Modelli per la specifica del software

- Modelli operazionali
- Modelli descrittivi (logica)
- Specifiche algebriche
- Specifiche a modelli (Z)

I modelli operazionali

- Fanno riferimento alle operazioni effettuate da una ***macchina astratta*** la cui esecuzione specifica il comportamento del sistema modellato

- Specifica di un sistema tramite:
  - descrizione degli ***stati*** in cui può venirsi a trovare durante la sua evoluzione
  - ***transizioni*** che portano il sistema da uno stato a un altro

- Due ***modelli operazionali***:
  - Automi a stati finiti
  - Reti di Petri

Automi a stati finiti

- Un *automa a stati finiti* (FSA, Finite State Automaton) e` un modello matematico di un sistema con ingressi e uscite discreti

- In un certo istante il sistema puo` trovarsi in uno *stato* scelto tra un *numero finito* di stati possibili

Esempi:

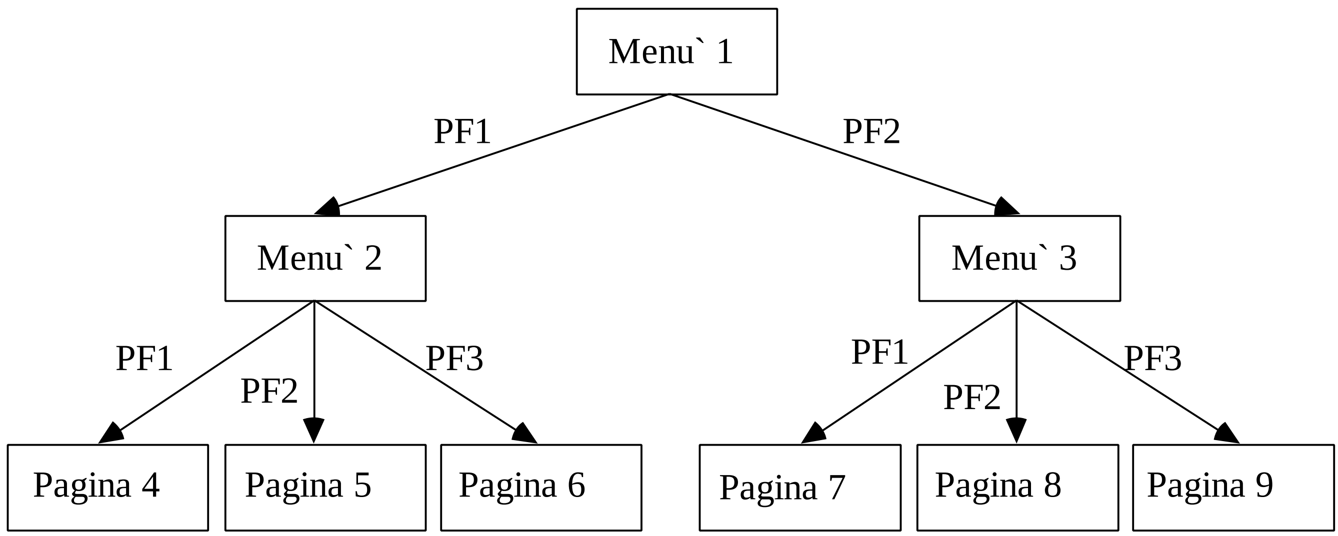
- meccanismo di controllo di un ascensore
- analizzatore lessicale
- video gioco

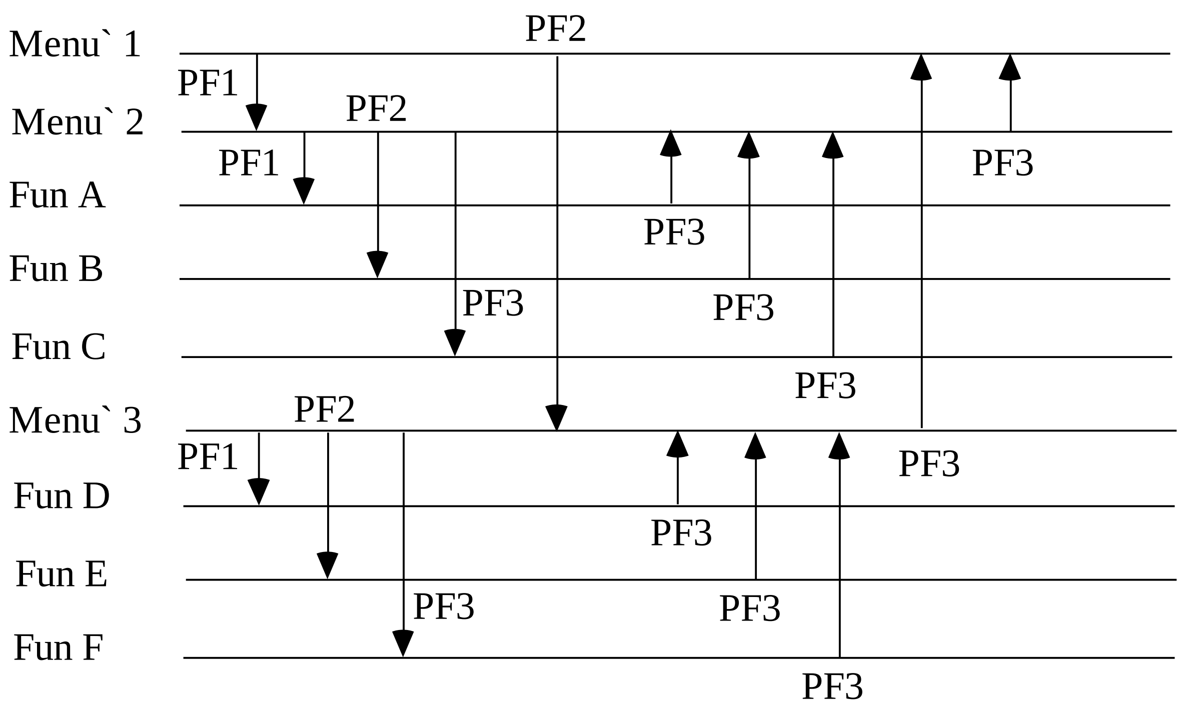
- Lo stato corrente del sistema riassume l'informazione circa la sequenza di ingresso fornita in passato e serve per determinare il comportamento del sistema al successivo ingresso (stato futuro).

- Il passaggio tra stati e` detto *transizione*.

Specifiche con FSA

- Sono spesso utilizzati per specificare le funzionalita` di interfacce utente



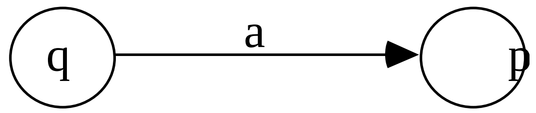


Definizione (FSA):

