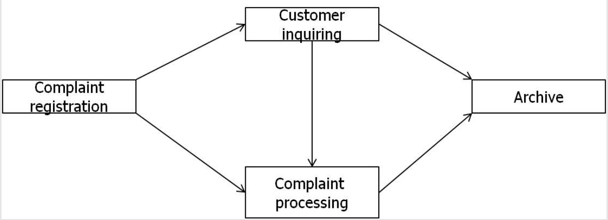
Chapter 12: Modeling and Analysis of Distributed Applications

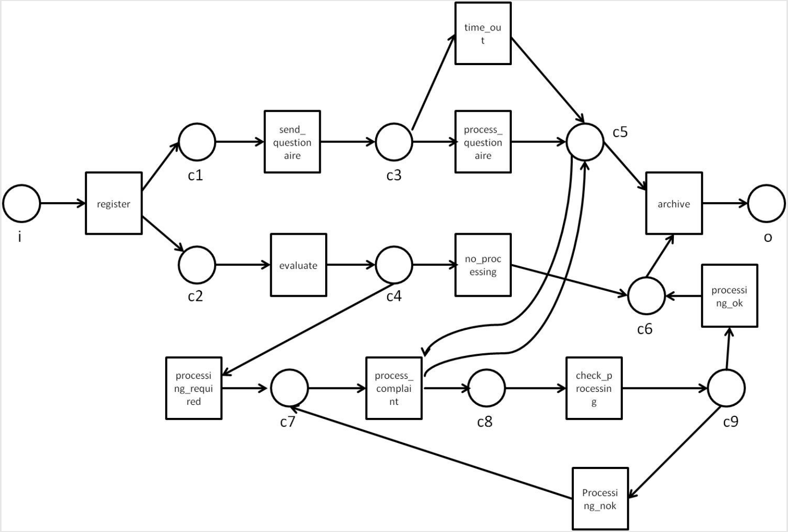
Petri-Nets

- 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.

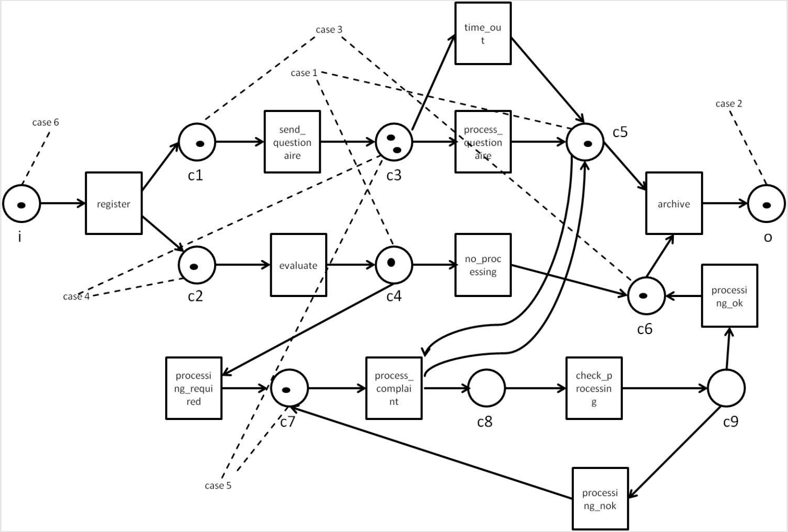


Complaints processing: formal Petri-net orchestration.[1]

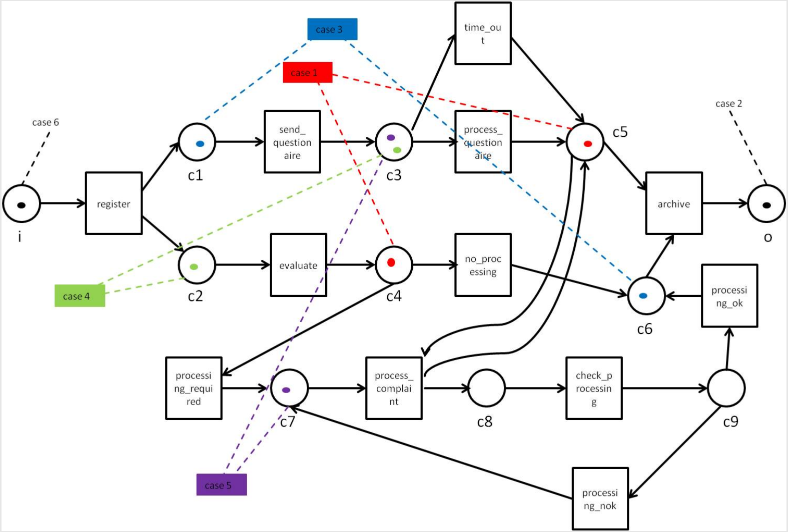


[1] van der Aalst: The Application of Petri nets to Workflow Management. Journal of Circuits, Systems, and Computers 8(1): 21-66 (1998)

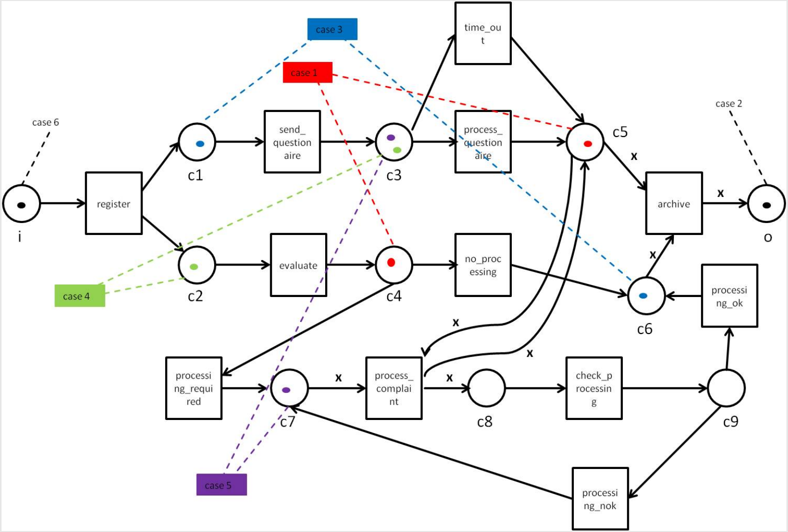
Complaints processing: more than one complaint



Complaints processing: how to distinguish complaints



Complaints processing: keeping things together



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, causual 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.

