Petri nets: Structural analysis
Structural Analysis: Motivation

We shall consider another class of techniques that can extract information about the behaviour of the system by analyzing it locally (i.e., without first constructing an object that represents the entire behaviour of the net).

This class of techniques is called structural analysis. Some its components are:

- Place invariants
- Traps
Example 1
Let $N = \langle P, T, F, W, M_0 \rangle$ be a P/T net. The corresponding incidence matrix $C : P \times T \rightarrow \mathbb{Z}$ is the matrix whose rows correspond to places and whose columns correspond to transitions. Column $t \in T$ denotes how the firing of $t$ affects the marking of the net: $C(t, p) = W(t, p) - W(p, t)$.

The incidence matrix of Example 1:

$$
\begin{pmatrix}
-1 & 0 & 1 & 0 & 0 & 0 \\
1 & -1 & 0 & 0 & 0 & 0 \\
0 & 1 & -1 & 0 & 0 & 0 \\
0 & -1 & 1 & 0 & -1 & 1 \\
0 & 0 & 0 & -1 & 0 & 1 \\
0 & 0 & 0 & 1 & -1 & 0 \\
0 & 0 & 0 & 0 & 1 & -1 \\
\end{pmatrix}
$$
Markings as vectors

Let us now write markings as column vectors. E.g., the initial marking in Example 1 is $M_0 = (1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0)^T$.

Likewise, we can write firing counts as column vectors with one entry for each transition. E.g., if each of the transitions $t_1$, $t_2$, and $t_4$ fires once, we can express this with $u = (1 \ 1 \ 0 \ 1 \ 0 \ 0)^T$.

Then, the result of firing these transitions can be computed as $M_0 + C \cdot u$.

\[
\begin{pmatrix}
1 \\
0 \\
0 \\
1 \\
1 \\
0 \\
0
\end{pmatrix}
+ 
\begin{pmatrix}
-1 & 0 & 1 & 0 & 0 & 0 \\
1 & -1 & 0 & 0 & 0 & 0 \\
0 & 1 & -1 & 0 & 0 & 0 \\
0 & -1 & 1 & 0 & -1 & 1 \\
0 & 0 & 0 & -1 & 0 & 1 \\
0 & 0 & 0 & 1 & -1 & 0 \\
0 & 0 & 0 & 0 & 1 & -1
\end{pmatrix}
\cdot 
\begin{pmatrix}
1 \\
1 \\
0 \\
1 \\
0 \\
0 \\
0
\end{pmatrix}
= 
\begin{pmatrix}
0 \\
0 \\
1 \\
1 \\
0 \\
1 \\
0
\end{pmatrix}
\]
Let $N$ be a P/T net with indiscence matrix $C$, and let $M, M'$ be two markings of $N$. The following implication holds:

If $M' \in \text{reach}(M)$, then there exists a vector $u$ such that $M' = M + C \cdot u$ such that all entries in $u$ are natural numbers.

Notice that the reverse implication does not hold in general! E.g., bi-directional arcs (an arc from a place to a transition and back) cancel each other out in the matrix. For instance, if Example 1 contained a bi-directional arc between $p_1$ and $t_3$, the matrix would remain the same, but the marking $\{p_3, p_6\}$ (obtained on the previous slide) would be unreachable!
Let $N$ be a P/T net with indicence matrix $C$, and let $M, M'$ be two markings of $N$. The following implication holds:

If $M' \in \text{reach}(M)$, then there exists a vector $u$ such that $M' = M + C \cdot u$ such that all entries in $u$ are natural numbers.

Notice that the reverse implication does not hold in general!

E.g., bi-directional arcs (an arc from a place to a transition and back) cancel each other out in the matrix. For instance, if Example 1 contained a bi-directional arc between $p_1$ and $t_3$, the matrix would remain the same, but the marking $\{p_3, p_6\}$ (obtained on the previous slide) would be unreachable!
A more complicated example:

Even though we have

\[
\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} -1 & 1 \\ 1 & -1 \\ -1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix},
\]

none of the sequences corresponding to \((1 \ 1)^T\), i.e. \(t_1t_2\) or \(t_2t_1\), can happen.
Proving unreachability using the incidence matrix

To summarize: The markings obtained by computing with the incidence matrix are an over-approximation of the actual reachable markings.

However, we *can* sometimes use the matrix equations to show that a marking $M$ is *unreachable*. (Compare coverability graphs. . .)