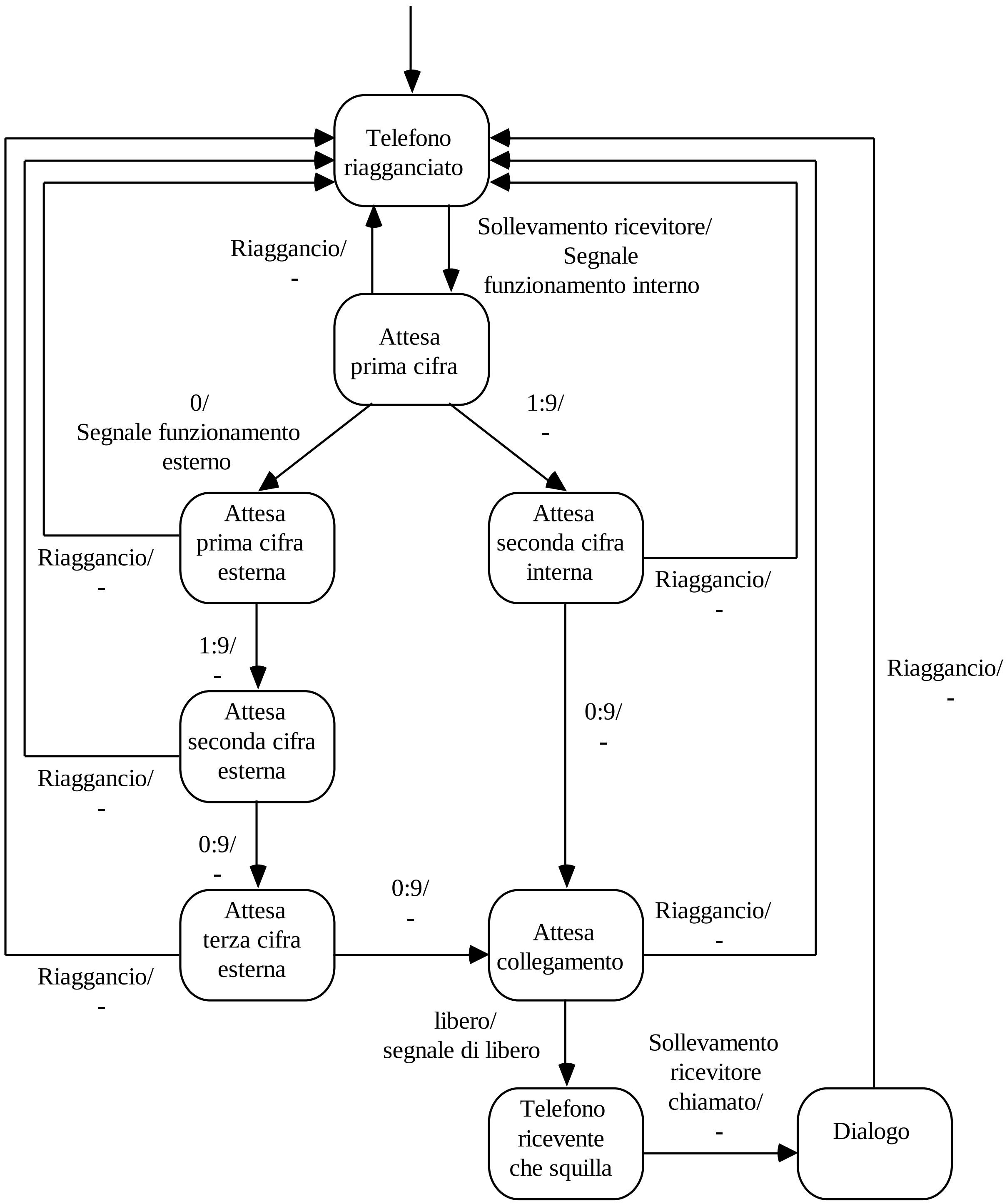
- Un *automa a stati finiti* e\` costituito da un insieme finito di *stati* S e da un insieme finito di *transizioni* da stato a stato che hanno luogo sulla base dei simboli ricevuti in ingresso, scelti da un alfabeto Σ. Tra gli stati, uno e\` lo *stato iniziale* (s_0). Alcuni stati vengono detti *stati finali* o di accettazione (F).

- Associato a un FSA c'e\` un grafo orientato detto *grafo delle transizioni* (nodi, stati del FSA; archi, transizioni di stato etichettati con simboli di ingresso).

- Se c'e\` una transizione dallo stato q allo stato p ricevuto l'ingresso a, allora c'e\` un arco da q a p etichettato con a:



- **Esempio:** Comportamento di un sistema telefonico di una società nei riguardi di un utente che deve effettuare una singola chiamata

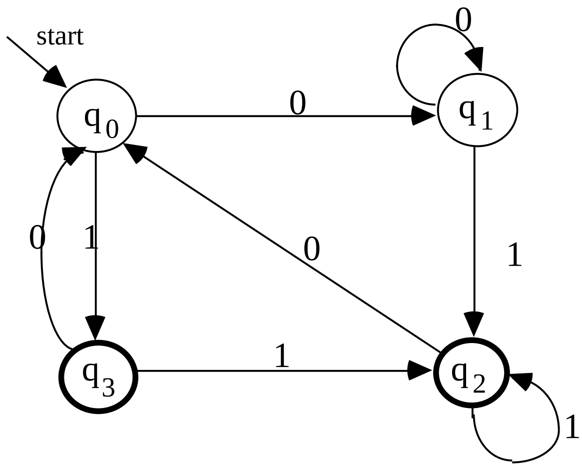


FSA deterministici

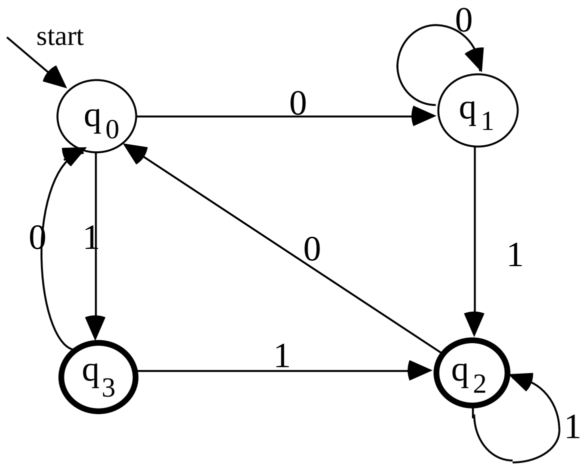
- Un automa a stati finiti *deterministico* (Deterministic Finite State Automaton, DFSA) e` una quintupla:

$$(S, \Sigma, t: S \infty \Sigma \varnothing S, s_0, F \prod S)$$

dove t e` la *funzione* di transizione (eventualmente parziale) e F l'insieme degli stati finali



q_0 stato iniziale; q_2, q_3 stati finali.



La funzione di transizione viene spesso espressa in forma tabellare:

Stato	Input	Stato futuro
q0	0	q1
q0	1	q3
q1	0	q1
q1	1	q2
q2	0	q0
q2	1	q2
q3	0	q0
q3	1	q2

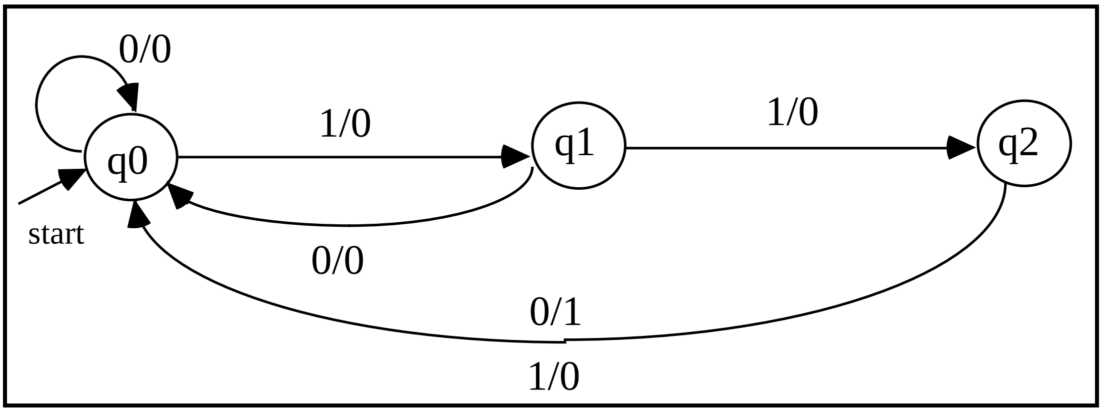
- Nel caso di automi con uscita, l'automa e` definito da una sestupla:

$$(S, \Sigma, U, t: S\infty\Sigma\emptyset S, out: t: S\infty\Sigma\emptyset U, s_0)$$

dove:

- S, insieme degli stati
- Σ, insieme dei simboli di ingresso
- U, insieme dei simboli di uscita
- t, funzione di transizione
- out, funzione di uscita

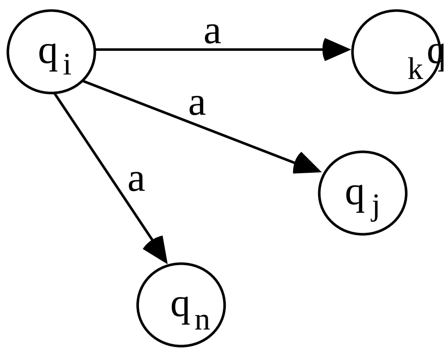
Esempio:



Combinazione di una cassaforte: produce 1 in uscita ogni volta che riconosce la stringa 110

Automi a stati finiti
non determinisitici (NFSA)