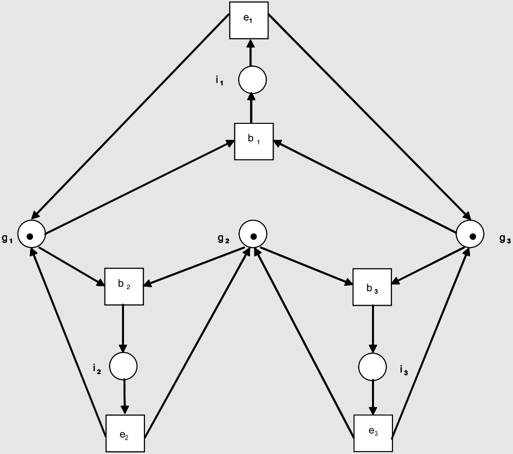
Section 12.1 Elementary System Nets

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 *occurence* of activities.

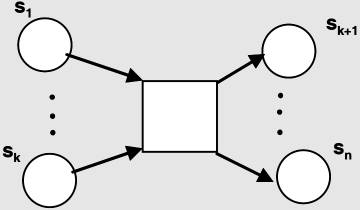
3-Philosopher-Problem

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



A transition *may* occur when certain conditions with respect to the markings of its directly connected places are fulfilled; the *occurence* 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 *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 $dom(F) \cup cod(F) = P \cup T$.

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 NAT is called a *marking* of P.

A mapping $P \to NAT \cup \{\omega\}$ is called ω-*marking*. ω represents an infinitly large number of tokens.

Arithmetic of ω:

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

where $n \in NAT, n > 0$.

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,
- $V : F \rightarrow NAT^+$ a *multiplicity*,
- m_0 a *marking* called *initial marking*.

N is called *ordinary* eS-Net, whenever $V(f) = 1, \forall f \in F$.

A 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:

$$m'(p) := \begin{cases} m(p) - V(p,t) + V(t,p) & \text{falls } p \in Ft, p \in tF, \\ m(p) - V(p,t) & \text{falls } p \in Ft, p \notin tF, \\ m(p) + V(t,p) & \text{falls } p \notin Ft, p \in tF, \\ m(p) & \text{sonst.} \end{cases}$$

Transitions and markings in terms of vectors

Let places in P be linearily ordered.

- Markings of a net can be considered as vectors of nonnegative integers of dimension $\mid P \mid$, called *place-vectors*.
- Transitions t can be characterized as vectors of nonnegative integers of dimension $\mid P \mid$, called *transition vectors* $\Delta t, t^+, t^-$:

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

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

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

$$\Delta t(p) := t^+(p) - t^-(p).$$

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 $t^- \leq m$,
- $m[\, t \succ m'$ 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* $[\, * \succ$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.

- $R_N(m) := \{m' \mid m[*\succ m'\}$, 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,
- $\Delta w := \sum_{i=1}^{n} \Delta t_i$, wobei $w = t_1 t_2 \ldots t_n$.

Results

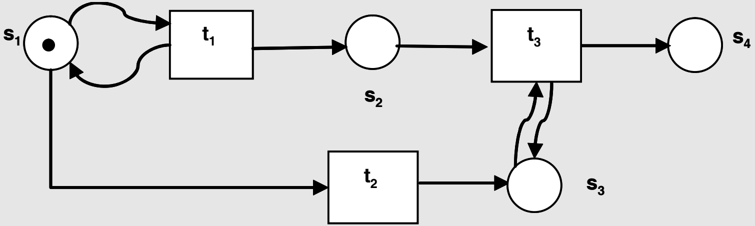
- $[*\succ$ is reflexiv and transitiv.
- $m[w\succ m' \Rightarrow (m+m^*)[w\succ(m'+m^*), \forall m^* \in NAT^{|S|}$. (Monotonie)
- $m[w\succ m' \Rightarrow m' = m + \Delta w$.

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:



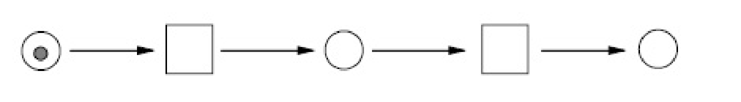
$$\begin{aligned} R_N(m_0) = \{ \quad & (1,0,0,0),(1,1,0,0),(1,2,0,0),(1,3,0,0),\ldots, \\ & (0,0,1,0),(0,1,1,0),(0,2,1,0),(0,3,1,0),\ldots, \\ & (0,0,1,1),(0,1,1,1),(0,0,1,2),(0,2,1,1),(0,1,1,2),(0,0,1,3),\ldots\} \\ L_N(m_0) = \{ \quad & \epsilon, t_1, t_1t_1, t_1t_1t_1, \ldots, \\ & t_2, t_1t_2, t_1t_1t_2, t_1t_1t_1t_2, \ldots, \\ & t_1t_2t_3, t_1t_1t_2t_3, t_1t_1t_2t_3t_3, t_1t_1t_1t_2t_3, t_1t_1t_1t_2t_3t_3, t_1t_1t_1t_2t_3t_3t_3, \ldots\} \end{aligned}$$

Section 12.2 Control Patterns

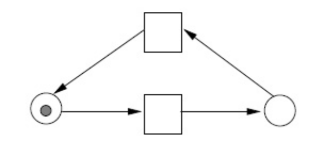
- eS-nets can be used to model *causal dependencies*; for modelling temporal aspects extensions of the formalism are required.
- Whenever between some transitions there are no causal dependencies, the transitions are called *concurrent*; concurrency is a prerequisite for parallelism.

