Lezione 30 MSC
Petri Nets: Basic Definitions

Roberto Gorrieri

Modello distribuito non-interleaving

- Stato globale

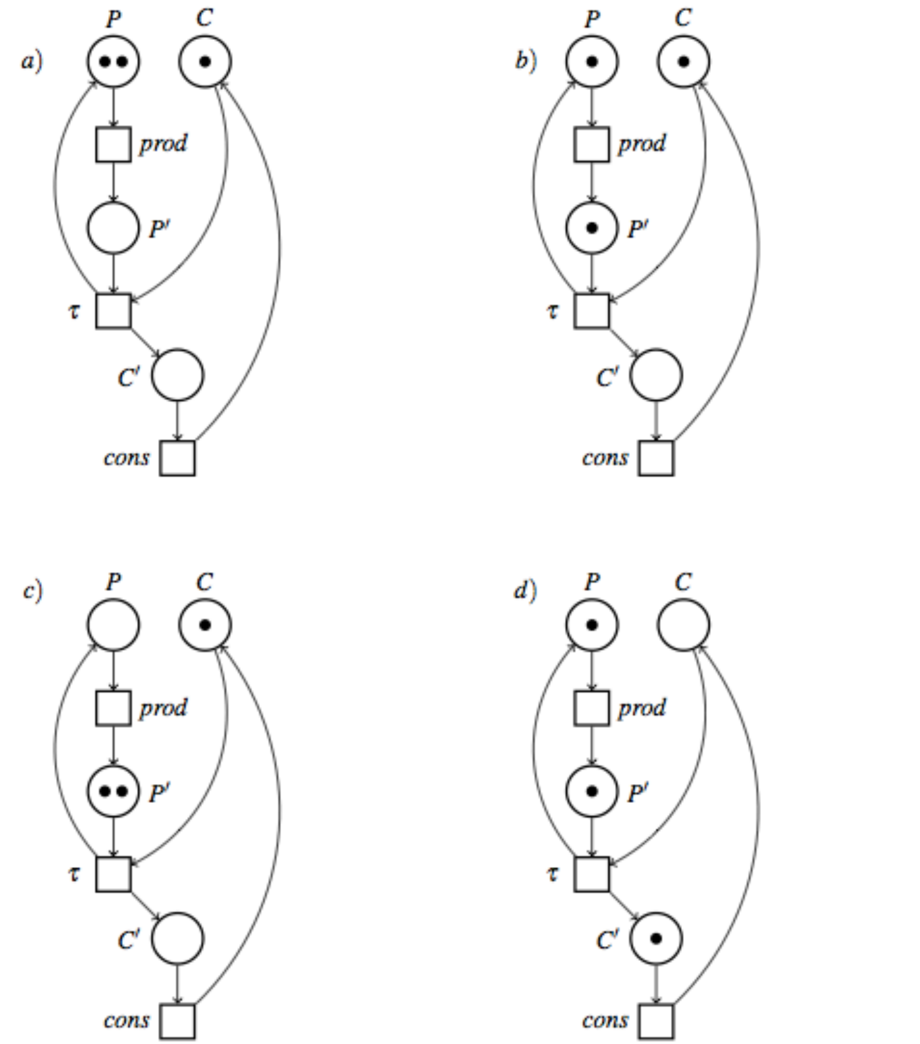
= multinsieme di stati locali

- Transizioni coinvolgono

solo qualche stato locale

- Token game
- Parallelismo esplicito

- Esempio: 2 produttori e
  un consumatore



Multiset (1)

A *multiset* M over a set A is an unordered, possibly infinite, list of elements of A, where no element of A can occur infinitely many times.

This is usually represented as a set with *multiplicities*; for instance, $M = \{a,\tau,a,\tau,\tau\}$ is a multiset over the set $A = \{a,\tau\}$ with two occurrences of action a and three occurrences of action τ.

Given a countable set S, a *finite multiset* over S is a function $m : S \to \mathbb{N}$ such that the *support* set $dom(m) = \{s \in S \mid m(s) \neq 0\}$ is finite. The *multiplicity* of s in m is given by the number $m(s)$.

The set of all finite multisets over S, denoted by $\mathrm{M}_{fin}(S)$, is ranged over by m, possibly indexed.

A multiset m such that $dom(m) = \emptyset$ is called *empty* and is denoted by $\emptyset$, with abuse of notation.

Multiset (2)

Ordering: We write $m \subseteq m'$ if $m(s) \leq m'(s)$ for all $s \in S$. We also write $m \subset m'$ if $m \subseteq m'$ and $m(s) < m'(s)$ for some $s \in S$.

- The operator $\oplus$ denotes *multiset union* and is defined as follows: $(m \oplus m')(s) = m(s) + m'(s)$; the operation $\oplus$ is commutative, associative and has $\varnothing$ as neutral element.
- If $m_2 \subseteq m_1$, then we can define *multiset difference*, denoted by the operator $\ominus$, as follows: $(m_1 \ominus m_2)(s) = m_1(s) - m_2(s)$.
- The *scalar product* of a number j with a multiset m is the multiset $j \cdot m$ defined as $(j \cdot m)(s) = j \cdot (m(s))$.

A finite multiset m over $S = \{s_1, s_2, \ldots\}$ can be represented as $k_1 \cdot s_{i_1} \oplus k_2 \cdot s_{i_2} \oplus \ldots \oplus k_n \cdot s_{i_n}$, where $dom(m) = \{s_{i_1}, \ldots s_{i_n}\} \subseteq S$ and $k_j = m(s_{i_j}) > 0$ for $j = 1, \ldots, n$. If S is finite, i.e., $S = \{s_1, \ldots, s_n\}$, then a finite multiset can be represented also as $k_1 \cdot s_1 \oplus k_2 \cdot s_2 \oplus \ldots \oplus k_n \cdot s_n$, where $k_j = m(s_j) \geq 0$ for $j = 1, \ldots, n$. $\square$

Place/Transition Petri Net

Definition 3.2. (P/T Petri net) A labeled *Place/Transition* Petri net (P/T net for short) is a tuple $N = (S, A, T)$, where

- S is the countable set of *places*, ranged over by s (possibly indexed),
- $A \subseteq Lab$ is the countable set of *labels*, ranged over by ℓ (possibly indexed), and
- $T \subseteq (\mathscr{M}_{fin}(S) \setminus \{\emptyset\}) \times A \times \mathscr{M}_{fin}(S)$ is the countable set of *transitions*, ranged over by t (possibly indexed), such that, for each $\ell \in A$, there exists a transition $t \in T$ of the form (m, ℓ, m').