- Per uno stesso simbolo di ingresso sono permesse piu` transizioni di stato



NFSA = $(S, \Sigma, t: S \infty \Sigma \emptyset 2^S, s_0, F \prod S)$

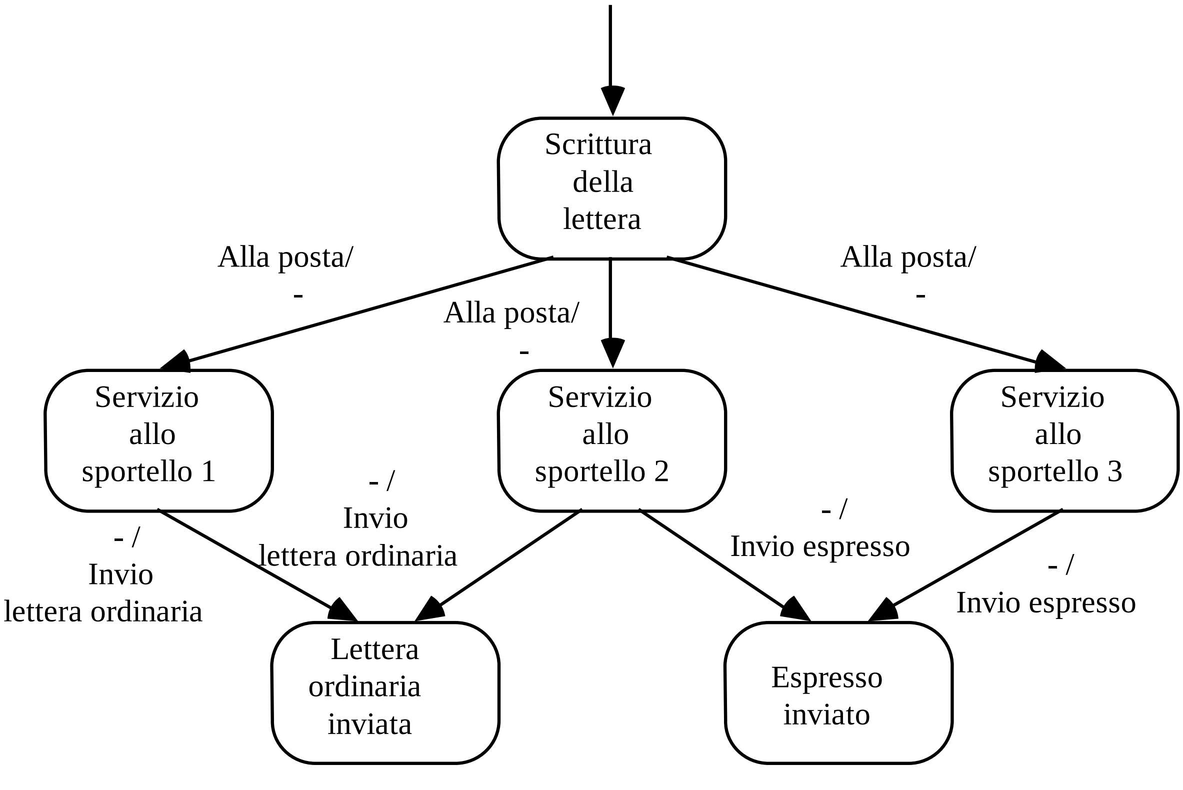
2^S, insieme potenza o insieme delle parti di S (e` l'insieme di tutti i sottoinsiemi di S)

- Possono essere utilizzati per una specifica di un sistema ad alto livello in cui per il momento i dettagli non sono precisati

- Un automa nondeterministico è in grado di descrivere specifiche di sistemi in cui in corrispondenza di un ingresso possono esistere più valori ammissibili in uscita (relazioni piuttosto che funzioni tra ingressi e uscite)

NFSA: Esempio

- Spedizione di una lettera: il servizio può essere effettuato da tre sportelli. Lo sportello 1 effettua solo il servizio di posta ordinaria, lo sportello 3 è delegato alla sola spedizione degli espressi, mentre lo sportello 2 è abilitato a effettuare entrambi i servizi



Automa probabilistico

- Si adotta un approccio stocastico e il meccanismo di scelta viene precisato tramite l'effettuazione di esperimenti casuali che seguono leggi probabilistiche date e perciò note

- La differenza tra un automa deterministico e un automa probabilistico sta perciò nel fatto che nel primo lo *stato futuro* è noto con certezza, mentre nel secondo viene determinato tramite un esperimento casuale

- Per l'automa probabilistico viene precisato il *meccanismo*, in questo caso stocastico, di scelta

- In un automa probabilistico le transizioni in uscita da ogni stato sono associate a valori che rappresentano la probabilità con cui ciascuna viene percorsa (somma degli archi in uscita pari a 1)

FSA e sistemi concorrenti

- FSA, formalismo semplice ed espressivo per modellare attività o agenti che eseguono sequenze di operazioni

- Cooperazione e sincronizzazione fra diverse attività (sottosistemi), anche concorrenti

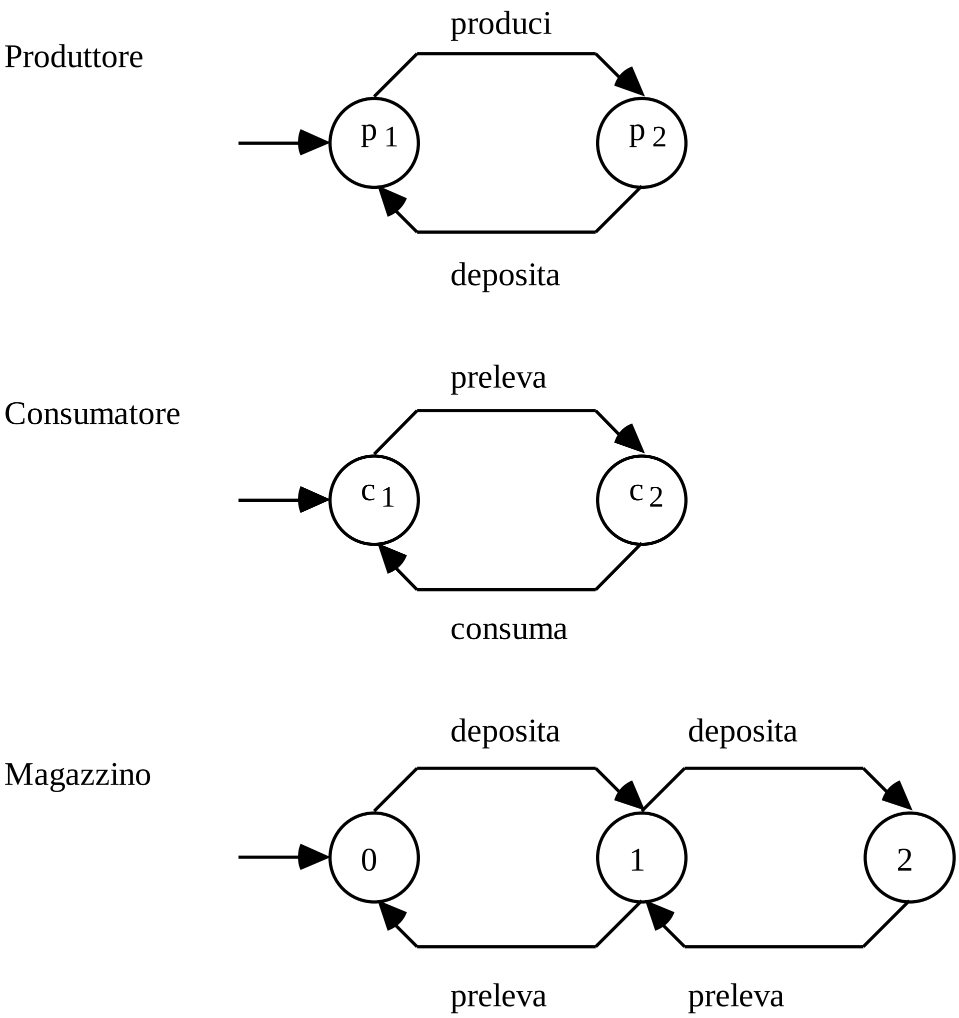
- In generale, se un sistema s è composto di n sottosistemi s_1, s_2, …, s_n e il numero di stati dei sottosistemi è rispettivamente, q_1, q_2, …, q_n, il numero di stati q di s è $q = q_1 \cdot q_2 \cdot \ldots \cdot q_n$

- La complessità dell'automa risultante (in termini di numero di stati) è ben maggiore di quella che risulterebbe esaminando ciascun componente separatamente, e cioè $q_1 + q_2 + \ldots + q_n$

- Altri sistemi di specifica (Reti di Petri)