Some typical causalities

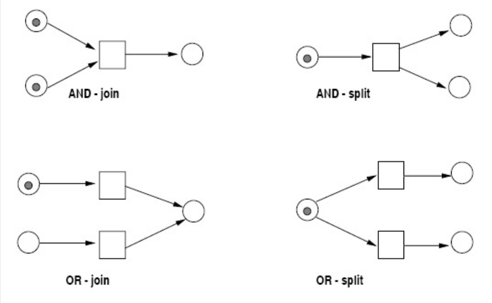
Sequence



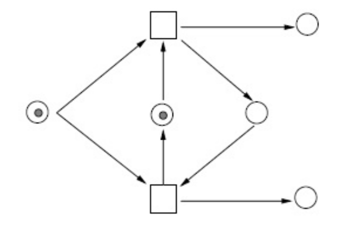
Iteration



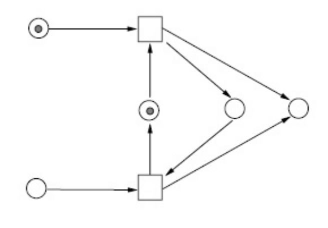
AND-join, OR-join, AND-split, OR-split



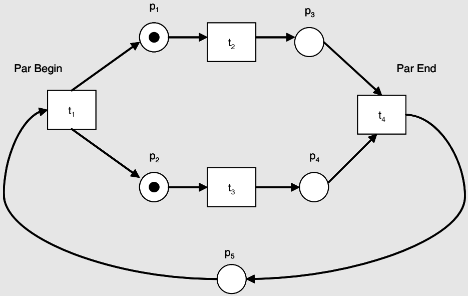
OR-Split with regulation



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 $k \in NAT^+$. 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 $k \in NAT^+$.
- 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 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 proof $\Rightarrow$ we first proof:

Lemma

For each infinite sequence of markings (m_i) of markings there exists an infinite subsequencev (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 $\Rightarrow$

- 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 infinitly many paths. Let $m_0 \to m_1$ be one such edge.
- The same argument can be applied w.r.t. m_1 such that we get $m_0 \to m_1 \to m_2$, where $m_1 \to m_2$ is part of an infinite number of paths.
- The above construction can be repeated infinitly 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.

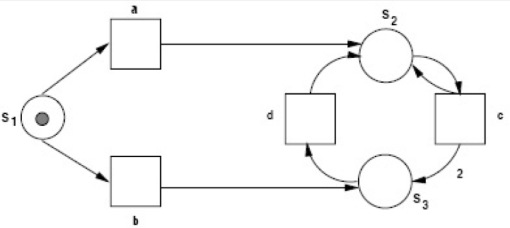
Coverability

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

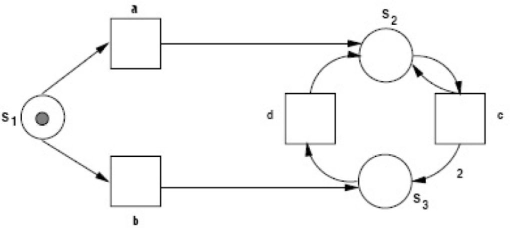
Let $N = (P, T, F, V, m_0)$ a eS-Net. The *Coverability Graph* of N is given by $CG(N) := (R, B)$ as follows:

- *inductive definition of an auxiliary tree $T(N)$:*

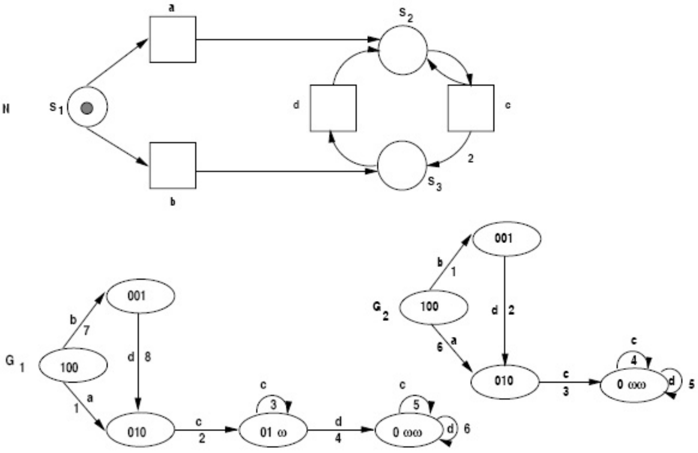
  The values of the nodes in $T(N)$ are ω-markings of N. The value of the root node r is m_0. Let m be the value of some node n of $T(N)$, $t \in T$, and $m[\,t \succ m'$.

  - 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.

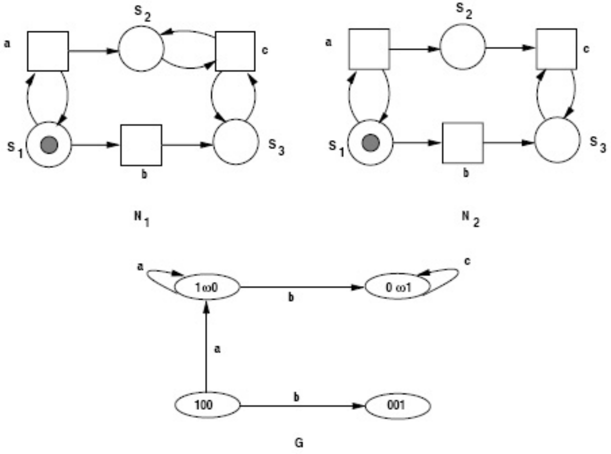
Give a coverability tree.



A eS-net with two different coverability graphs.



Two eS-Nets with identical coverability graphs.



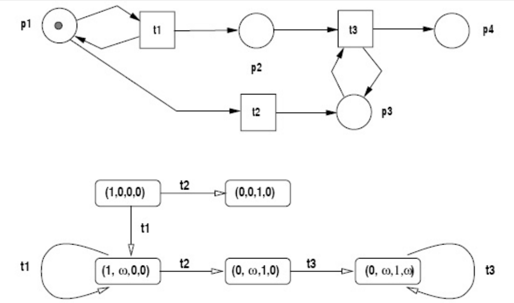
Theorem

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 ω-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 ω 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 $w = t_1^6 t_2 t_3^3$.

Live, dead and deadlockfree

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

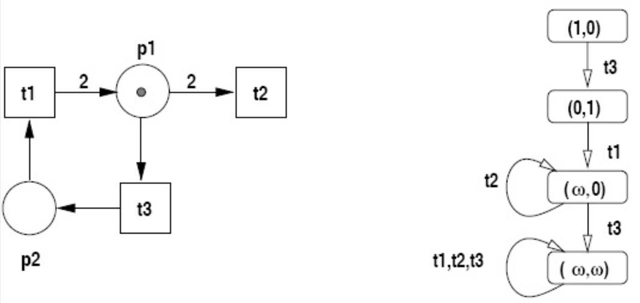
- A marking m is called *dead* in N, if there is no $t \in T$ which is enabled at m.
- A transition t is called *dead* at marking m, if there is no marking reachable from m, such that t is enabled.