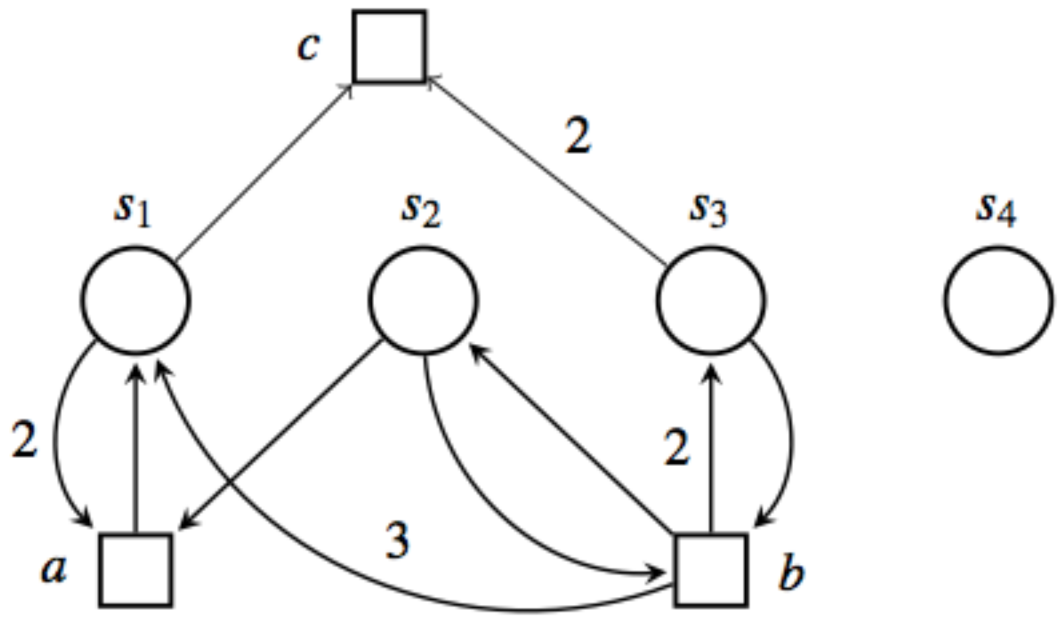
Given a transition $t = (m, \ell, m')$, we use the notation:

- ${}^\bullet t$ to denote its *pre-set* m (which cannot be an empty multiset) of tokens to be consumed;
- $l(t)$ for its *label* ℓ, and
- $t^\bullet$ to denote its *post-set* m' of tokens to be produced.

Hence, transition t can be also represented as ${}^\bullet t \xrightarrow{l(t)} t^\bullet$. We also define pre-sets and post-sets for places as follows: ${}^\bullet s = \{t \in T \mid s \in t^\bullet\}$ and $s^\bullet = \{t \in T \mid s \in {}^\bullet t\}$. Note that while the pre-set (post-set) of a transition is, in general, a multiset, the pre-set (post-set) of a place is a set. □

Example

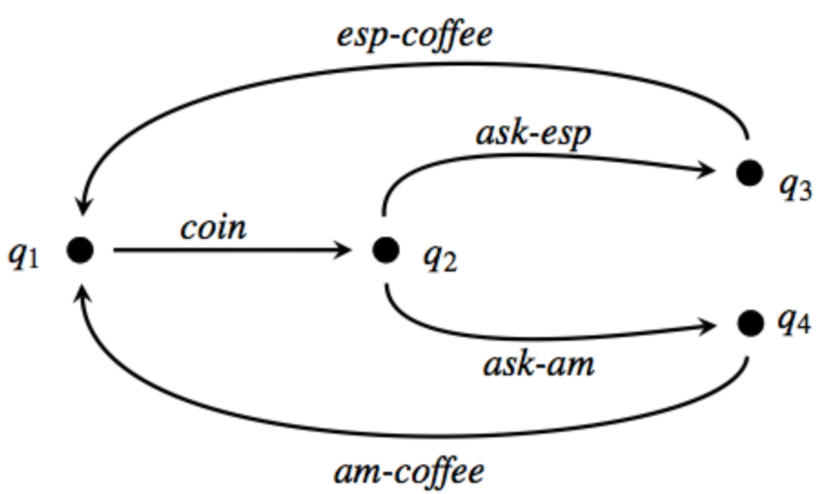
- $N = (S,A,T)$, where $S = \{s_1,s_2,s_3,s_4\}$, $A = \{a,b,c\}$ and $T = \{(2\cdot s_1 \oplus s_2,a,s_1),(s_2 \oplus s_3,b,3\cdot s_1 \oplus s_2 \oplus 2\cdot s_3),$ $(s_1 \oplus 2\cdot s_3,c,\varnothing)\}$.

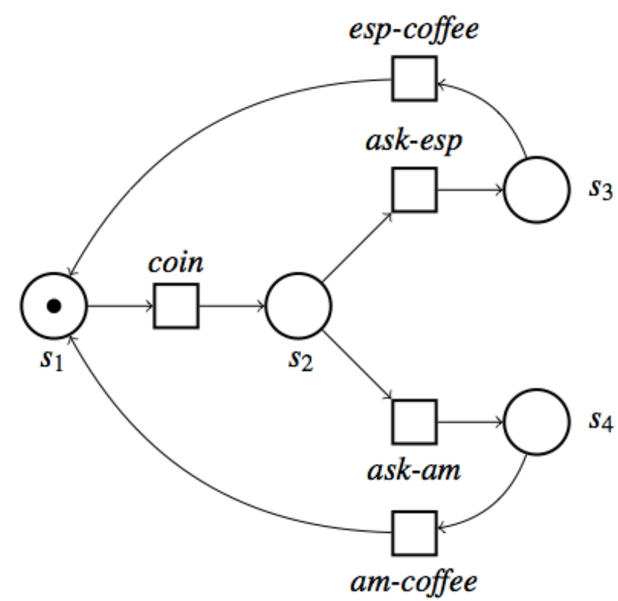


Osservazione

- LTS's are a subclass of P/T nets.