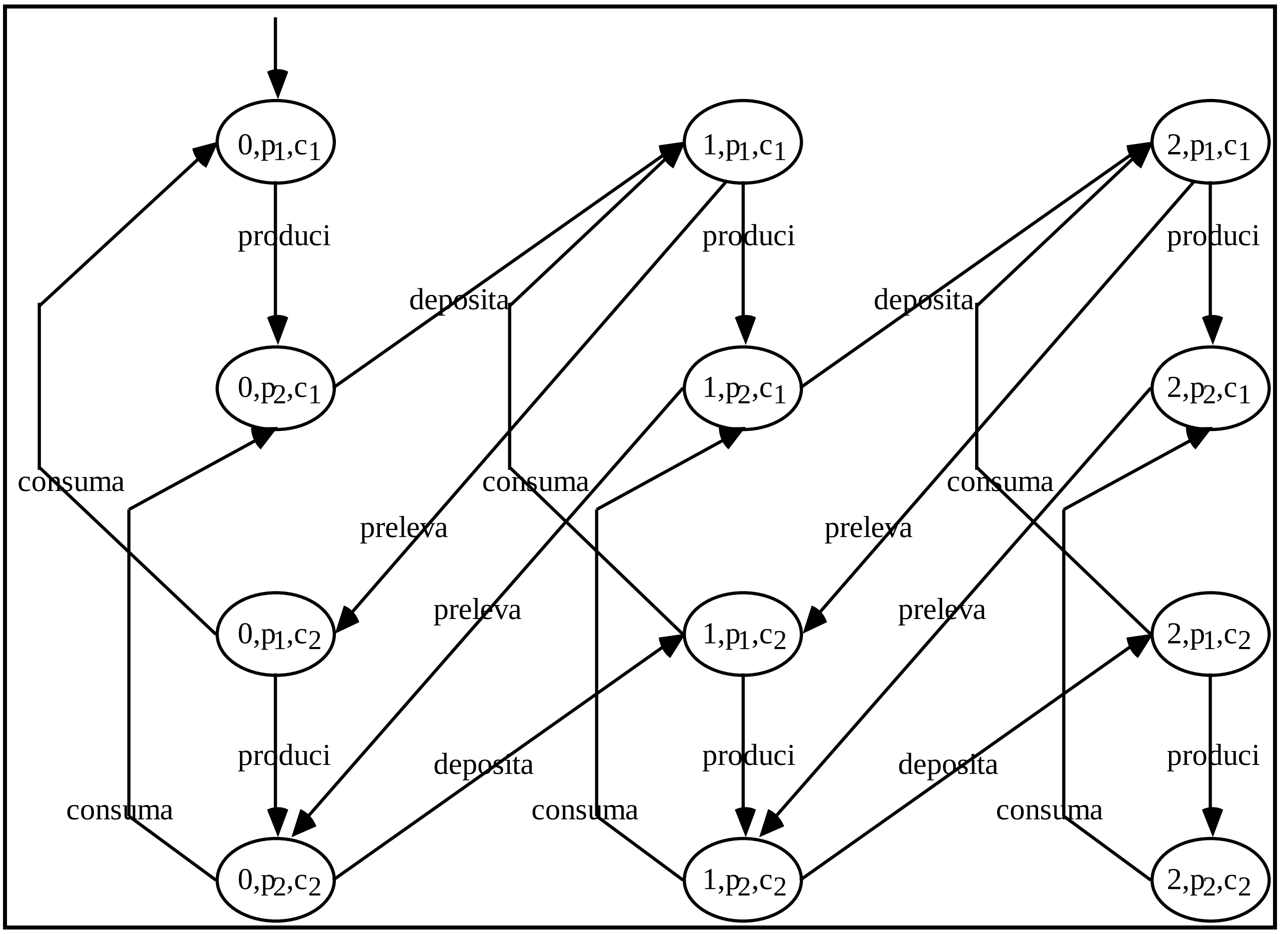
Esempio:

- Sistema concorrente, costituito da tre sottosistemi (produttore, consumatore e magazzino), ciascuno modellato da un automa a stati finiti



Il magazzino ha tre stati, corrispondenti a magazzino vuoto, magazzino contenente un elemento e magazzino contenente due elementi (per ipotesi, capacita` massima pari a due)

Volendo descrivere anche le interazioni tra i sottosistemi modellati dai tre automi precedenti, si ottiene:



FSA: considerazioni finali

- Modello orientato alla ***specifica del controllo***

- Notazione adatta per macchine che hanno da 1 a 10 stati

- La ***composizione*** di FSA e` un'operazione che genera un FSA piu` complesso:

  - l'insieme degli stati e` il prodotto cartesiano degli stati dei componennti

  - archi che denotano la stessa azione in componenti diverse devono diventare unici nella macchina finale

- Modello ***sincrono*** di un sistema: in ogni momento, uno stato globale e una sola azione possibile

- E` un modello troppo semplice:

  - memoria finita

  - impossibilita` di specificare condizioni sulle transizioni

  - impossibilita` di specificare azioni concorrenti alle transizioni

Le Reti di Petri

- Utilizzate per modellare sistemi concorrenti

- Estensione dei modelli ad automi a stati finiti, (nuova concezione di stato e di transizione di stato)

- Lo stato di un sistema e la transizione che porta il sistema da uno stato originario a un nuovo stato sono concetti distribuiti: ogni stato è la riunione di più stati parziali e indipendenti e una transizione in generale non riguarda lo stato globale del sistema, ma si limita a variarne solo una parte

- Due ***eventi*** che in un determinato stato possano verificarsi l'uno indipendentemente dall'altro vengono rappresentati da due ***transizioni*** della rete che possono avere luogo ***concorrentemente***

- Negli automi a stati, invece, il verificarsi di una transizione impedisce alle altre di avere luogo

- Possibilità di modellare ***sistemi asincroni***, in cui cioè gli eventi non sono forzati ad accadere secondo una frequenza definita

- Si astrae completamente da ogni nozione di tempo e si definisce soltanto un ordinamento parziale tra gli eventi (precedenze)

Definizione (1): Rete

Una rete N è una tripla:

$$N = (P,T;F)$$

dove P è detto insieme dei ***posti***, T è detto insieme delle ***transizioni*** e F è detta ***relazione di flusso***. P e T sono due insiemi finiti.

Devono valere inoltre le seguenti proprietà

(1) $P \leftrightarrow T = Ø$

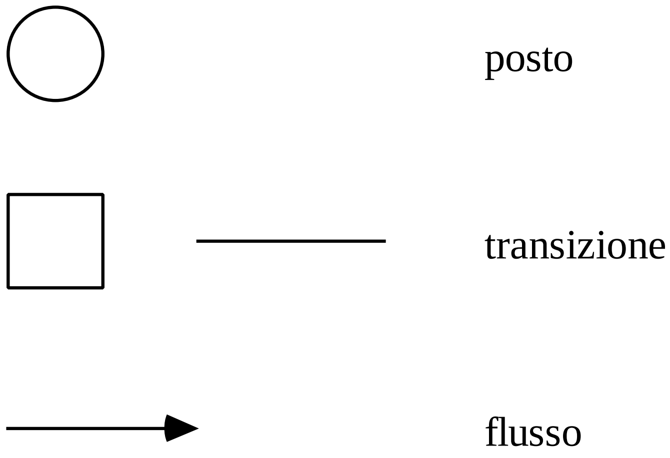
(2) $P \approx T \; ? \; Ø$

(3) $F \prod (P \infty T) \approx (T \infty P)$

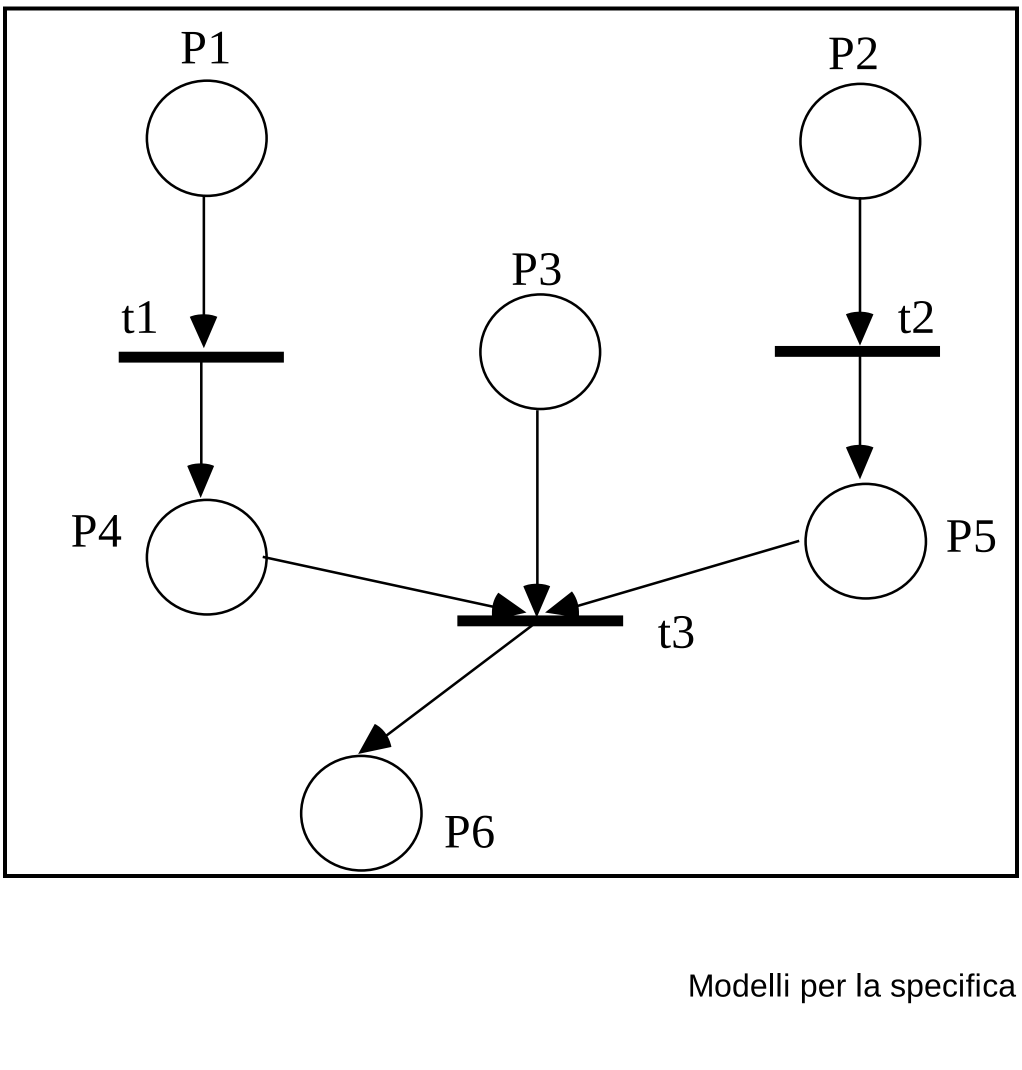
ossia (1) gli insiemi dei posti e delle transizioni sono disgiunti, (2) la rete non è vuota (esiste nella rete almeno un posto oppure una transizione) e (3) posti e transizioni sono tra loro in relazione tramite F, che lega posti a transizioni e transizioni a posti, ma non posti a posti o transizioni a transizioni