  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 transitionen $t \in T$ 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!



Lifeness cannnot be tested by inspection of the coverability graph.

Do there exist other techniques for analysis?

Section 12.4 Invariants

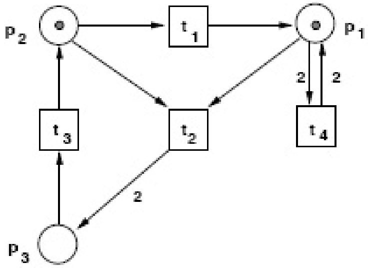
Basics

- A Petri-net invariant is a property of a Petri-net, which holds for any marking, respectively transition word, of the net.
- We study place- and transition-invariants, which are based on a matrix representation of a net, respectively vector representation of markings and transitions.

Incidence Matrix

- Let $N = (P, T, F, V, m_0)$ a eS-Net, $T = \{t_1, \ldots, t_n\}$, $P = \{p_1, \ldots, p_m\}$, $n, m \geq 1$.
- A vector of dimension n (m) is called T- (P-)vector.
- For any $t \in T$, Δt can be represented as a column P-vector.
- The *incidence matrix* of N is given as a $m \times n$-matrix $C = (\Delta t_1, \ldots, \Delta t_n)$, respectively $C = (c_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}$, where $c_{ij} := \Delta t_j(s_i)$.

Example



$$C = \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & -1 & 1 & 0 \\ 0 & 2 & -1 & 0 \end{pmatrix}$$

- Incidence matrices are independent of concrete markings,
- In case of loops, information concerning multiplicities is lost.

Parikh-Vektor

The transpose of a vector x, resp. matrix C is denoted by $x^\top$, bzw. $C^\top$.

The *Parikh-Vektor* $\bar{q}$ of some $q \in W(T)$ is a column T-vector, $n = \mid T \mid$, defined as follows:

$$\bar{q} : T \to NAT, \text{ where } \bar{q}(t) \text{ is the number of occurences of } t \text{ in } q.$$

State Equation

Let $q \in W(T)$ and m, m' markings.

If $m[\,q \succ m'$, then $\sum_{t \in T} (\bar{q}(t) \cdot \Delta t) = C \cdot \bar{q} = \Delta q$.

Moreover, as $m[\,q \succ m'$, we have

- $m' = m + \Delta q^\top$.

  The equation:

  $$m' = m + (C \cdot \bar{q})^\top$$

  is called *state equation*.
- The system of linear equations given by

  $$C \cdot x = (m' - m)^\top$$

  has an integer nonnegative solution x.

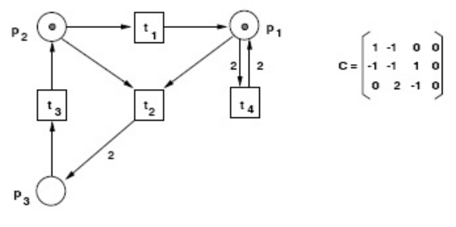
however the following does not hold in general:

If $C \cdot x = (m' - m)^\top$ has an integer nonnegative solution then

$$\exists q \in W(T) : m[\, q \succ m',$$

I.e., the reachability problem cannot be solved, in general.

Example



Let $m = (1, 0, 0)$, $m' = (0, 0, 1)$.
$x = (0, 1, 1, 0)^\top$ is a solution for $C \cdot x = (m' - m)^\top$, however we cannot find a word which can be fired at m.

Theorem

Let N be a eS-Net and Δ a P-vector. There exists a marking m^* and a word $q \in W(T)$, such that $m^*[\, q \succ (m^* + \Delta)$, iff $C \cdot x = \Delta^\top$ has an integer nonnegative solution.

Proof:
"$\Rightarrow$": trivial.

"$\Leftarrow$": Let $m^* := \sum_{t \in T} x(t) \cdot t^-$.

Corollary

Let $N = (P, T, F, V, m_0)$ be a eS-Net. There exists a marking m^* such that $N = (P, T, F, V, m^*)$ unbounded, iff $C \cdot x > 0$ has an integer nonnegative solution.

Useful application of the corollary:

If there does not exist an integer nonnegative solution for $C \cdot x > 0$, then for any initial marking, N is bounded.

Transition-Invariants (T-Invariants)

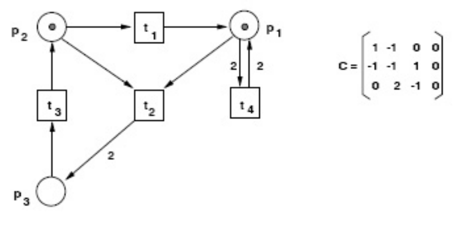
Let $N = (P, T, F, V, m_0)$ be a eS-Net.

- Any nontrivial integer solution x of the homogenous linear equation system $C \cdot x = 0$ is called *transition-invariant (T-invariant)* of N.
- A T-invariant x is called *proper*, if $x \geq 0$.
- A T-invariant x is called *realizable* in N, if there exists a word $q \in W(T)$ with $\bar{q} = x$ and a reachable marking m such that $m[\, q \succ m$.
- N is called *covered with T-invariants*, if there exists a T-invariant x of N with all components positive, i.e. greater than 0.

Proper T-invariants denote *possible* cycles of the reachability graph - realizable T-invariants denote cycles which indeed may occur.

Example

T-invariants of



are as follows:

$$x = \lambda_1 \begin{pmatrix} 1 \\ 1 \\ 2 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

where λ_1, λ_2 integers.

Theorem

Let $N = (S, T, F, V, m_0)$ be a eS-Net. If there exists a marking m, such that N live and bounded at m, then N covered by T-invariants.

Proof: Let N live and bounded at some m.

As N is live at m, there exists a word $q_1 \in L_N(m)$, which contains all transitions in T and the marking $m + \Delta q_1$ is reachable from m.

Moreover, N is live at $m + \Delta q_1$ as well. Therefore, there exits a word $q_2 \in L_N(m)$, which contains all transitions in T and N is live at the marking $m + \Delta q_1 q_2$.

There exists an infinite sequence of markings (m_i), where $m_i := m + \Delta q_1 \ldots q_i$, such that:

$$m[\, q_1 \succ m_1[\, q_2 \succ m_2 \ldots m_i[\, q_{i+1} \succ m_{i+1} \ldots$$

As N is bounded at m, there is only a finite number of markings which are reachable. Therefore, there exist $i, j \in NAT : i < j$ such that $m_i = m_j$. Thus

$$m_i[\, q_{i+1} \ldots q_j \succ m_j = m_i$$

As all these q_i mention all transitions, we finally conclude

$$x = \bar{q}_{i+1} + \ldots + \bar{q}_j$$

is a T-Invariant which covers N.