Note that the latter is a generalization of the former: a transition system is just a special case of Petri net, where each net transition $t = (m,a,m')$ is such that m and m' are singletons.





P/T net system and token game

Definition 3.3. (Marking, token, P/T net system) A finite multiset over S is called a *marking*. Given a marking m and a place s, we say that the place s contains $m(s)$ *tokens*, graphically represented by $m(s)$ bullets inside place s. A *P/T net system* $N(m_0)$ is a tuple (S, A, T, m_0), where (S, A, T) is a P/T net and m_0 is a marking over S, called the *initial marking*. We also say that $N(m_0)$ is a *marked* net. □

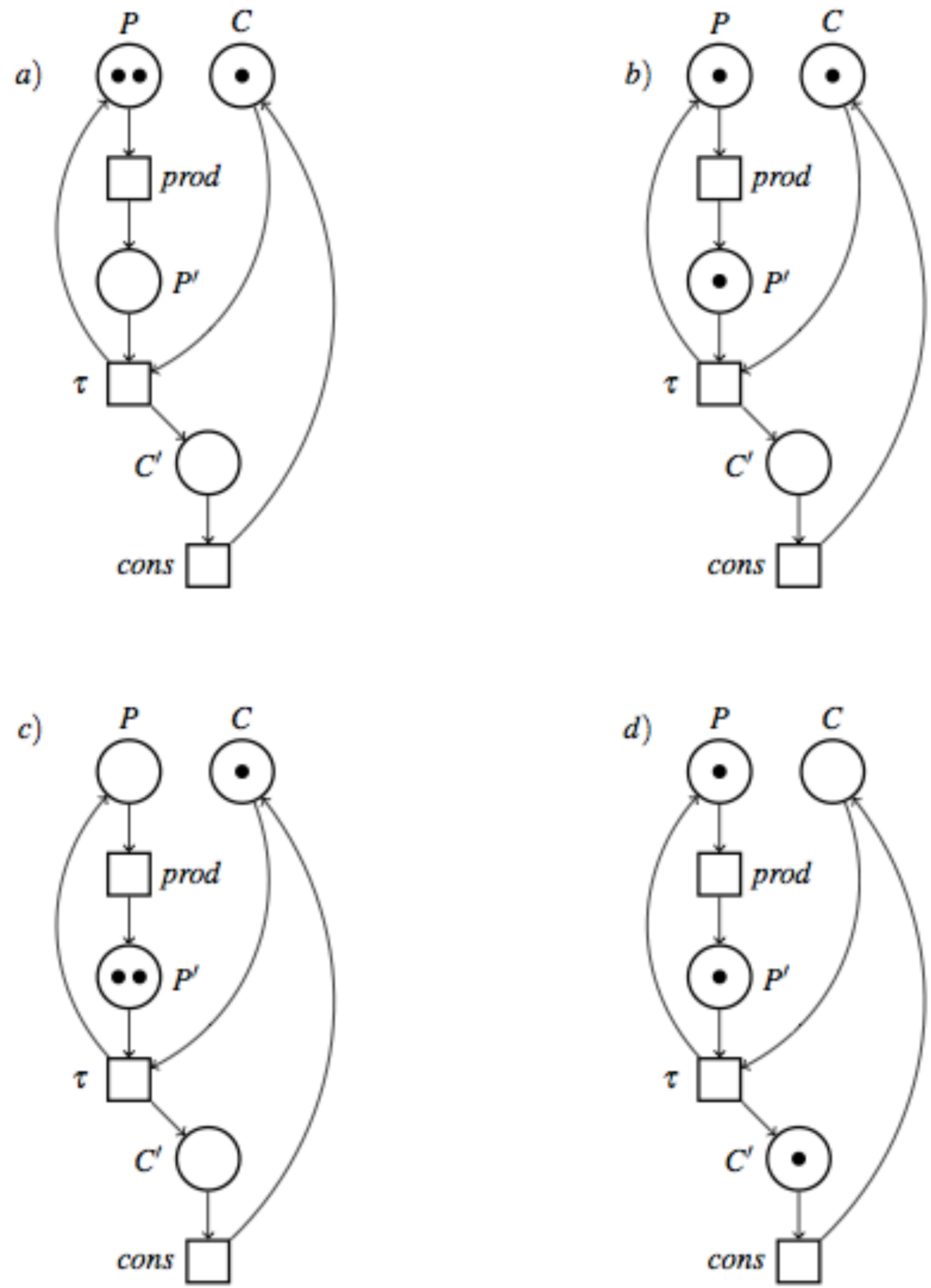
Definition 3.4. (Token game) Given a labeled P/T net $N = (S, A, T)$, we say that a transition t is *enabled* at marking m, denoted by $m[t\rangle$, if ${}^\bullet t \subseteq m$. The execution (or *firing*) of t enabled at m produces the marking $m' = (m \ominus {}^\bullet t) \oplus t^\bullet$. This is written $m[t\rangle m'$. □

Permissive nature of P/T Petri nets: if t is enabled at m, then t is enabled also by any other marking m' covering m, i.e., by any m' such that $m \subseteq m'$.

This is in contrast with *nonpermissive* Petri nets, we will see in the following, where a transition t enabled at m may be disabled at m' because m' can contain a token in an inhibiting place for t.

