1's appear in nodes.
• Any firing sequence of the marked Petri net can be matched by a "walk" through the coverability graph.
• The reverse is not true!!!!
Limitation: Loss of information

Two nets with the same coverability graph!

\{[p1], [p1, p2^1], [p1, p2^2], [p1, p2^3], [p1, p2^4], ...\}

\{[p1], [p1, p2^3], [p1, p2^6], [p1, p2^9], [p1, p2^{12}], ...\}
State-explosion problem (1)

\[2^{n+1} \text{ states}\]
State-explosion problem (2)

Each round the number of tokens in s can be doubled.

place s is $2^n$ bounded
Variants

• Construct the coverability graph on the fly (i.e., do not first construct the coverability tree): the graph may become smaller but process is typically non-deterministic.

• Several approaches have been proposed to construct "minimal" coverability graphs/sets (see "Alain Finkel: The Minimal Coverability Graph for Petri Nets. Applications and Theory of Petri Nets 1991: 210-243", and "Gilles Geeraerts, Jean-François Raskin, Laurent Van Begin: On the Efficient Computation of the Minimal Coverability Set for Petri Nets. ATVA 2007: 98-113")
Conclusion
The coverability graph is finite but ...

- some information gets lost in case of unbounded behavior, and
- it may be huge and impossible to construct.

Next: structural methods like invariants, siphons, traps, etc.
After this lecture you should be able to:

- Understand the formalizations, i.e., \((P,T,F,W), M, (N,M)[t>(N,M')],\) etc.
- Determine whether a concrete marked net is terminating, deadlock-free, live, bounded, safe, and/or reversible, whether a transition is live and/or dead, whether a place is \(k\)-bounded, etc.
- Construct a Petri net that has a set of desirable properties, e.g., a net that is live and bounded but not reversible.
- Construct the reachability graph of a marked net.
- Construct the coverability tree of a marked net.
- Construct the coverability graph of a marked net.
- Tell which properties can(not) be derived from the coverability tree/graph.
- Understand the limitations of the coverability tree/graph (loss of information, inability to decide liveness, etc.).
- Derive conclusions from a concrete coverability tree/graph.
Appendix: Formalization of Coverability Graph based on Desel & Reisig
Coverability tree & graph

- Idea: cut-off unbounded behavior using omega (ω) markings

Formally, an $\omega$-marking of a net $N$ is a mapping $\overline{m}: S_N \rightarrow \mathbb{N} \cup \{\omega\}$ where $\omega \notin \mathbb{N}$. Clearly, every (conventional) marking can be viewed as a particular $\omega$-marking without $\omega$-entries.

$(1,0,\omega,1,\omega,1,2,0)$

$\omega$-markings are interpreted as follows: If a marking $m'$ is reachable from a marking $m$ and satisfies $m'(s) \geq m(s)$ for each place $s$, the occurrence sequence leading from $m$ to $m'$ can be iterated arbitrarily often (Proposition 5). If moreover $m'(s_0) > m(s_0)$ for some place $s_0$ then the number of tokens on $s_0$ increases with each iteration of the occurrence sequence. This increasing sequence of markings is now replaced by one $\omega$-marking $\overline{m'}$ with $\overline{m'}(s_0) = \omega$, denoting that, for each $b \in \mathbb{N}$, there is a reachable marking that coincides with $m'$ for all places except $s_0$ and assigns at least $b$ tokens to $s_0$. More generally, several places may map to $\omega$, representing simultaneous growth of the token count on these places.
Trivial example

marked net
reachability graph
coverability tree
coverability graph
Extended example

marked net

reachability graph

coverability tree

coverability graph
Approach

1. Define omega ($\omega$) occurrence sequences.
2. Show that these are finite.
3. Construct coverability tree.
4. Construct coverability graph.
Example of a $\omega$-occurrence sequence