E` un particolare grafo: in un grafo infatti si ha un solo tipo di nodi, mentre in una rete si introduce una differenziazione all'interno dell'insieme dei nodi tra posti e transizioni, con i vincoli ulteriori di collegamento sopra descritti

Rappresentazione grafica



- Grafo bipartito, i cui nodi sono di due tipi distinti (i posti e le transizioni) e sono collegati tramite archi orientati (gli elementi della relazione di flusso)



Rete

- Posti, contengono informazioni relative ai possibili stati parziali della rete

- Transizioni, indicano le modifiche elementari dello stato della rete (eventi, ciascuno produce un cambiamento negli stati parziali)

- La rete evidenzia la struttura topologica del sistema indicando quale sia l'***ordinamento parziale*** che deve valere tra i nodi, ossia quali eventi possono avere luogo e in che ordine data una certa configurazione di stati parziali e quali nuove configurazioni di stati parziali possono essere generate

- In alternativa alla specifica della relazione di flusso, definizione delle funzioni *Pre* e *Post* per ogni nodo y della rete, che associano a y gli elementi d'ingresso e gli elementi di uscita

  Se X = P ≈ T, si ha:

  (3') Pre: X ∅ 2^X

  Pre(y) = {z X| <z,y> F}

  (3'') Post: X ∅ 2^X

  Post(y) = {z X| <y,z> F}

Esercizio: Costruzione di una RdP

- Si definisca la Rete di Petri relativa a una macchina che esegue ordini.

- Si abbiano quattro eventi:

  e1: arriva un ordine

  e2: inizia l'elaborazione dell'ordine

  e3: termina l'elaborazione dell'ordine

  e4: viene prodotto il risultato

- La macchina puo` essere nelle condizioni:

  m1: bloccata in attesa di ordini

  m2: in corso di elaborazione di un ordine

- Un ordine puo` essere in una delle tre condizioni:

  o1: bloccato in attesa di essere elaborato

  o2: in corso di elaborazione

  o3: elaborato

(Si noti che m2=o2)

- Le condizioni significative sono quindi solo quattro:

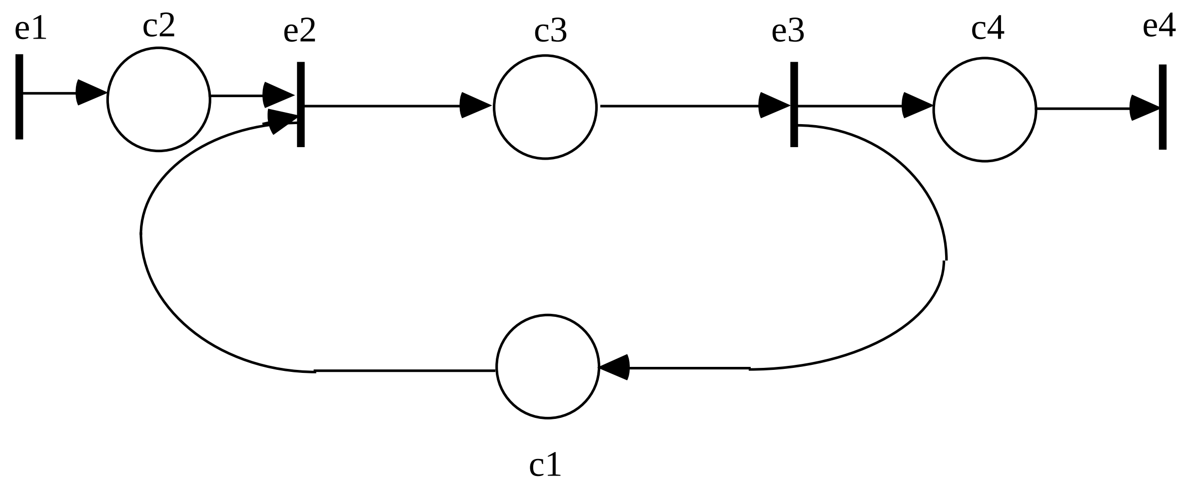
  c1: macchina bloccata in attesa di ordini

  c2: ordine bloccato in attesa di essere elaborato

  c3: ordine in corso di elaborazione

  c4: ordine elaborato

Evento	**Pre-cond**	**Post-cond**
e1	-	c2
e2	c1, c2	c3
e3	c3	c4, c1
e4	c4	-



Marcatura di una rete

Definizione (2): Rete Posti/Transizioni

Una rete Posti/Transizioni (o rete P/T) è una quintupla:

$$P/T = (P,T;F,W,M_0)$$

dove P, T e F definiscono una rete e W e M_0 sono due funzioni:

(4) $W: F \varnothing N-\{0\}$

(5) $M_0: P \varnothing N$

dove (4) W associa a ogni elemento della relazione di flusso un numero intero positivo detto ***peso*** o molteplicità e (5) M_0, detta ***marcatura iniziale*** della rete P/T, associa a ogni posto un numero intero non negativo

- La marcatura iniziale M_0 indica l'insieme degli stati parziali, ossia lo stato globale, in cui la rete si trova all'inizio della sua evoluzione

Rappresentazione grafica delle reti di Petri

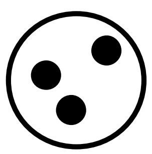
- Consente simulazioni o almeno animazioni, per esaminare rapidamente e chiaramente il comportamento del sistema

- Rete P/T come un grafo bipartito

- La funzione peso W viene rappresentata con un'annotazione sull'arco corrispondente

- La funzione marcatura M viene rappresentata con dei *token* (marche) rappresentati da tondini neri all'interno di un posto in numero uguale al valore che la funzione M assume nel posto