2-Producers/
1-Consumer

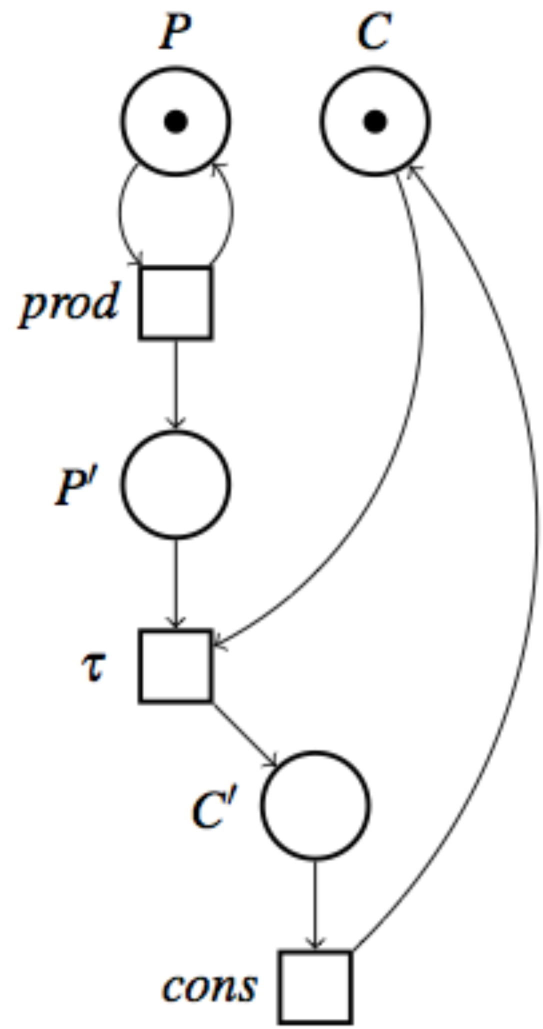
Rete bounded: Al massimo 2 tokens in ogni place



Unbounded Producer/Consumer

Note that place *P′* can hold an unbounded number of tokens, as the producer *P* can perform the initial transition ***prod*** repeatedly, depositing each time one token in that place.

A finite Petri net model for a system whose reachable markings are infinitely many.



Reachable markings and firing sequences

Definition 3.5. (Reachable markings and firing sequences) Given a P/T net system $N(m_0) = (S, A, T, m_0)$, the set of markings *reachable from m*, denoted $[m\rangle$, is defined as the least set such that

- $m \in [m\rangle$ and
- if $m_1 \in [m\rangle$ and, for some transition $t \in T$, $m_1[t\rangle m_2$, then $m_2 \in [m\rangle$.

We say that m is *reachable* if m is reachable from the initial marking m_0. A *firing sequence* starting at m is defined inductively as follows:

- m is a firing sequence and
- if $m_1[t_1\rangle m_2 \ldots [t_{n-1}\rangle m_n$ (with $m = m_1$ and $n \geq 1$) is a firing sequence and $m_n[t_n\rangle m_{n+1}$, then $m = m_1[t_1\rangle m_2 \ldots [t_{n-1}\rangle m_n[t_n\rangle m_{n+1}$ is a firing sequence.

A firing sequence $m = m_1[t_1\rangle m_2 \ldots [t_n\rangle m_{n+1}$ is usually abbreviated as $m[t_1 \ldots t_n\rangle m_{n+1}$ and $t_1 \ldots t_n$ is called a *transition sequence* starting at m and ending at m_{n+1}. □

Some classes of P/T nets

Definition 3.6. (Classes of P/T Petri nets) A P/T Petri net $N = (S, A, T)$ is

- *statically acyclic* if there exists no sequence $x_1 x_2 \ldots x_n$, such that $n \geq 3$, $x_i \in S \cup T$ for $i = 1, \ldots, n$, $x_1 = x_n$, $x_1 \in S$ and $x_i \in {}^\bullet x_{i+1}$ for $i = 1, \ldots, n-1$;
- *distinct* if all the transitions have distinct labels: for all $t_1, t_2 \in T$, if $l(t_1) = l(t_2)$, then $t_1 = t_2$;
- *finite* if both S and T are finite sets;

- a *finite-state machine* (FSM, for short) if N is finite and for all $t \in T$, $|{}^\bullet t| = 1$ and $|t^\bullet| \leq 1$;
- a *BPP net* if N is finite and every transition has exactly one input place, i.e., for all $t \in T$, $|{}^\bullet t| = 1$;
- a *CCS net* if for all $t \in T$, $1 \leq |{}^\bullet t| \leq 2$ and if $|{}^\bullet t| = 2$ then $l(t) = \tau$.

Some classes of P/T net systems

A P/T net system $N(m_0)$ is

- *dynamically acyclic* if there exists no $m_1 \in [m_0\rangle$ with a nonempty (i.e, with $n \geq 2$) firing sequence $m_1[t_1\rangle m_2 \dots [t_{n-1}\rangle m_n$ such that $m_1 \subseteq m_n$;
- a *sequential* FSM if N is an FSM and m_0 is a singleton, i.e., $|m_0| = 1$;
- a *concurrent* FSM if N is an FSM and m_0 is arbitrary;
- *k-bounded* if any place contains at most k tokens in any reachable marking, i.e., $\forall s \in S\ m(s) \leq k$ for all $m \in [m_0\rangle$;
- *safe* if it is 1-bounded;
- *bounded* if $\forall s \in S\ \exists k \in \mathbb{N}$ such that $m(s) \leq k$ for all $m \in [m_0\rangle$. $\square$