- $\omega$-occurrence sequence: $t1 \ t1$
- $(1,0) - t1 -> (1, \omega)$ - $t1 -> (1, \omega)$

```
(1,0)  
|  t1
(1,\omega)  
|  t1  
(1,\omega)
```

marked net:

```
p1  
\arrow{t1}  
\arrow{p2}  
\arrow{t2}
```
A (finite or infinite) sequence of transitions \( t_1 \ t_2 \ t_3 \ldots \) is an \( \omega \)-occurrence sequence of a marked net with initial marking \( m_0 \) if there exist \( \omega \)-markings \( \overline{m}_0, \overline{m}_1, \overline{m}_2, \ldots \) such that \( m_0 \) and \( \overline{m}_0 \) coincide for all places and, for each index \( i \) occurring in the sequence \( t_1 \ t_2 \ t_3 \ldots \) the following conditions hold:

1. For each place \( s \) in \( \bullet t_i \), either \( \overline{m}_{i-1}(s) > 0 \) or \( \overline{m}_{i-1}(s) = \omega \) (the enabling condition).

2. For each place \( s \) satisfying \( \overline{m}_i(s) \neq \omega \),

\[
\overline{m}_i(s) = \overline{m}_{i-1}(s) - |F_N \cap \{(s, t_i)\}| + |F_N \cap \{(t_i, s)\}|
\]

(the conventional marking transformation).

3. A place \( s \) satisfies \( \overline{m}_i(s) = \omega \) if and only if
   - either \( \overline{m}_{i-1}(s) = \omega \) (places marked by \( \omega \) remain marked by \( \omega \)),
   - or \( \overline{m}_{i-1}(s) \neq \omega \) and there exists an index \( j, j < i \), such that \( \overline{m}_j(s) \neq \omega \) and \( \overline{m}_j(s) < \overline{m}_{i-1}(s) - |F_N \cap \{(s, t_i)\}| + |F_N \cap \{(t_i, s)\}| \)

and \( \overline{m}_j(s') \leq \overline{m}_{i-1}(s') - |F_N \cap \{(s', t_i)\}| + |F_N \cap \{(t_i, s')\}| \) for each place \( s' \) satisfying \( \overline{m}_j(s') \neq \omega \) and \( \overline{m}_{i-1}(s') \neq \omega \) (places with increasing token count are marked by \( \omega \)).

4. If \( i > 1 \) then \( \overline{m}_{i-1} \notin \{\overline{m}_0, \ldots, \overline{m}_{i-2}\} \) (after reaching an \( \omega \)-marking the second time, the sequence stops).

We call an \( \omega \)-marking \( \overline{m} \) reachable in a marked net if some \( \omega \)-occurrence sequence leads to \( \overline{m} \).
(1) Transitions need to be enabled

Only $t_1$ is enabled in $(1,0)$, not $t_2$.

(1) For each place $s$ in $\bullet t_i$, either $m_{i-1}(s) > 0$ or $m_{i-1}(s) = \omega$ (the enabling condition).
(2) For non-$\omega$ place markings: business as usual

\[ m_i(s) = m_{i-1}(s) - |F_N \cap \{(s,t_i)\}| + |F_N \cap \{(t_i,s)\}| \]

(the conventional marking transformation).
3) Introducing omegas

(1,ω) is "reachable" from (1,0) because there is a j (j=0) such that ...

(3) A place s satisfies $\overline{m}_i(s) = \omega$ if and only if

- either $\overline{m}_{i-1}(s) = \omega$
  (places marked by $\omega$ remain marked by $\omega$),
- or $\overline{m}_{i-1}(s) \neq \omega$ and there exists an index $j, j < i$, such that $\overline{m}_j(s) \neq \omega$
  and $\overline{m}_j(s) < \overline{m}_{i-1}(s) - |F_N \cap \{(s, t_i)\}| + |F_N \cap \{(t_i, s)\}|$
  and $\overline{m}_j(s') \leq \overline{m}_{i-1}(s') - |F_N \cap \{(s', t_i)\}| + |F_N \cap \{(t_i, s')\}|$ for each place $s'$ satisfying $\overline{m}_j(s') \neq \omega$ and $\overline{m}_{i-1}(s') \neq \omega$
  (places with increasing token count are marked by $\omega$).
(4) Stop after second identical marking

Marking $(0, \omega)$ is dead while $(1, \omega)$ markings are not continued after second occurrence.

\[(4) \text{ If } i > 1 \text{ then } \overline{m}_{i-1} \notin \{\overline{m}_0, \ldots, \overline{m}_{i-2}\} \]

(after reaching an $\omega$-marking the second time, the sequence stops).
Finite?