peso

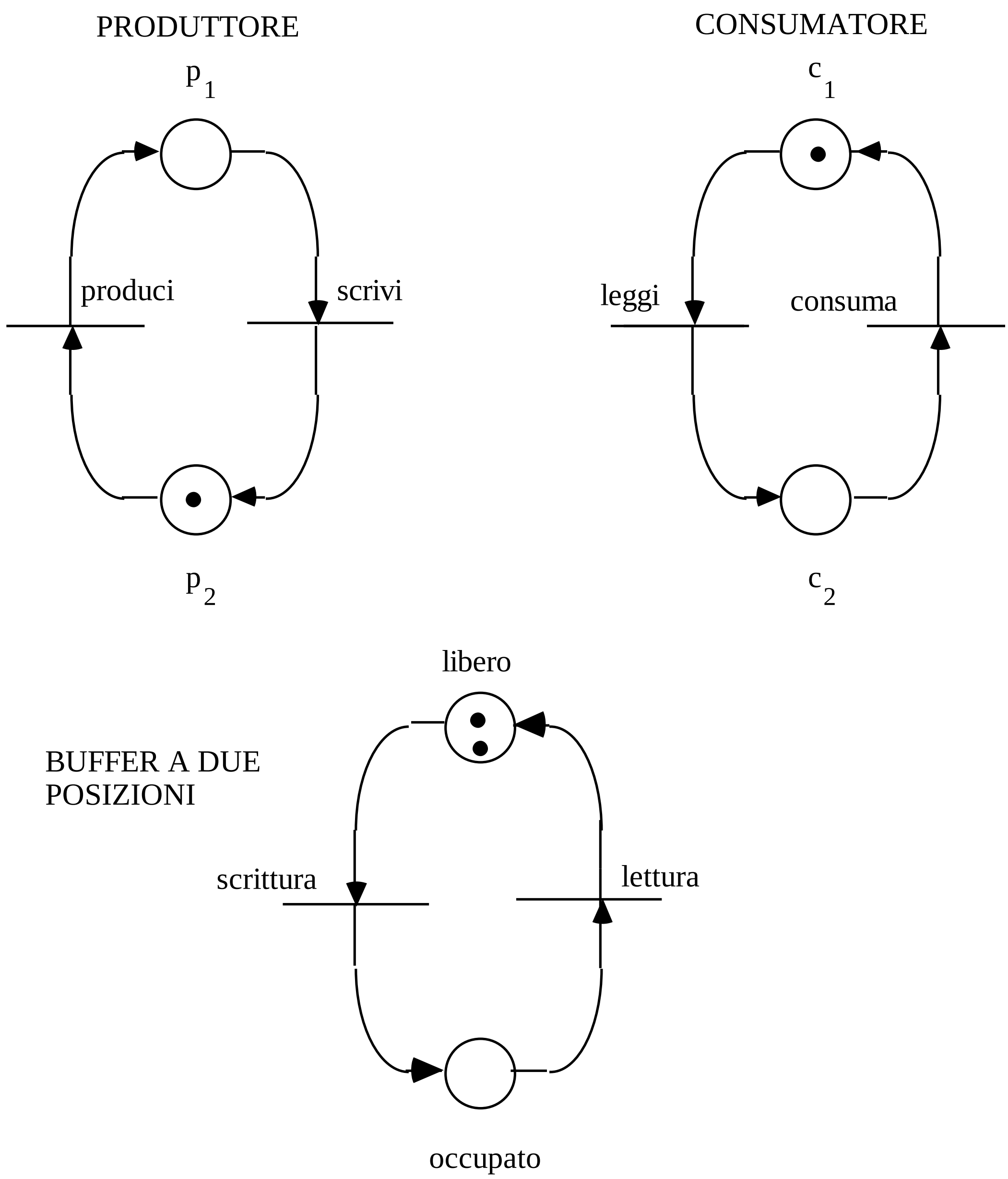


marcatura

- Un token in un posto indica che la condizione associata e` verificata

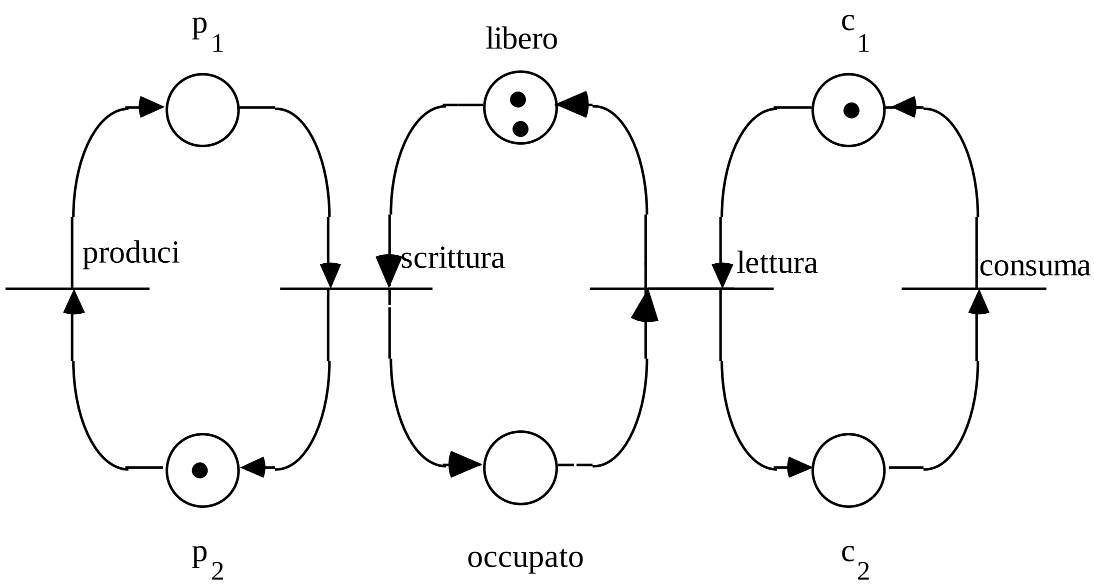
Esempio: Produttore/Consumatore/Magazzino

- Tre Reti di Petri:

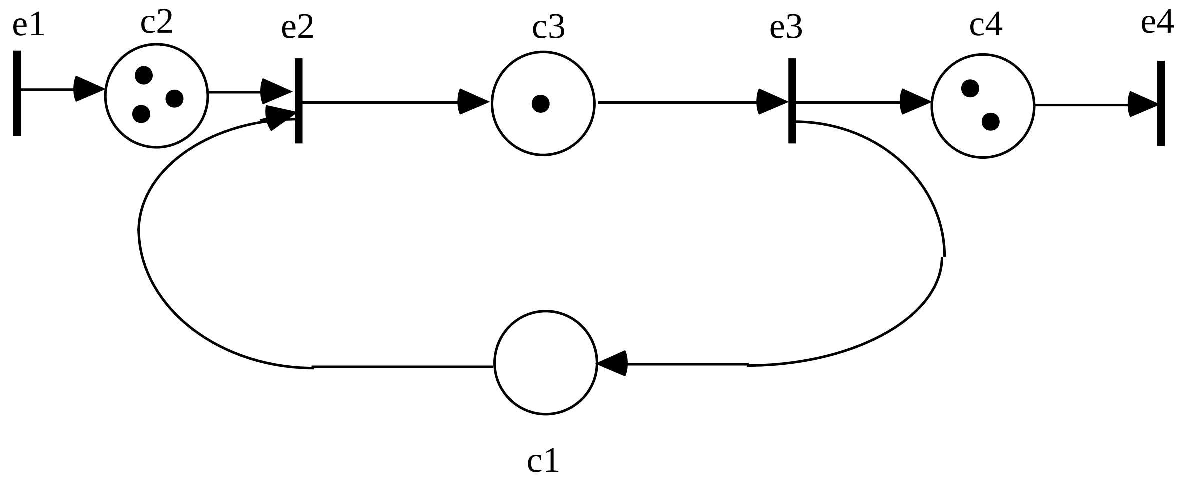


Esempio: Produttore/Consumatore/Magazzino

- La rete combinata si ottiene a partire dalle singole componenti identificando le transizioni comuni:



Esempio elaborazione ordini:



Tre ordini in attesa, uno in elaborazione, due evasi

Evoluzione della rete

- Il sistema modellato da una rete P/T evolve tramite il verificarsi di uno o più eventi

- Per il verificarsi di un evento, occorre considerare due aspetti:
  - Possibilità che l'evento si verifichi, detto ***abilitazione*** di una transizione (esame della marcatura)
  - Effetto che l'evento ha sullo stato del sistema, detto ***regola di scatto*** di una transizione (generazione di una nuova marcatura a partire da quella preesistente a tale scatto)

- Una transizione t è abilitata (può scattare o ha concessione in una marcatura M) quando in M ogni posto p d'ingresso a t contiene un numero di token almeno uguale (>=) al peso dell'arco che collega p a t

Definizione (3): Abilitazione di una transizione

Una transizione t è abilitata nella marcatura M se e solo se:

$$\forall p \quad Pre(t), \quad M(p) = W(<p,t>)$$

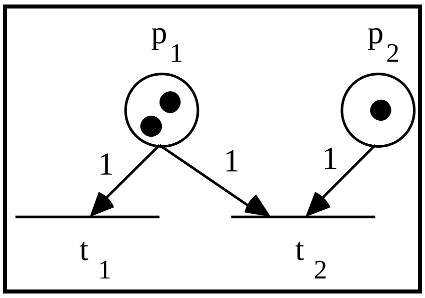
- Il fatto che una transizione t sia abilitata in una determinata marcatura M viene abbreviato con la notazione:

  M[t>

- L'insieme di token che abilita una transizione t viene detto ***tupla abilitante*** di t

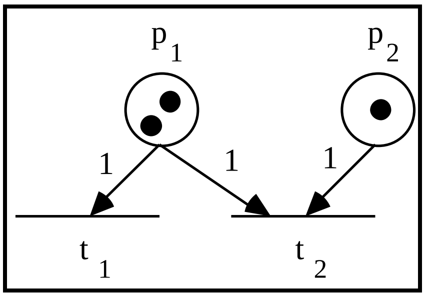
- Una transizione sotto una determinata marcatura può avere più di una tupla abilitante

  Esempio: la transizione t_1 è abilitata indipendentemente da due token in p_1



- Uno stesso token può appartenere a due diverse tuple abilitanti che possono anche riguardare due transizioni diverse