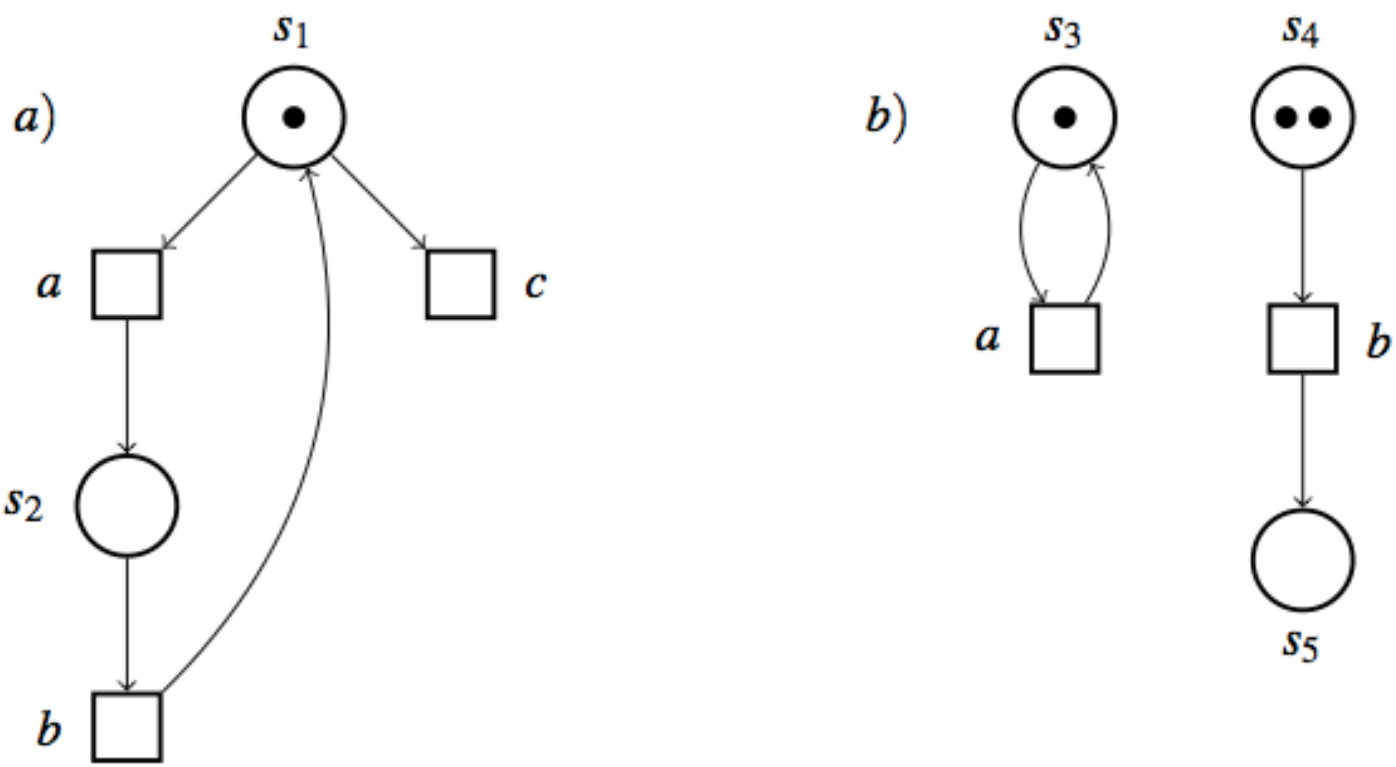


Fig. 3.4 A sequential finite-state machine in (a), and a concurrent finite-state machine in (b)

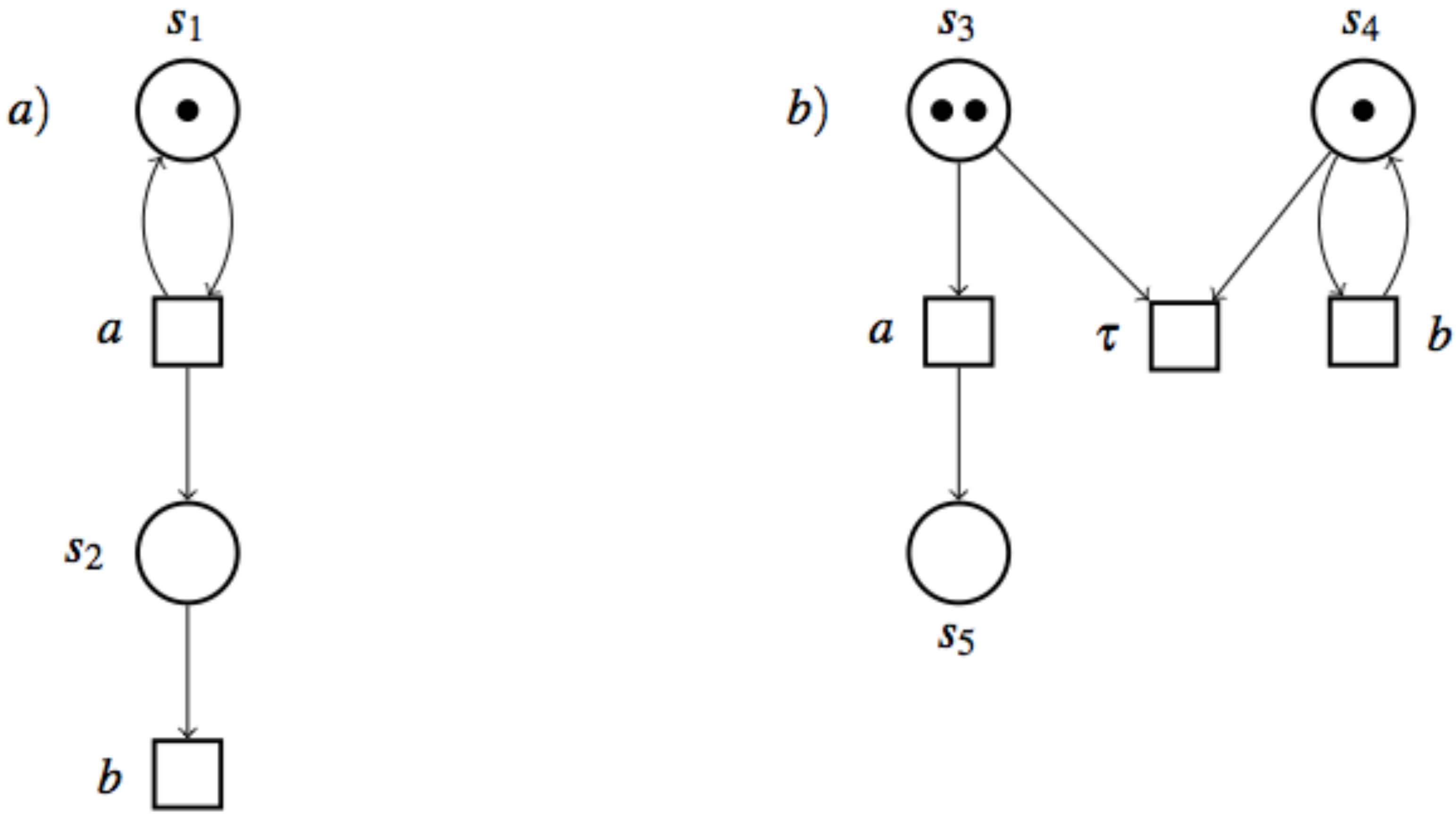


Fig. 3.5 Some further nets: a BPP net in (a), and a CCS net in (b)