- How long can a $\omega$-occurrence sequence be?
- How many $\omega$-occurrence sequences are there?
- Is the coverability tree/graph finite?
Lemma 17. Let $S$ be a finite set and let $\varphi_1 \varphi_2 \varphi_3 \ldots$ be an infinite sequence of mappings from $S$ to $\mathbb{N} \cup \{\omega\}$. There exists an infinite sequence of indices $i_1 i_2 i_3 \ldots$ which is strongly monotonic (i.e., $i_1 < i_2 < i_3 < \ldots$) such that, for each $s$ in $S$,

$$\varphi_{i_1}(s) \leq \varphi_{i_2}(s) \leq \varphi_{i_3}(s) \leq \ldots$$
Proof. We prove the following stronger proposition: For each subset $S'$ of $S$, there exists an infinite strongly monotonic sequence of indices $i_1, i_2, i_3, \ldots$ such that, for each $s$ in $S'$, $\varphi_{i_1}(s) \leq \varphi_{i_2}(s) \leq \varphi_{i_3}(s) \leq \cdots$. We proceed by induction on the number of elements in $S'$.

Base. If $S' = \emptyset$ then nothing has to be shown.

Step. Assume $S' \neq \emptyset$ and let $s \in S'$. By the induction hypothesis, there exists an infinite strongly monotonic sequence $i_1, i_2, i_3, \ldots$ such that, for each $s'$ in $S' \setminus \{s\}$,

$$\varphi_{i_1}(s') \leq \varphi_{i_2}(s') \leq \varphi_{i_3}(s') \leq \cdots.$$ 

Now we restrict the sequence $i_1, i_2, i_3, \ldots$ to indices $i_k$ satisfying

$$\varphi_{i_k}(s) \leq \varphi_{i_{k+1}}(s), \quad \varphi_{i_k}(s) \leq \varphi_{i_{k+2}}(s), \quad \varphi_{i_k}(s) \leq \varphi_{i_{k+3}}(s) \ldots$$

Clearly, the obtained sequence $i_{k_1}, i_{k_2}, i_{k_3}, \ldots$ satisfies the required property

$$\varphi_{i_{k_1}}(s) \leq \varphi_{i_{k_2}}(s) \leq \varphi_{i_{k_3}}(s) \leq \cdots$$

for each place $s$ in $S'$. This sequence is infinite because, for each index $i_k$, every index $i_l$ in $\{i_{k+1}, i_{k+2}, i_{k+3} \ldots\}$ satisfying

$$\varphi_{i_l}(s) \leq \varphi_{i_{k+1}}(s), \varphi_{i_{k+2}}(s), \varphi_{i_{k+3}}(s) \ldots$$

belongs to the sequence, too. Such an index $i_l$ always exists because every nonempty subset of $\mathbb{N} \cup \{\omega\}$ has a minimal element. \qed
Theorem 18. Every $\omega$-occurrence sequence of a finite marked net is finite.

Proof. By contraposition, assume a finite marked net that has an infinite $\omega$-occurrence sequence $t_1 t_2 t_3 \ldots$, 

$$\overline{m}_1 \xrightarrow{t_1} \overline{m}_2 \xrightarrow{t_2} \overline{m}_3 \xrightarrow{t_3} \ldots.$$ 

By Dickson's Lemma (Lemma 17), there exists an infinite strongly monotonic sequence of indices $i_1, i_2, i_3 \ldots$ such that, for each place $s$,

$$\overline{m}_{i_1}(s) \leq \overline{m}_{i_2}(s) \leq \overline{m}_{i_3}(s) \leq \ldots.$$ 