I.e., a corollary of the previous implication is that if $M' = M + Cu$ has no natural solution for $u$, then $M' \notin \text{reach}(M)$.

Note: When we are talking about natural (integral) solutions of equations, we mean those whose components are natural (integral) numbers.
Example 3

Consider the following net and the marking $M = (1 \ 1)^T$.

$$
\begin{pmatrix}
1 \\
0
\end{pmatrix}
+ 
\begin{pmatrix}
-1 & 1 \\
1 & -1
\end{pmatrix}
\cdot 
\begin{pmatrix}
u_1 \\
u_2
\end{pmatrix}
= 
\begin{pmatrix}
1 \\
1
\end{pmatrix}
$$

has no solution, and therefore $M$ is not reachable.
Place invariants

Let $N$ be a net and $C$ its incidence matrix. A natural solution of the equation $C^T x = 0$ such that $x \neq 0$ is called a place invariant (or: P-invariant) of $N$.

Notice that a P-invariant is a vector with one entry for each place.

For instance, in Example 1, $x_1 = (1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0)^T$, $x_2 = (0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1)^T$, and $x_3 = (0 \ 0 \ 0 \ 1 \ 1 \ 1)^T$ are all P-invariants.

A P-invariant indicates that the number of tokens in all reachable markings satisfies some linear invariant (see next slide).
Properties of P-invariants

Let $M$ be marking reachable with a transition sequence whose firing count is expressed by $u$, i.e. $M = M_0 + Cu$. Let $x$ be a P-invariant. Then, the following holds:

$$M^T x = (M_0 + Cu)^T x = M_0^T x + (Cu)^T x = M_0^T x + u^T C^T x = M_0^T x$$

For instance, invariant $x_2$ means that all reachable markings $M$ satisfy (switching to the functional notation for markings):

$$M(p_3) + M(p_4) + M(p_7) = M_0(p_3) + M_0(p_4) + M_0(p_7) = 1$$  \hspace{1cm} (1)

As a special case, a P-invariant in which all entries are either 0 or 1 indicates a set of places in which the number of tokens remains unchanged in all reachable markings.
Note that linear combinations of P-invariants (i.e. multiplying an invariant by a constant or component-wise addition of two invariants) will again yield a P-invariant.

We can use P-invariants to prove mutual exclusion properties.

Example: According to equation 1, in every reachable marking of Example 1 exactly one of the places $p_3, p_4,$ and $p_7$ is marked. In particular, $p_3$ and $p_7$ cannot be marked concurrently!
Traps

Let \( \langle P, T, F, W, M_0 \rangle \) be a P/T net. A trap is a set of places \( S \subseteq P \) such that \( S^\bullet \subseteq \bullet S \).

In other words, each transition which removes tokens from a trap must also put at least one token back to the trap.

A trap \( S \) is called marked in marking \( M \) iff for at least one place \( s \in S \) it holds that \( M(s) \geq 1 \).

Note: If a trap \( S \) is marked initially (i.e. in \( M_0 \)), then it is also marked in all reachable markings.
In Example 4 (see next slide), $S_1 = \{nc_1, nc_2\}$ is a trap.

The only transitions that remove tokens from this set are $t_2$ and $t_5$. However, both also add new tokens to $S_1$.

$S_1$ is marked initially, and therefore in all reachable markings $M$ the following inequality holds: $M(nc_1) + M(nc_2) \geq 1$

Traps can be useful in combination with place invariants to recapture information lost in the incidence matrix due to the cancellation of self-loop arcs.
Example 4