  Esempio: i token in p_1 abilitano sia t_1 sia t_2



Scatto di una transizione

- Può avvenire solo se la transizione è abilitata a scattare nella marcatura M

- Produce una nuova marcatura M' tale che:
  - da ogni posto p in ingresso a t viene rimosso un numero di token uguale al peso dell'arco che collega p a t
  - in ogni posto q in uscita a t viene depositato un numero di token uguale al peso dell'arco che collega t a q
  - la marcatura dei posti che non siano né d'ingresso né d'uscita a t rimane inalterata

Definizione (4): Scatto di una transizione

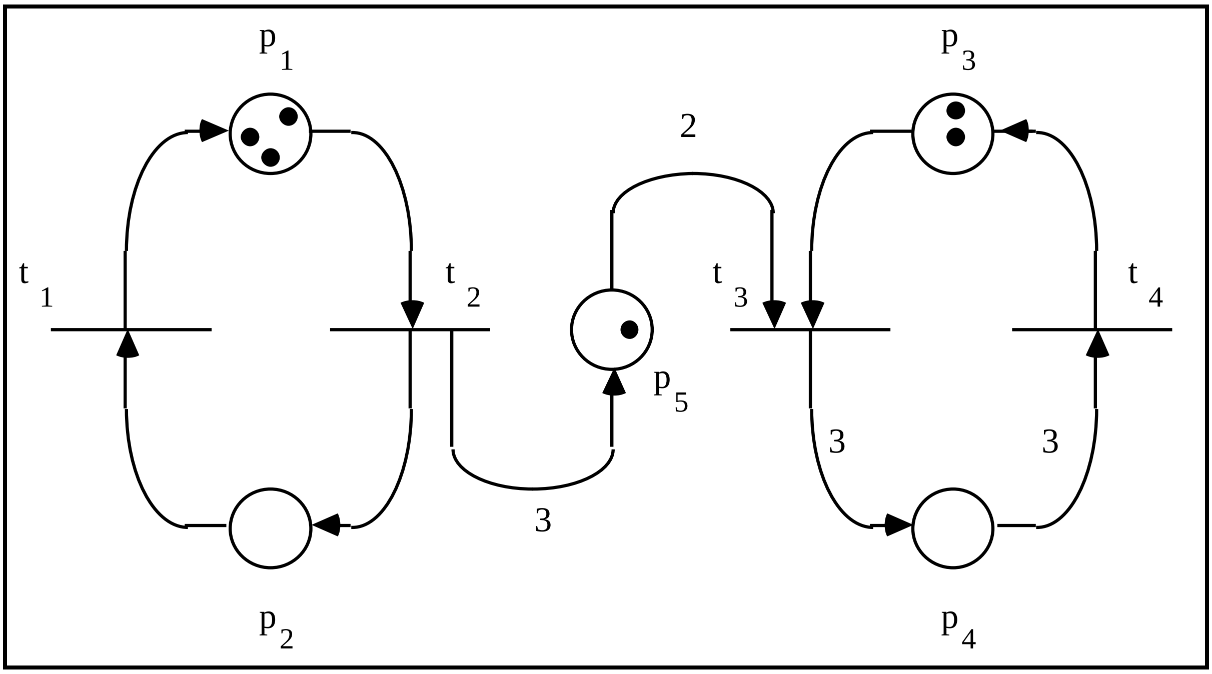
Data la marcatura M, lo scatto di una transizione t abilitata produce la nuova marcatura M' tale che:

∀p	Pre(t) - Post(t)	M'(p) = M(p) - W(<p,t>)
∀p	Post(t) - Pre(t)	M'(p) = M(p) + W(<t,p>)
∀p	Post(t) ↔ Pre(t)	M'(p)=M(p) - W(<p,t>) + W(<t,p>)
∀p	P-(Post(t)≈Pre(t))	M'(p) = M(p)

- Lo scatto della transizione t che porta da M a si indica con la notazione:

M [t> M'

Esempio produttori/consumatori

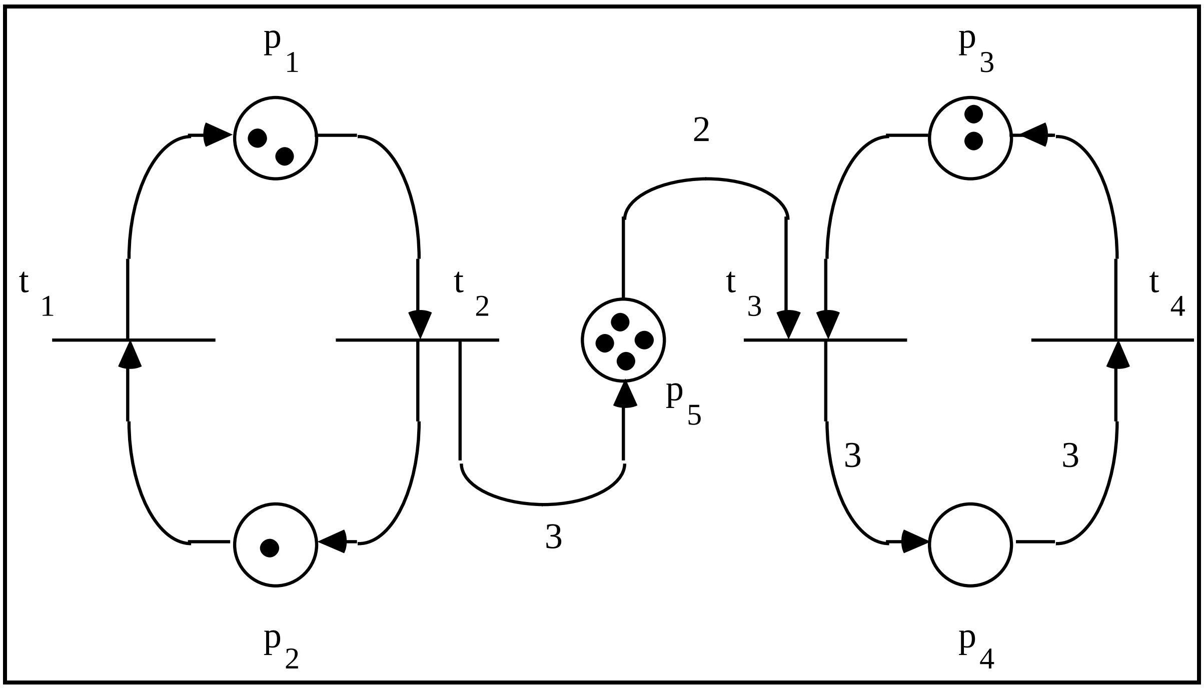


- Tre produttori (rappresentati dai tre token nel posto p_1), due consumatori (rappresentati dai due token in p_3)

- Il token in p_5 rappresenta un oggetto che, creato dai produttori, attende di essere utilizzato da un consumatore

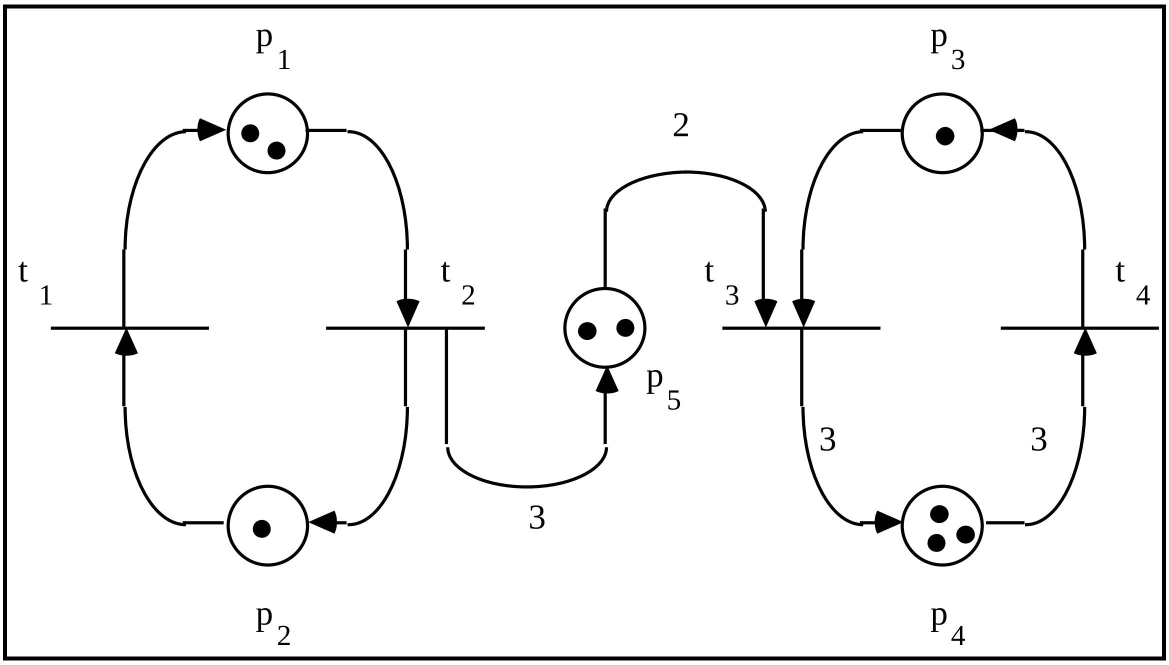
- Scatta t_2 (unica abilitata)