Let $i$ and $j$ be two subsequent indices of the sequence $i_1, i_2, i_3 \ldots$. By the definition of $\omega$-occurrence sequences (4) no $\omega$-marking appears twice in an infinite $\omega$-occurrence sequence. Hence $\overline{m}_i(s) \neq \overline{m}_j(s)$ for at least one place $s$. By the definition of $\omega$-occurrence sequences (3), $\overline{m}_i(s) \neq \omega$ and $\overline{m}_j(s) = \omega$. Again by (3), no place $s$ satisfies $\overline{m}_i(s) = \omega$ and $\overline{m}_j(s) \neq \omega$. Hence $\overline{m}_j$ has more places with $\omega$-entries than $\overline{m}_i$. Therefore, the set of places with $\omega$-entries increases infinitely, contradicting the finiteness of the set of all places of the net. \qed
Coverability tree

Diagrams are a bit misleading: vertices labeled with a $\omega$-marking are really sequences, e.g., initial node is $\varepsilon$ rather than $(1,0)$.

Formally, the coverability tree of a marked net is defined as a directed graph with a distinguished initial vertex and edges labeled by transitions:

- the vertices are the finite $\omega$-occurrence sequences,
- a distinguished initial vertex is given by the empty sequence $\varepsilon$ (which by definition is an $\omega$-occurrence sequence),
- labeled edges are all triples $(\sigma, t, \sigma t)$ such that $\sigma$ as well as $\sigma t$ are $\omega$-occurrence sequences.
Finiteness

Theorem 19. The coverability tree of a finite marked net is finite.$^8$

Proof. By contraposition, assume a finite marked net with an infinite coverability tree. Each vertex $\sigma$ of the coverability tree has only finitely many immediate successors, one for each transition enabled by the $\omega$-marking reached by $\sigma$. Hence every vertex $\sigma$ with infinitely many successors has at least one immediate successor which also has infinitely many successors. By assumption, the initial vertex $\varepsilon$ has infinitely many successors. Hence, starting with $\varepsilon$, we can construct an infinite directed path of the tree. The concatenation of the labels of the edges of this path yields an infinite $\omega$-occurrence sequence — contradicting Theorem 18.

Corollary 20. A finite marked net has finitely many reachable $\omega$-markings.
Example

Fig. 12. An unbounded marked Petri net
Marking graph  
(i.e., reachability graph)
Coverability tree

find the error (also in paper)...
Relation $\omega$-markings and normal markings

**Theorem 21.** Let $\overline{m}$ be a reachable $\omega$-marking of a finite marked net. For each $b$ in $\mathbb{N}$, there is a reachable marking $m$ such that every place $s$ satisfies:

- if $\overline{m}(s) \neq \omega$ then $m(s) = \overline{m}(s)$,
- if $\overline{m}(s) = \omega$ then $m(s) \geq b$.

Let $b=180$. There is a marking reachable with 0 tokens in $p_1$ and at least 180 tokens in $p_2$. 
Boundedness = "all $\omega$-markings are $\omega$-free"

**Theorem 23.** A place $s$ of a marked net is not bounded if and only if some reachable $\omega$-marking $\overline{m}$ satisfies $\overline{m}(s) = \omega$ (i.e., some vertex of the coverability tree represents the $\omega$-marking $\overline{m}$).

**Proof.**

$(\Leftarrow)$ follows immediately from Theorem 21.

$(\Rightarrow)$ Since there are only finitely many reachable $\omega$-markings by Theorem 19 there is a number $b \in \mathbb{N}$ such that each reachable $\omega$-marking $\overline{m}$ satisfies either $\overline{m}(s) = \omega$ or $\overline{m}(s) < b$. Since $s$ is not bounded, some reachable marking $m$ satisfies $m(s) \geq b$. Since $m(s)$ does not coincide with $\overline{m}(s)$ for any reachable $\omega$-marking $\overline{m}(s)$, there exists some reachable $\omega$-marking $\overline{m}$ satisfying $\overline{m}(s) = \omega$ by Theorem 22. \qed
Corollary 24. A place $s$ of a marked net is b-bounded if and only if each reachable $\omega$-marking $m$ satisfies $m(s) \neq \omega$ and $m(s) \leq b$.

$p1$ is 1-bounded (safe)
$p2$ is unbounded
Dead transitions do not appear in cov.

dead transitions do not appear in cov.

dead transitions do not appear in cov.

dead transitions do not appear in cov.

**Theorem 25.** A transition \( t \) of a marked net is dead if and only if \( t \) does not occur in any \( \omega \)-occurrence sequence (i.e., some arc of the coverability tree is labeled by \( t \)).