Proposition 3.1. *Given a P/T system $N(m_0)$, the following hold:*

1. *if N is an FSM net, then N is also a BPP net;*
2. *if N is a BPP net, then N is also a finite CCS net;*
3. *if $N(m_0)$ is a sequential FSM, then $N(m_0)$ is also a concurrent FSM;*
4. *if $N(m_0)$ is a sequential FSM, then $N(m_0)$ is also safe;*
5. *if $N(m_0)$ is a concurrent FSM, then $N(m_0)$ is also $|m_0|$-bounded;*
6. *if $N(m_0)$ is finite and bounded, then $N(m_0)$ is also k-bounded for some suitable $k \in \mathbb{N}$;*
7. *if $N(m_0)$ is finite and bounded, then the set $[m_0\rangle$ of the markings reachable from m_0 is finite;*
8. *if N is statically acyclic, then $N(m_0)$ is dynamically acyclic;*
9. *if $N(m_0)$ is finite and dynamically acyclic, then the set of its firing sequences is finite.*

Proof. We prove only (7). Assume $N(m_0)$ is finite and bounded, where the cardinality of the set S of places is n and the bound limit on places is k. Then, there cannot be more than $(k+1)^n$ different markings, because each place s can hold any number of tokens in the range $\{0,\ldots,k\}$. $\square$

Finite and bounded implies k-bounded

Any finite net that is bounded is also k-bounded for some suitable $k \in$ N; in fact, boundedness implies that

for all $s \in S$ there exists an upper bound k_s on the number of tokens that can be accumulated on s; if the net is finite, then it is enough to choose the largest k_s (call it k'), which has the property that for all s, $k_s \leq k'$, so that the net is k'-bounded.

It follows that a bounded net that is not k-bounded for any k is infinite. For instance, consider the net $N(m_0)=(S,A,T,m_0)$— where$S=\{s_i \mid i \in \mathrm{N}\}$, $A=\{a_i \mid i \in \mathrm{N}\}$, $T = \{(s_i,a_i,2 \cdot s_{i+1}) \mid i \in \mathrm{N}\}$, $m_0 = \{s_0\}$ — is an infinite net such that place s_i can hold up to 2^i tokens; hence, $N(m_0)$ is bounded, but there is no k such that $2^i \leq k$ for all $i \in$ N.

Why these classes?

The interest in these classes is because we will see that they are strictly related to particular process algebras derived from CCS and Multi-CCS. In particular, we will see that

- SFM process terms (essentially finite-state CCS) originate sequential FSMs (Chapter 4),
- CFM process terms (finite-state CCS with an external operator of asynchronous parallelism) represent concurrent FSMs (Section 5.1),
- BPP process terms are mapped to BPP nets (Section 5.2),
- FNC process terms (essentially finite-net CCS) originate finite CCS P/T nets (Chapter 6), and finally
- FNM process terms (essentially finite-net Multi-CCS) represent all finite P/T nets (Chapter 7).