Useful application of the theorem:

Whenever N is not covered by T-invariants, then for every marking it holds N not live or not bounded.

Place-Invariants (P-Invariants)

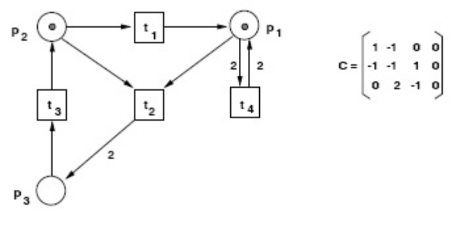
Let $N = (P, T, F, V, m_0)$ be a eS-Net.

- Any nontrivial integer solution y of the homogeneous linear equation system $y \cdot C = 0$ is called *place-invariant (P-invariant)* of N.
- A P-invariant y is called *proper P-invariant*, if $y \geq 0$.
- N is called *covered with P-invariants*, if there exists a P-invariant y with all components positive, i.e. greater than 0.

If y is a P-invariant, then for any marking m the sum of the number of tokens on the places p is invariant with respect to the firing of the transitions weighted by $y(p)$.

Example

P-invariants of



are as follows:

$$y^T = \lambda \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

where λ an integer.

Theorem

Let $N = (P, T, F, V, m_0)$ a eS-Net and let y a P-invariant of N. Then:

$$m \in R_N(m_0) \Rightarrow y \cdot m^\top = y \cdot m_0^\top.$$

Proof:
Assume $m_0[\, q \succ m$. Then $m = m_0 + (C \cdot \bar{q})^\top$ and also:

$$y \cdot m^\top = y \cdot m_0^\top + y \cdot (C \cdot \bar{q}) =$$

$$= y \cdot m_0^\top + (y \cdot C) \cdot \bar{q} = y \cdot m_0^\top + 0 \cdot \bar{q} = y \cdot m_0^\top.$$

Corollary:

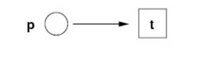
- Let y P-invariante of N, m marking.

  $y \cdot m^\top \neq y \cdot m_0^\top \Rightarrow m \notin R_N(m_0)$.
- Let y proper P-invariant of N. Let $p \in P$ such that $y(p) > 0$.

  Then, for any initial marking, p is bounded.

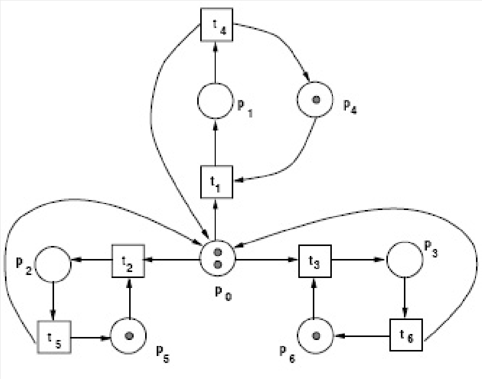
  Proof: $y \cdot m_0^\top = y \cdot m^\top \geq y(p) \cdot m(p) \geq m(p)$.
- Let N be covered by P-invariants. N is bounded for any initial marking.

Note, the following net is bounded for any initial marking, however does not have a P-invariant:



P-invariants allow sufficient tests for non-reachability and boundedeness.

Example: Prove freedom from deadlocks.



$$C = \begin{bmatrix} -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 \end{bmatrix}$$

P-invariants:

$$Y_1 = (0, 1, 0, 0, 1, 0, 0)$$
$$Y_2 = (0, 0, 1, 0, 0, 1, 0)$$
$$Y_3 = (0, 0, 0, 1, 0, 0, 1)$$
$$Y_4 = (1, 1, 1, 1, 0, 0, 0)$$

Initial marking is given by $m_0 = (2, 0, 0, 0, 1, 1, 1)$. Assume there exist a dead marking m, $m_0[\, q \succ m$. Then it must hold $m(p_1) = m(p_2) = m(p_3) = 0$. Because of Y_4 it follows $m(p_0) = 2$. As m dead it follows $m(p_4) = m(p_5) = m(p_6) = 0$. However this contradicts $Y_1 m_0 = Y_1 m$.

Section 12.5 Place Capacities

Sometimes when modelling we would like to fix an upper bound for the number of tokens in a place.

- Let $N = (P, T, F, V, m_0)$ be a eS-Net, c a ω-marking of P and let $m_0 \leq c$. (N, c) is called *eS-Net with capacities*. $c(p), p \in P$ is called *capacity* of p.
- For eS-nets with capacities the notion of being enabled is adapted:

  a transition $t \in T$ *is* enabled at marking m, *if* $t^- \leq m$ *and* $m + \Delta t \leq c$.

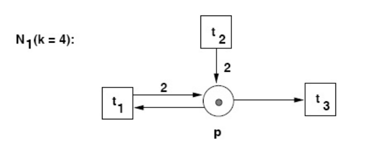
- Capacities graphically are labels of places - no label means capacity ω.

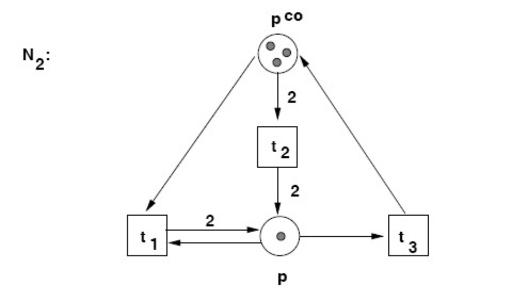
Any eS-net with capacities can be simulated by a eS-Net without capacities.

Construction

- Let p a palce with capacity $k = c(p), k \geq 1$. Let p^{co} be the complementary place of p which is assigned the initial marking $k - m_0(p)$.
- Whenever for a transition t we have $\Delta t(p) > 0$, we introduce an arc from p^{co} to t with multiplicity $\Delta t(p)$;
  whenever $\Delta t(p) < 0$, we introduce an arc from t to p^{co} with multiplicity $-\Delta t(p)$.

A eS-Net with capacities and its simulation by a bounded eS-Net.