Consider the following attempt at a mutual exclusion algorithm for $cr_1$ and $cr_2$:

```
<table>
<thead>
<tr>
<th></th>
<th>t1</th>
<th>q1</th>
<th>t2</th>
<th>t3</th>
<th>q2</th>
<th>t4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>pend1</td>
<td>cr1</td>
<td>nc1</td>
<td>cr2</td>
<td>nc2</td>
<td>cr2</td>
</tr>
</tbody>
</table>

The idea is to achieve mutual exclusion by entering the critical section only if the other process is not already there.
Proving mutual exclusion properties using traps

In Example 4, we want to prove that in all reachable markings $M$, $cr_1$ and $cr_2$ cannot be marked at the same time. This can be expressed by the following inequality:

$$M(cr_1) + M(cr_2) \leq 1$$

The P-invariants we can derive in the net yield these equalities:

$$M(q_1) + M(pend_1) + M(cr_1) = 1 \quad (2)$$
$$M(q_2) + M(pend_2) + M(cr_2) = 1 \quad (3)$$
$$M(cr_1) + M(nc_1) = 1 \quad (4)$$
$$M(cr_2) + M(nc_2) = 1 \quad (5)$$

However, these equalities are insufficient to prove the desired property!
Recall that $S_1 = \{nc_1, nc_2\}$ is a trap.

$S_1$ is marked initially and therefore in all reachable markings $M$. Thus:

$$M(nc_1) + M(nc_2) \geq 1 \quad (6)$$

Now, adding (4) and (5) and subtracting (6) yields $M(cr_1) + M(cr_2) \leq 1$, which proves the mutual exclusion property.
Unfoldings
Unfoldings are a data structure that represents the behaviour of a Petri net.

We will study it for 1-safe nets.

Unfoldings represent a trade-off in terms of time/space requirements; their size is in between that of a net and its reachability graph, and checking whether a marking is reachable becomes easier than for the net, but more difficult than from the reachability graph.
Unfoldings for finite transition systems

Let $\mathcal{T}$ be a finite transition system with initial state $X$. One can define the acyclic unfolding $U_{\mathcal{T}}$ (which is used for CTL model checking):

![Diagram of Upsilon notation]

Remark: $U_{\mathcal{T}}$ can be viewed as a structure in which every state is labelled by a state from $\mathcal{T}$. We denote this labelling by the function $B$.

$U_{\mathcal{T}}$ contains the same behaviours as $\mathcal{T}$ (and the same reachable states). Additionally, $U_{\mathcal{T}}$ has a simpler structure (acyclic, in fact, a tree). However, in general, $U_{\mathcal{T}}$ is infinite.
Prefixes

$\mathcal{P}$ is called a prefix of $U_T$ if $\mathcal{P}$ is obtained by “pruning” arbitrary branches of $U_T$. Example:

\[
\begin{array}{c}
X \\
Y \\
Z \\
\vdots
\end{array} \quad \xrightarrow{\text{pruning}} \quad \begin{array}{c}
X \\
Y \\
Z \\
X
\end{array}
\]

Observation: One can always find a finite prefix containing the same reachable states as the infinite unfolding (by unrolling loops exactly once). We shall call such a prefix complete.
Construction of complete prefixes

Let us discuss an algorithm to obtain a complete prefix of $U_T$.

The algorithm maintains a set $E$, the set of states observed so far.

Some arcs in the prefix will be called cutoffs, we shall mark them red.
1. Initially, the prefix contains only the root, labelled by $X$. We set $\mathcal{E} := \{X\}$.

2. Select a node $n$ on the prefix that is not the target of a cutoff edge. Let $B(n) = Y$ be the label of the node, and let $Z$ be a state with $Y \rightarrow Z$ such that the prefix does not contain any edge from $n$ to a $Z$-labelled node.

2a. If no such pair $n, Z$ exists, we are done.

2b. Otherwise, add a new, $Z$-labelled node to the prefix and add an edge from $n$ to it.

2c. If $Z \in \mathcal{E}$, then the new edge is a cutoff. Otherwise, set $\mathcal{E} := \mathcal{E} \cup \{Z\}$.

3. Continue at step 2.
Example

Step-by-step construction of the prefix in the previous example:

Observation (1): A complete prefix contains as many transitions as $T$.

Observation (2): The shape of the prefix depends on the order in which edges are added!
The unfolding of a Petri net $\mathcal{P}$ (or, a prefix of the same) is an infinite acyclic Petri net $\mathcal{U}$. We shall be interested in computing a finite prefix $\mathcal{Q}$ of $\mathcal{U}$.

Remark: In the following, we call the places of $\mathcal{Q}$ conditions, the transitions of $\mathcal{Q}$ events. This merely serves to better distinguish the elements of $\mathcal{P}$ and $\mathcal{Q}$, functionally they are the same!
Every condition of $Q$ is labelled by a place of $P$, every event of $Q$ by a transition of $P$.