The Hierarchy

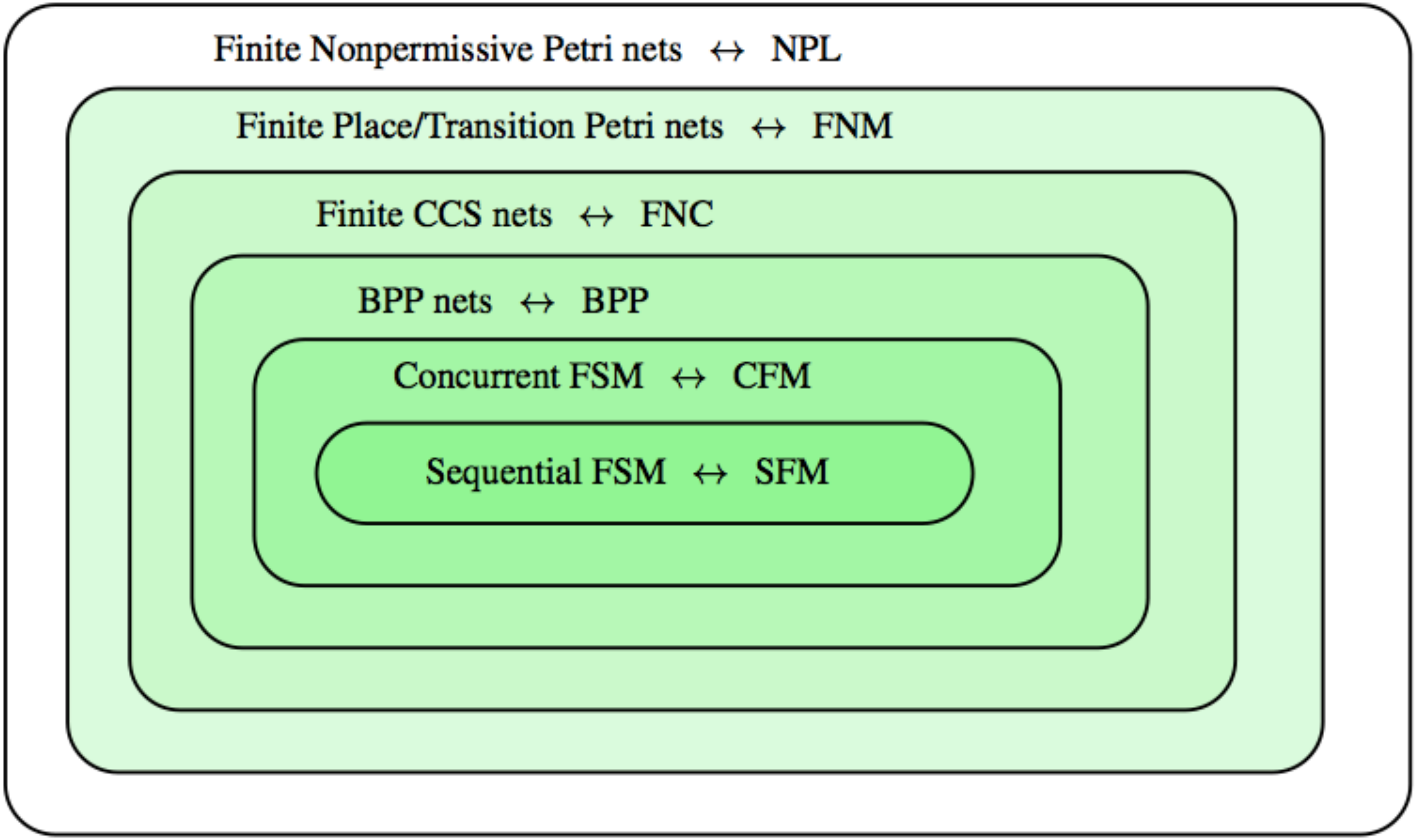


Fig. 1.5 The hierarchy of net classes and process algebras

Dynamically reachable subnet

Definition 3.7. (Dynamically reachable subnet) Given a P/T net system $N(m_0) = (S, A, T, m_0)$, the *dynamically reachable subnet* $Net_d(N(m_0))$ is (S', A', T', m_0), where

$$
\begin{aligned}
S' &= \{s \in S \mid \exists m \in [m_0\rangle \text{ such that } m(s) \geq 1\}, \\
T' &= \{t \in T \mid \exists m \in [m_0\rangle \text{ such that } m[t\rangle\}, \\
A' &= \{\ell \mid \exists t \in T' \text{ such that } l(t) = \ell\}.
\end{aligned}
$$

□

Definition 3.8. (Dynamically reduced net) A P/T net system $N(m_0) = (S, A, T, m_0)$ is *dynamically reduced* if $N(m_0) = Net_d(N(m_0))$, i.e., the net system is equal to its dynamically reachable subnet. □

- $Net_d(N(m_0))$ is algorithmically computable for any finite P/T net system (complexity: exponential)

Example

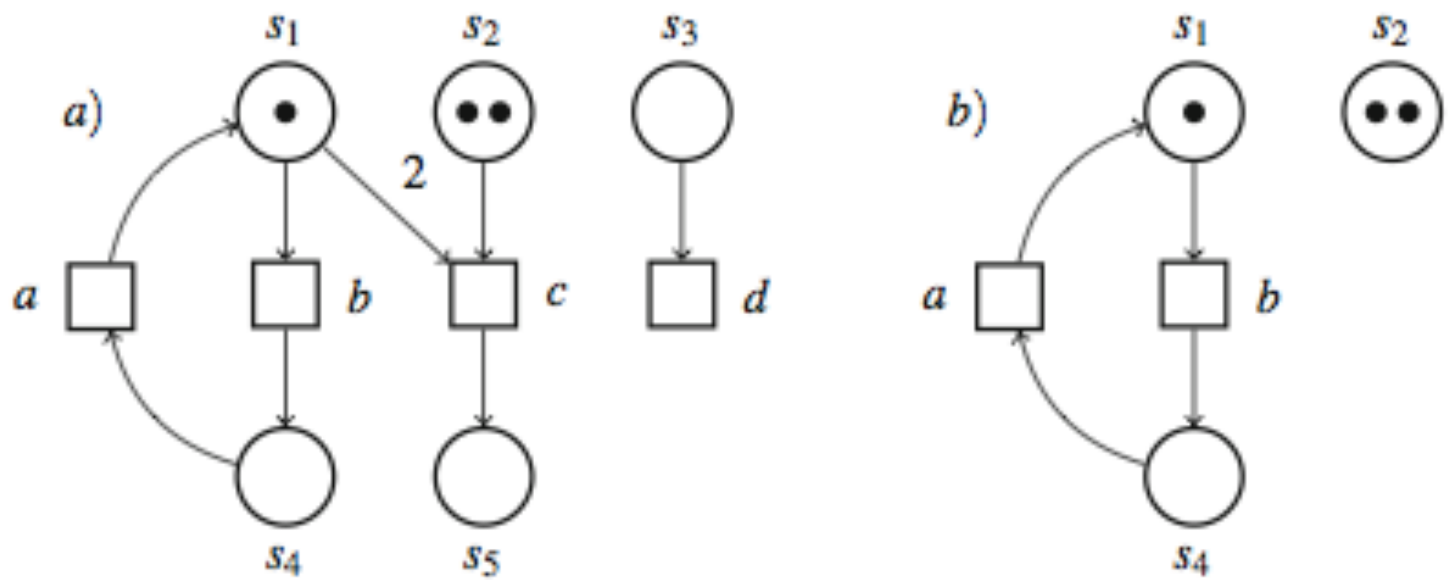


Fig. 3.7 A net system in (a) and its dynamically reachable subnet in (b)

Statically reachable subnet (1)

Definition 3.9. (Statically reachable subnet and statically reduced net) Given a finite P/T net $N = (S, A, T)$, we say that a transition t is *statically enabled* by a set of places $S' \subseteq S$, denoted by $S'[\![t\rangle$, if $dom({}^{\bullet}t) \subseteq S'$.