**Proof.**

(\( \iff \)) Assume some reachable marking \( m \) enables \( t \). By Theorem 22, a corresponding reachable \( \omega \)-marking \( \overline{m} \) satisfies \( \overline{m}(s) \neq 0 \) for each place \( s \) in \( \bullet t \). Hence, this \( \omega \)-marking enables \( t \), too.

(\( \Rightarrow \)) Assume some reachable \( \omega \)-marking \( \overline{m} \) enables \( t \). By Theorem 21, there is a corresponding reachable marking \( m \) that marks all places satisfying \( \overline{m} = \omega \) at least once. This marking \( m \) enables \( t \), too.

\( \square \)
The **coverability graph** of a marked net is defined as an arc-labeled directed graph with a distinguished initial vertex and edges labeled by transitions:

- the *vertices* are the reachable \( \omega \)-markings,
- the distinguished *initial vertex* is given by the \( \omega \)-marking that coincides with the initial marking for each place,
- labeled edges are given by all triples \((\overline{m}, t, \overline{m}')\) such that \(\overline{m}\) and \(\overline{m}'\) are reachable \(\omega\)-markings satisfying \(\overline{m} \xrightarrow{t} \overline{m}'\).
Boundedness implies equivalence

**Theorem 27.** The coverability graph and the marking graph of a bounded marked net are identical (up to different co-domains of markings and $\omega$-markings).

**Proof.** The result follows immediately from Corollary 26 and the definition of $\omega$-occurrence sequences. $\square$
Appendix: Examples taken from Murata
The coverability tree for a Petri net \((N, M_0)\) is constructed by the following algorithm.

Step 1) Label the initial marking \(M_0\) as the root and tag it "new."

Step 2) While "new" markings exist, do the following:
   Step 2.1) Select a new marking \(M\).
   Step 2.2) If \(M\) is identical to a marking on the path from the root to \(M\), then tag \(M\) "old" and go to another new marking.
   Step 2.3) If no transitions are enabled at \(M\), tag \(M\) "dead-end."
   Step 2.4) While there exist enabled transitions at \(M\), do the following for each enabled transition \(t\) at \(M\):
      Step 2.4.1) Obtain the marking \(M'\) that results from firing \(t\) at \(M\).
      Step 2.4.2) On the path from the root to \(M\) if there exists a marking \(M''\) such that \(M'(p) \geq M''(p)\) for each place \(p\) and \(M' \neq M''\), i.e., \(M''\) is coverable, then replace \(M'(p)\) by \(\omega\) for each \(p\) such that \(M'(p) > M''(p)\).
      Step 2.4.3) Introduce \(M'\) as a node, draw an arc with label \(t\) from \(M\) to \(M'\), and tag \(M'\) "new."
Example

$\begin{align*}
M_0 &= (1 \ 0 \ 0) \\
M_1 &= (0 \ 0 \ 1) \\
&M_2 = (1 \ \omega \ 0) \\
&M_3 = (1 \ \omega \ 0) \\
&M_4 = (0 \ \omega \ 1) \\
&M_5 = (0 \ \omega \ 1) \\
&M_6 = (1 \ \omega \ 0)
\end{align*}$

"dead-end"
Some of the properties that can be studied by using the coverability tree $T$ for a Petri Net $(N, M_0)$ are the following:

1) A net $(N, M_0)$ is bounded and thus $R(M_0)$ is finite iff (if and only if) $\omega$ does not appear in any node labels in $T$.
2) A net $(N, M_0)$ is safe iff only 0’s and 1’s appear in node labels in $T$.
3) A transition $t$ is dead iff it does not appear as an arc label in $T$.
4) If $M$ is reachable from $M_0$, then there exists a node labeled $M'$ such that $M \leq M'$.
Coverability graph
Fig. 19. Two Petri nets having the same coverability tree
(a) A live Petri net. (b) A nonlive Petri net.

Fig. 20. (a) The coverability tree for both Petri nets shown in Fig. 19(a) and 19(b). (b) The coverability graph for the two nets shown in Fig. 19(a) and 19(b).