Every event $e$ is of the form $(S, t)$, where $S$ is the preset of $e$ and $t$ the label of $e$.

Let $S$ be a set of conditions. $B(S)$ denotes the set of places labelling the elements of $S$.

Every condition has exactly one incoming arc.
Unfolding construction for Petri nets

We first discuss the construction of $U$ (possibly infinite).

1. Let $m_0$ be the initial marking of $P$. Then the initial marking of $U$ contains exactly one condition for each place in $m_0$.

2. Let $S$ the subset of a reachable marking in $U$. Let $B(S) = \bullet t$ for some transition $t$ of $P$ such that $(S, t)$ is not yet contained in $U$.

2a. If no such pair $(S, t)$ exists, we are done.

2b. Add the event $e := (S, t)$ to the prefix (with $S$ as preset and label $t$). Moreover, extend the prefix by one condition for every output place of $t$ and make it an output place of $e$. 
Example 1: Petri net...
...and a possible prefix of the unfolding
We shall now amend the construction so that it prunes certain branches of the unfolding, creating a *finite* prefix.

More precisely, certain events will be called *cutoffs*. These events lead to markings that we have already seen.
Prefix construction for Petri nets

1. Let $m_0$ be the initial marking of $\mathcal{P}$. Then the initial marking of $\mathcal{Q}$ contains exactly one condition for each place in $m_0$. We set $\mathcal{E} := \{m_0\}$.

2. Let $S$ the subset of a reachable marking in $\mathcal{Q}$. Suppose that no element of $S$ is the output place of a cutoff event. Let $B(S) = \bullet t$ for some transition $t$ of $\mathcal{P}$ such that $(S, t)$ is not yet contained in $\mathcal{Q}$.

2a. If no such pair $(S, t)$ exists, we are done.

2b. Add the event $e := (S, t)$ to the prefix (with $S$ as preset and label $t$). Moreover, extend the prefix by one condition for every output place of $t$ and make it an output place of $e$.

2c. We associate with $e$ a marking $m_e$ (which is reachable in $\mathcal{P}$) (see below). If $m_e \in \mathcal{E}$, then $e$ is a cutoff. Otherwise $\mathcal{E} := \mathcal{E} \cup \{m_e\}$.
Determining $m_e$

For the event $e = (S, t)$, we determine $m_e$, a marking of $P$, as follows:

**Idea:** $m_e$ is the label of the marking obtained by making the “minimal” effort to fire $e$.

Let $x, y$ be two nodes (conditions or events) in $Q$. Let $<$ be the smallest partial order where $x < y$ if there is an edge from $x$ to $y$.

Let $x$ be a node of $Q$. We define $\lfloor x \rfloor := \{ y \mid y \leq x \}$.

Let $m_e$ be the labels of the marking obtained by firing the events of $\lfloor e \rfloor$ (in any order). **Note:** Such a firing sequence exists due to the properties of $S$. 
Complete prefixes

Let $\mathcal{P}$ be a Petri net and $\mathcal{Q}$ a prefix of its unfolding $\mathcal{U}$ with labelling $B$. We call $\mathcal{Q}$ complete if it satisfies the following property:

A marking $m$ is reachable in $\mathcal{P}$ iff a marking $m'$ with $B(m') = m$ is reachable in $\mathcal{Q}$.

Thus, if $\mathcal{Q}$ is complete, we can decide reachability in $\mathcal{P}$ by examining $\mathcal{Q}$.

Unfortunately, the algorithm given previously does not always produce a complete prefix. Indeed, its shape depends on the order in which events are added. We shall discuss an example that demonstrates this effect.
Example 2

Consider the following Petri net:
In Example 2 the marking \( \{p\} \) is reachable, e.g. by firing \( A \ B \ T \).

The net can also reach the marking \( \{e, f\} \) by firing either \( A \ C \) or \( B \ D \), and then return by firing \( E \ F \) to the initial marking.

We shall see that a prefix generated according to depth-first order will “overlook” the transition \( T \).
Depth-first order generated the prefix shown below (order and cutoffs indicated in red):
Configurations

Let $m$ be a reachable marking in $\mathcal{U}$ and let $C$ be the set of events in $\bigcup_{c \in m} [c]$. Then we call $C$ a configuration.

A configuration $C$ represents a set of events that can all fire in one execution. Given $C$, we denote the marking (of $\mathcal{U}$) reached by such an execution by $m_C$.

Remark: For every event $e$, the set $[e] =: C_e$ is a configuration. We have $B(m_{C_e}) = m_e$.

We call $E$ an extension of $C$ iff $C \cap E = \emptyset$ and $C \cup E$ is a configuration. In this case, we write $C \oplus E$ to denote the configuration $C \cup E$.