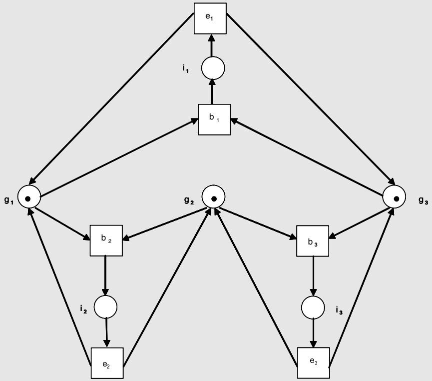




Section 12.6 S-Nets with Colors

- eS-Nets in practice may become huge and difficult to understand.
- Sometimes such nets exhibit certain regularities which give rise to questions how to reduce the size of the net without losing modeling properties.

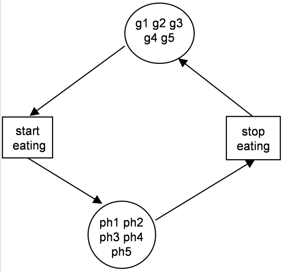
What about a n-philosopher problem with $n >> 3$?



Why not introduce tokens with individual information?

Abstraction 5-philosopher problem

Note: the intention of the marking shown only is to demonstrate „individual“ tokens.



What about being enabled and firing?

Colored System-Nets

A colored System-Net distinguishes different kinds of sorts for markings - the so called *colors* - and functions over these sorts which are used to label the edges of the net.

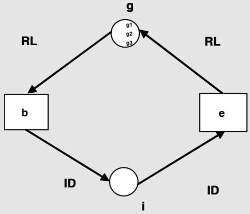
Generalizing eS-Nets, in a colored net a transition will be called enabled, if certain conditions are true, which are based on the functions which are assigned to the edges of the transitions surrounding.

Thus, we have colors, to characterize markings (*place colors*), and colors, to characterize the firing of transitions (*transition colors*).

As a marking of a place now can be built out of different kind of tokens, we introduce multisets.

- Let A be a set. A *multiset m* over A is given by a maping $m : A \to NAT$.
- Let $a \in A$. If $m[a] = k$ then there exist k occurences of a in m.
- A multiset oftenly is written as a (formal) sum, e.g. $[Apple, Apple, Pear]$ is written as $2 \cdot Apple + 1 \cdot Pear$.

A colored version of the 3-Philosopher-Problem



Colors

$$C(g) = \{g_1, g_2, g_3\},\ C(i) = \{ph_1, ph_2, ph_3\} \quad \text{place colors}$$
$$C(b) = \{ph_1, ph_2, ph_3\},\ C(e) = \{ph_1, ph_2, ph_3\} \quad \text{transition colors}$$

Functions

$$ID(ph_j) := 1 \cdot ph_j, 1 \leq j \leq 3$$
$$RL(ph_j) := \begin{cases} 1 \cdot g_1 + 1 \cdot g_3 & \text{if } j = 1, \\ 1 \cdot g_{j-1} + 1 \cdot g_j & \text{if } j \in \{2, 3\}. \end{cases}$$

Multiplicities

A *multiplicity* assigned to an edge between a place p and a transition t is a mapping from the set of transition colors of t into the set of multisets over the colors of p.

In the example:

$$V(b,i) = V(i,e) = ID,\ V(g,b) = V(e,g) = RL,$$

where:

$$ID(ph_j) := 1 \cdot ph_j, 1 \leq j \leq 3$$
$$RL(ph_j) := \begin{cases} 1 \cdot g_1 + 1 \cdot g_3 & \text{if } j = 1, \\ 1 \cdot g_{j-1} + 1 \cdot g_j & \text{if } j \in \{2,3\}. \end{cases}$$

ID denotes the identity mapping.

Marking

Markings are multisets over the respective place colors.

In the example:

$$m_0(p) := \begin{cases} 1 \cdot g_1 + 1 \cdot g_2 + 1 \cdot g_3 & \text{if } p = g, \\ 0 & \text{otherwise.} \end{cases}$$

A *colored Net* $CN = (P, T, F, C, V, m_0)$ is given by:

- A net (P, T, F).
- A mapping C which assignes to each $x \in P \cup T$ a finite nonempty set $C(x)$ of *colors*.
- Mapping V assignes to each edge $f \in F$ a mapping $V(f)$.

  Let f be an edge connecting palce p and transition t.
  $V(f)$ is a mapping from $C(t)$ into the set of multisets over $C(p)$.
- m_0 is the initial marking given by a mapping which assignes to each place p a multiset $m_0(p)$ over $C(p)$.

Let $CN = (P, T, F, C, V, m_0)$ be a colored System-Net.

- A marking m of P is mapping which assignes to each place p a multiset $m(p)$ over $C(p)$.
- A transition t *is enabled in color* $d \in C(t)$ at m, if for all pre-places $p \in Ft$ there holds:

$$V(p, t)(d) \leq m(p).$$

- Assume t is enabled in color d at marking m. Firing of t in color d transforms m to a marking m':

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

Fold and Unfold of a Colored System-Net

Folding

By folding of a eS-Net we can reduce the number of places and transitions; places and transitions are represented by appropriate place and transition colors, on which certain functions defining the multiplicities are defined.

Let $N = (P, T, F, V, m_0)$ a eS-Net. A folding is defined by π and τ:

- $\pi = \{q_1, \dots, q_k\}$ a (disjoint) partition of P,
- $\tau = \{u_1, \dots, u_n\}$ a (disjoint) partition of T.

Two special cases

Call $GN(\pi, \tau) := (P', T', F', C', V', m_0')$ the result of folding.

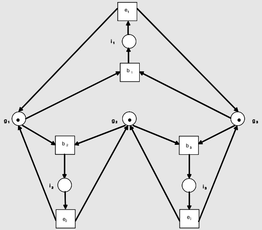
- All elements of π, τ are one-elementary:

$$\Rightarrow N \text{ and } GN(\pi, \tau) \text{ are isomorph,}$$

- π, τ contain only one element:

$$\Rightarrow |P'| = |T'| = 1, \text{"the model is represented by the labellings".}$$

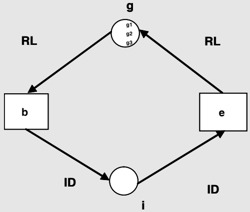
3-Philosopher-Problem



Folding $\pi = \{\{g_1, g_2, g_3\}, \{i_1, i_2, i_3\}\}$, $\tau = \{\{b_1, b_2, b_3\}, \{e_1, e_2, e_3\}\}$.