Given two sets of places $S_1, S_2 \subseteq S$, we say that S_2 is *statically reachable in one step* from S_1 if there exists a transition $t \in T$, such that $S_1[\![t\rangle$, $dom(t^{\bullet}) \not\subseteq S_1$ and $S_2 = S_1 \cup dom(t^{\bullet})$; this is denoted by $S_1 \stackrel{t}{\Longrightarrow} S_2$. The *static reachability relation* $\Longrightarrow^* \subseteq \mathscr{P}_{fin}(S) \times \mathscr{P}_{fin}(S)$ is the least relation such that

- $S_1 \Longrightarrow^* S_1$ and
- if $S_1 \Longrightarrow^* S_2$ and $S_2 \stackrel{t}{\Longrightarrow} S_3$, then $S_1 \Longrightarrow^* S_3$.

A set of places $S_k \subseteq S$ is the *largest* set statically reachable from S_1 if $S_1 \Longrightarrow^* S_k$ and for all $t \in T$ such that $S_k[\![t\rangle$, we have that $dom(t^{\bullet}) \subseteq S_k$.

Statically reachable subnet (2)

Given a finite P/T net system $N(m_0) = (S, A, T, m_0)$, we denote by $[\![dom(m_0)\rangle$ the largest set of places statically reachable from $dom(m_0)$, i.e., the largest S_k such that $dom(m_0) \Longrightarrow^* S_k$.

The *statically reachable subnet* $Net_s(N(m_0))$ is the net (S', A', T', m_0), where

$$
\begin{aligned}
S' &= [\![dom(m_0)\rangle, \\
T' &= \{t \in T \mid S'[\![t\rangle\}, \\
A' &= \{\ell \mid \exists t \in T' \text{ such that } l(t) = \ell\}.
\end{aligned}
$$

A finite P/T net system $N(m_0) = (S, A, T, m_0)$ is *statically reduced* if $Net_s(N(m_0)) = N(m_0)$, i.e., the net system is equal to its statically reachable subnet. □

- $Net_s(N(m_0))$ is algorithmically computable for any finite P/T net system (complexity: polynomial)

Example (revisited)

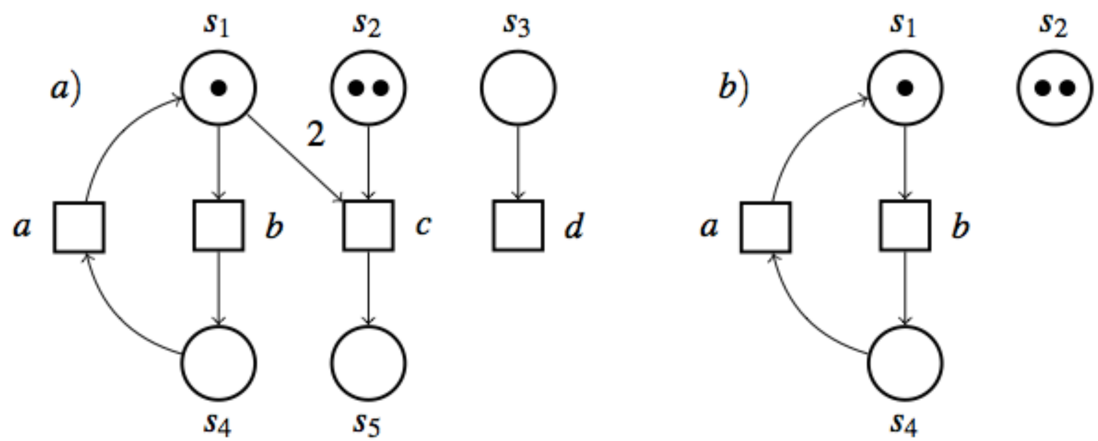


Fig. 3.7 A net system in (a) and its dynamically reachable subnet in (b)

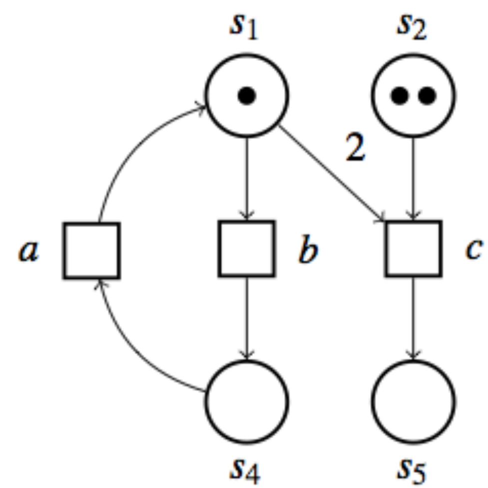


Fig. 3.8 The statically reachable subnet of Figure 3.7(a)

Properties

Proposition 3.2. *Given a P/T net system $N(m_0) = (S, A, T, m_0)$, if $N(m_0)$ is dynamically reduced, then it is also statically reduced.*

Proposition 3.3. *Given a P/T net system $N(m_0) = (S, A, T, m_0)$, if its dynamically reachable subnet $Net_d(N(m_0))$ is (S', A', T', m_0) and its statically reachable subnet $Net_s(N(m_0))$ is (S'', A'', T'', m_0), then $S' \subseteq S''$, $T' \subseteq T''$ and $A' \subseteq A''$.* □

For some classes of nets, however, the two notions coincide.

Proposition 3.4. *If $N(m_0)$ is a BPP net that is statically reduced, then it is also dynamically reduced.*

Proof. *A BPP transition t is such that $|{}^\bullet t| = 1$; therefore, the notions of dynamically enabled transition and statically enabled transition coincide.* □

Decidable Properties

- Computing Net_d and Net_s for any finite P/T net system $N(m_0)$
- Reachability: deciding whether a given marking is reachable from the initial marking for a finite P/T net system (complexity: non-primitive recursive).
- Deadlock: deciding whether a finite P/T net system has a deadlock, i.e., reaches a marking that does not enable any transition.
- Liveness: a transition *t* is *live* if for each marking *m* reachable from m_0 there exists a marking *m*′ reachable from *m* such that *t* is enabled at *m*′. The finite P/T net system $N(m_0)$ is *live* if each of its transitions is live. This problem is decidable.