Let $C, C'$ be two configurations such that $B(m_C) = B(m_{C'})$. If $E$ is an extension of $C$, then there is an extension $E'$ of $C'$ that is isomorphic to $E$. 
Adequate orders

Let $\prec$ be a well-founded total order on configurations that refines $\subset$ (i.e. $C \subset C'$ implies $C \prec C'$).

**Intuition:** $\prec$ is a possible order in which the events of $\mathcal{U}$ can be generated; i.e., $e$ is added before $e'$ if $C_e \prec C_{e'}$.

Let $Q \prec$ be the prefix of $\mathcal{U}$ generated by adding events in the order given by $\prec$ as above.

We call $\prec$ adequate iff $Q \prec$ is complete.
A sufficient condition for adequate orders

The following condition guarantees that $\prec$ is adequate:

Let $C, C'$ be two configurations with $C \prec C'$ and $B(m_C) = B(m_{C'})$, and let $E$ an extension of $C$ and $E'$ the extension of $C'$ isomorphic to $E$. Then $D \prec D'$ must hold, where $D = C \oplus E$ and $D' = C' \oplus E'$.

Proof: Let $\prec$ be an order satisfying the above constraint. We show that $Q_\prec$ is complete. So let $m$ be a marking reachable in $P$. Then there is a marking $m'$ in $U$ with $B(m') = m$. Let $C'$ be the configuration containing the events in $\bigcup_{c \in m'}[c]$. Either $C'$ is contained in $Q_\prec$, or $C' = C_{e'} \oplus E'$ for some cutoff event $e'$. But then there is another event $e$ with $m_e = m_{e'}$ and $C_e \prec C_{e'}$ and therefore a configuration $C := C_e \oplus E$, where $E$ is isomorphic to $E'$, and we have $B(m_C) = B(m_{C'}) = m$. Now, since $C_e \prec C_{e'}$ we have $C \prec C'$. Either $C$ is contained in $Q_\prec$, or one repeats the argument, but only finitely often since $\prec$ is well-founded.
Conflict, causality, concurrency

From the structure of the unfolding we can derive statements about the mutual relationships of conditions:

Let $c, d$ be two (different) conditions of $Q$.

- **$c, d$ are called causally dependent** if $c < d$ or $d < c$. (I.e., in every firing sequence containing both conditions, one condition must be consumed to generate the other.)

- **$c, d$ are in conflict** if there are events $e, f$ (where $e \neq f$), $e \in [c]$, $f \in [d]$, and $\bullet e \cap \bullet f \neq \emptyset$. (I.e., $c, d$ can never occur in a reachable marking of $Q$!)

- **$c, d$ are called concurrent** if they are neither causally dependent nor in conflict with one another.
Concurrent conditions are jointly reachable

Let $C$ be a set of conditions. Then $C$ is a subset of a reachable marking in $U$ iff all conditions in $C$ are mutually concurrent.

Proof ("$\Rightarrow$": Obvious.

Proof ("$\Leftarrow$": (sketch) Let $E$ be the set of events in $\bigcup_{c \in C} \mathcal{C}_c$. Induction on the size of $E$: obvious for $E = \emptyset$, otherwise remove a maximal event $e$ from $E$ and prove that $(C \setminus e^\bullet) \cup e^\bullet$ is mutually concurrent.
Theorem: Let $P$ be a Petri net and $Q$ a complete unfolding prefix. Given $Q$ and a marking $m$ of $P$, it is NP-complete to determine whether $m$ is reachable in $P$.

Proof: Membership in NP: guess a marking $m'$ of $Q$ such that $B(m') = m$, check if it does not contain causally dependent or conflicting conditions.

Hardness: polynomial reduction from SAT (proof on blackboard)
Reducing reachability to SAT

In the other direction, we can, given $m$ and $Q$, produce a propositional logic formula, of polynomial size in $|m| + |Q|$, that is satisfiable iff $m$ is reachable in $\mathcal{P}$. This makes sense because extremely efficient SAT solvers are available.

The formula uses one boolean variable for each event and each condition. Its satisfying assignments are those that correspond to a reachable marking $m'$ (i.e. concurrent sets of conditions) in $Q$.

The formula assigns “true” to the conditions and events in $\bigcup_{c \in m'}[c]$ and false to all others; then it checks that no condition in $m'$ is consumed by one of the events in that set and that no condition is consumed twice.

Finally, one demands that the image of $m'$ in $\mathcal{P}$ is $m$. 
Remarks

Remark (1): Notice that the unfolding and most of the formula is independent of $m$ and needs to be generated from $P$ only once for an arbitrary number of reachability queries.

Remark (2): In a very similar way, one can check whether $P$ contains a deadlock, i.e. a reachable marking that does not enable any transition.