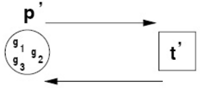
Colors from folding:
$C(g) = \{g_1, g_2, g_3\}, C(i) = \{i_1, i_2, i_3\}, C(b) = \{b_1, b_2, b_3\}, C(e) = \{e_1, e_2, e_3\}$

Multiplicities: ID, RL analogously to previous version.



3-Philosopher-Problem?

$\pi = \{P\},\ \tau = \{T\}$:
$S' = \{s'\},\ T' = \{t'\}$,
$C(s') = \{g_1, g_2, g_3, i_1, i_2, i_3\}$,
$C(t') = \{b_1, b_2, b_3, e_1, e_2, e_3\}$,
$m'_0(s') = g_1 + g_2 + g_3$,



$$V'(s',t')(t) = \begin{cases} g_1 + g_3 & \textit{falls } t = b_1, \\ g_1 + g_2 & \textit{falls } t = b_2, \\ g_2 + g_3 & \textit{falls } t = b_3, \\ i_1 & \textit{falls } t = e_1, \\ i_2 & \textit{falls } t = e_2, \\ i_3 & \textit{falls } t = e_3, \end{cases} \qquad V'(t',s')(t) = \begin{cases} g_1 + g_3 & \textit{falls } t = e_1, \\ g_1 + g_2 & \textit{falls } t = e_2, \\ g_2 + g_3 & \textit{falls } t = e_3, \\ i_1 & \textit{falls } t = b_1, \\ i_2 & \textit{falls } t = b_2, \\ i_3 & \textit{falls } t = b_3. \end{cases}$$

Given $\pi = \{q_1, \ldots, q_k\}$, $\tau = \{u_1, \ldots, u_n\}$.

The *folding* $GN(\pi, \tau) := (P', T', F', C', V', m_0')$ of N is defined as follows:

- $P' := \{p_1', \ldots, p_k'\}$; $T' := \{t_1', \ldots, t_n'\}$,
- $C'(p_i') = q_i$ für $i = 1, \ldots, k$; $C'(t_j') = u_j$ für $j = 1, \ldots, n$,
- $$F' := \begin{array}{l} \{(p', t') \mid C'(p') \times C'(t') \cap F \neq \emptyset\} \cup \\ \{(t', p') \mid C'(t') \times C'(p') \cap F \neq \emptyset\}, \end{array}$$
- $f' = (p', t') \in F'$: $V'(f')$ is defined $(t \in C'(t'))$:
$$V'(f')(t) = \sum_{p \in C'(p')} t^-(p) \cdot p,$$
- $f' = (t', p') \in F'$: $V'(f')$ is defined $(t \in C'(t'))$:
$$V'(f')(t) = \sum_{p \in C'(p')} t^+(p) \cdot p,$$
- $m_0'(p') := \sum_{p \in C'(p')} m_0(p) \cdot p.$

Unfolding

Let $GN = (P, T, F, C, V, m_0)$ a CN-Net.

The *Unfolding* of GN is a eS-Net $GN^* := (P^*, T^*, F^*, V^*, m_0^*)$ given as follows:

- $P^* := \{(p, c) \mid p \in P, c \in C(p)\}$,
- $T^* := \{(t, d) \mid t \in T, d \in C(t)\}$,
- $$\begin{aligned} F^* := \quad & \{((p, c), (t, d)) \mid (p, t) \in F, V(p, t)(d)[c] > 0\} \cup \\ & \{((t, d), (p, c)) \mid (t, p) \in F, V(t, p)(d)[p] > 0\}. \end{aligned}$$
- $V^*((p, c), (t, d)) := V(p, t)(d)[c]$,
- $V^*((t, d), (p, c)) := V(t, p)(d)[c]$,
- $m_0^*(p, c) := m_0(p)[c]$.

Definition

Let E be a certain property of a net, e.g. boundedness, liveness, or reachability.

A CS-Net GN has property E, whenever its unfolding GN^* has property E.

Analysis of colored System Nets

- Analyse unfolding:

  Advantage: Methods exist,
  Pitfall: Unfoldings may be huge eS-Nets.

- Analyse colored net:
  - Reachability graph and coverability graph can be defined in analogous way to eS-Nets.
  - There exists a theory for invariants, as well.
  - Tools for simulation and analysis are available.

Section 12.7 Workflow-Nets

Literature:

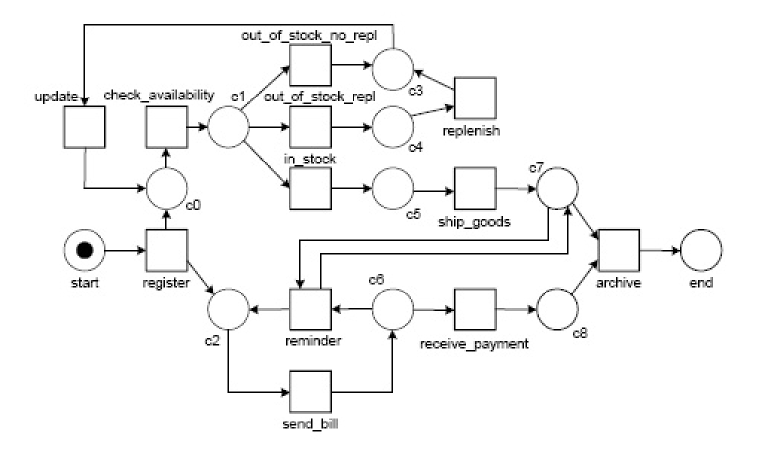
van der Aalst, Hofstede: http://is.tm.tue.nl/staff/wvdaalst/publications/p174.pdf

Workflow (WF)-Net

A eS-Net $N = (P, T, F)$ is a WF-Net, if

- There exists an *input-place* $i \in P$ where $Fi = \emptyset$.
- There exists an *output-place* $o \in P$ where $oF = \emptyset$.
- In N, every $x \in P \cup T$ is contained in a path from i to o.

Example: WF-net order handling



Properties of a WF-Net

Let $N = (P, T, F)$ a WF-Net with input-place *i*and output-place o.

- For $p \in P$ there holds $Fp \neq \emptyset$ or $p = i$.
- For $p \in P$ there holds $pF \neq \emptyset$ or $p = o$.
- Let $\overline{N} = (\overline{P}, \overline{T}, \overline{F})$, where $\overline{P} = P$, $\overline{T} = T \cup \{t^*\}$ and $\overline{F} = F \cup \{(o, t^*), (t^*, i)$.

  $\overline{N}$ is called the *shortcut* net of N.

  $\overline{N}$ is strongly connected.

Sound WF-Nets

A WF-Net is called *sound*, if the following holds.

Let m_i be a initial marking, such that only the input place i is marked.
Let m_o be a output marking, such that only the out-put place o is marked.

- From every marking m, which is reachable from m_i, marking m_o is reachable.
- m_o is the only marking reachable from m_i for which o is marked.
- The WF-Net does not contain dead transitions.

Theorem

A WF-Net N is sound iff $(\overline{N}, m_i)$ is life and bounded.

Lemma

A WF-Net N is sound, if $(\overline{N}, m_i)$ live and bounded.

Proof

As $(\overline{N}, m_i)$ live there exists for any reachable marking m (including m_i) a firing word leading to a marking m' such that t^* is enabled. Therefore o is marked in m'.

Consider an arbitrary such marking m' which is reachable from m_i, i.e. $m' = m'' + m_o$. t^* is enabled in m'. Thus marking $m'' + m_i$ is reachable from m_i. As $(\overline{N}, m_i)$ is bounded we have $m'' = 0$.

Lemma

Whenever a WF-Net N is sound, then $(\overline{N}, m_i)$ is bounded.

Proof

We show (N, m_i) bounded.

Assume (N, m_i) is not bounded. Then there exist markings m_1, m_2, such that $m_i[\, * \succ m_1$, $m_1[\, * \succ m_2$ and $m_2 > m_1$.

As N sound we have $m_1[\, q \succ m_o$. Moreover, because of $m_2 > m_1$, there exists a marking m with $m_2[\, q \succ m$ and $m > m_o$. This is a contradiction to N sound.

N sound and (N, m_i) bounded implies $(\overline{N}, m_i)$ bounded.

Lemma

If a WF-Netz N is sound, then $(\overline{N}, m_i)$ is life.

Proof

As N sound, from any marking m' which is reachable from m_i, we can reach m_o.

Therefore, from any m', which is reachable in $(\overline{N}, m_i)$, we can reach m_i. As N does not have any dead transitions w.r.t. m_i, it follows $(\overline{N}, m_i)$ is live.

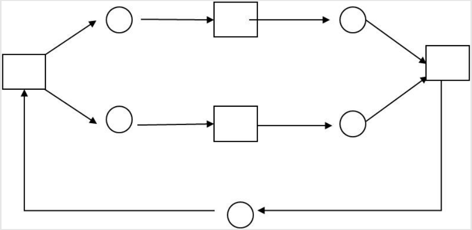
Excursus: Net-Classes

Let $N = (P, T, F, V, m_0)$.

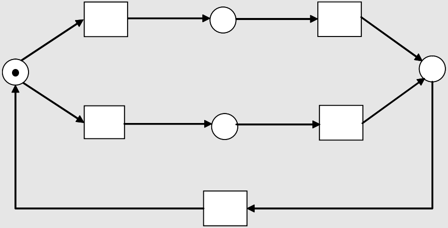
- N is called *Synchronization-Graph*, if for each place p it holds $\mid Fp \mid = \mid pF \mid = 1$.
- N is called *Statemachine*, if for each transition t it holds $\mid Ft \mid = \mid tF \mid = 1$.
- N is called *Free-Choice-Net (FC-Net)*, if $t, t' \in pF \Rightarrow Ft = \{s\} = Ft'$.
- N is called *Extended-Free-Choice-Net (EFC-Net)*, if $t, t' \in pF \Rightarrow Ft = Ft'$.

- A synchronization-graph is also a FC-Net.
- A statemachine is also a FC-Net.
- A FC-Net is also a EFC-Net.

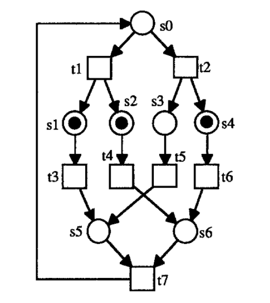
Synchronization-Graph



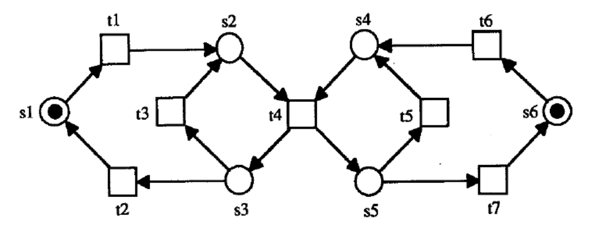
Statemachine



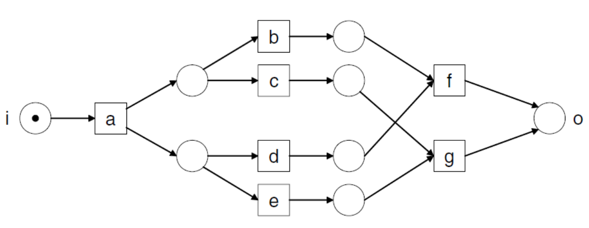
FC-Net


s0
t1
t2
s1
s2
s3
s4
t3
t4
t5
t6
s5
s6
t7

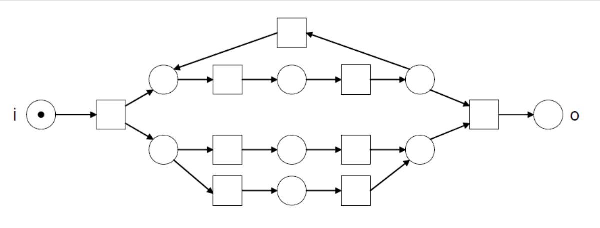
FC-Net


t1
s2
s4
t6
s1
t3
t4
t5
s6
t2
s3
s5
t7

A not sound WF-Net; the WF-Net is free-choice



A WF-Net which is sound, however not free-choice



Soundness of a WF-Net

A WF-Net, which is a FC-Net, can be checked for soundness in polynomial time.

... from practical experiences:

For modeling in practical applications FC-Nets are sufficient.

Example: WF-Net order handling - make it free-choice!