- Viene depositato un token in p_2 e si aggiungono tre token in p_5



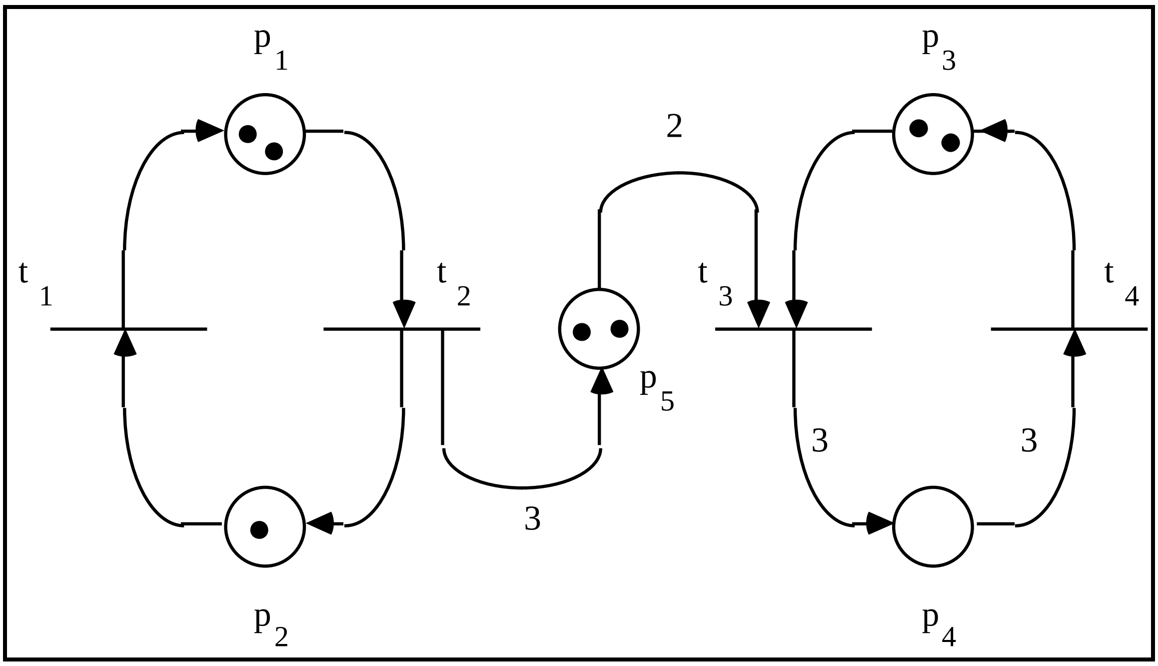
- Ora possono scattare tre transizioni, corrispondenti agli eventi possibili:
  - la produzione ancora di 3 oggetti (scatto di t_2)
  - il rifornimento del processo che ha appena prodotto i tre oggetti e il cui token corrispondente si trova ora in p_2 (scatto di t_1)
  - l'appropriazione di due qualsiasi degli oggetti prodotti, rappresentati dai token in p_5, da parte di un consumatore (scatto di t_3)

- Assumendo che scatti t_3:



,

- A partire da questa nuova marcatura si avrà tra le transizioni abilitate (in questo caso t_1, t_2, t_3 e t_4) una transizione che scatta (a esempio t_4):



e così via l'evoluzione della rete prosegue

Rappresentazione matriciale:

- Utile per poter effettuare analisi automatiche della rete

- Si associa un numero intero positivo a ciascun posto e ciascuna transizione, tramite le corrispondenze:

  p: 1..|P| ∅ P

  t: 1..|T| ∅ T

  (|P| e |T| cardinalità di P e T)

- Si costruiscono due matrici I e O che hanno una riga per ogni posto della rete e una colonna per ogni transizione della rete (matrici di dimensione |P| ∞ |T|)

Precondizioni

- L'elemento di I di posto (i,j) è un numero intero non negativo che indica il peso dell'arco che collega l'i-esimo posto alla j-esima transizione (0 se non sono collegati)

$\forall <p(i),t(j)> \quad F \qquad I_{i,j} = W(<p(i),t(j)>)$

$\forall <p(i),t(j)> \quad F \qquad I_{i,j} = 0$

Postcondizioni

- L'elemento di o di posto (i,j) è un numero intero non negativo che indica il peso dell'arco che collega la j-esima transizione all'i-esimo posto (0 se non sono collegati)

$\forall <t(j),p(i)> \quad F \qquad O_{i,j} = W(<t(j),p(i)>)$

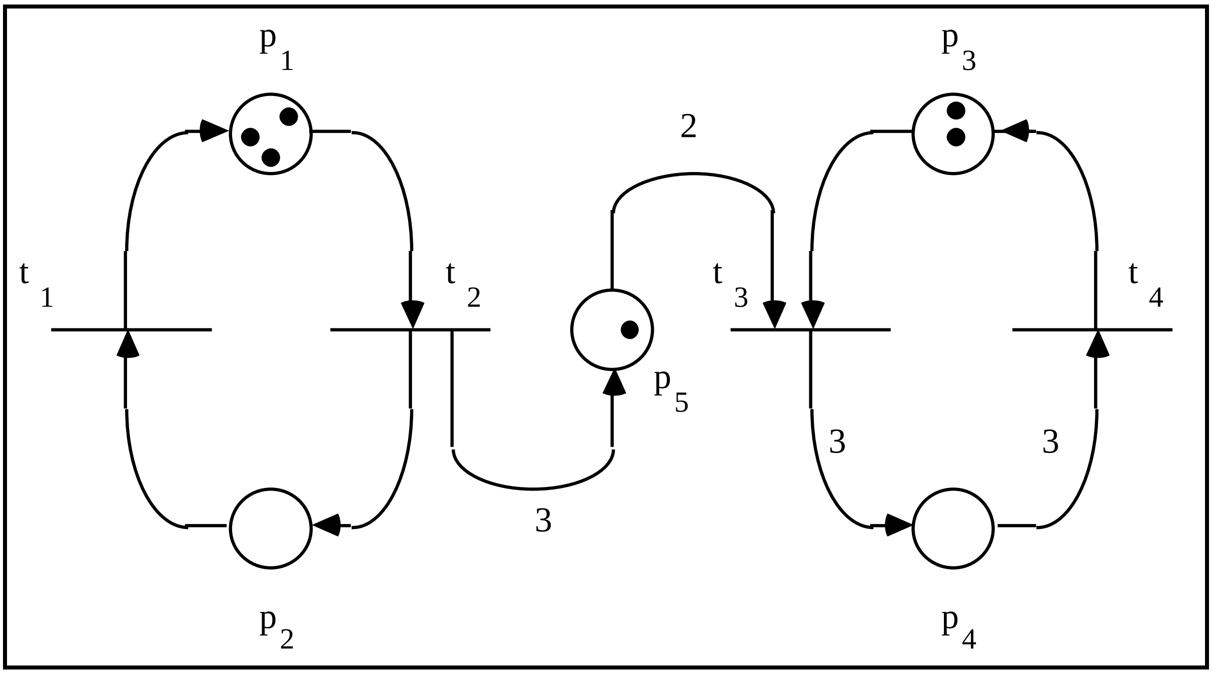
$\forall <t(j),p(i)> \quad F \qquad O_{i,j} = 0$

Marcatura

- La marcatura M viene definita come un vettore m, di dimensione $(1 \infty |P|)$, le cui componenti sono interi non negativi che indicano il numero di token presenti in ogni posto

$$m_i = M(p(i))$$

Esempio produttori/consumatori



$$m = \left| \begin{matrix} 3 \\ 0 \\ 2 \\ 0 \\ 1 \end{matrix} \right|$$

$$O = \left| \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 3 & 0 \\ 0 & 3 & 0 & 0 \end{matrix} \right| \qquad I = \left| \begin{matrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 2 & 0 \end{matrix} \right|$$

Rappresentazione matriciale (cont):

- I concetti di abilitazione e di scatto di una transizione t(j) possono essere dati nuovamente in base alla definizione matriciale

- t(j) è abilitata se e solo se, definito il vettore colonna $I_{.,j}$ come la j-esima colonna della matrice I, risulta m = $I_{.,j}$

- Lo scatto di transizione t(j) produce a partire dalla marcatura m una nuova marcatura:

$$m' = m - I_{.,j} + O_{.,j}$$

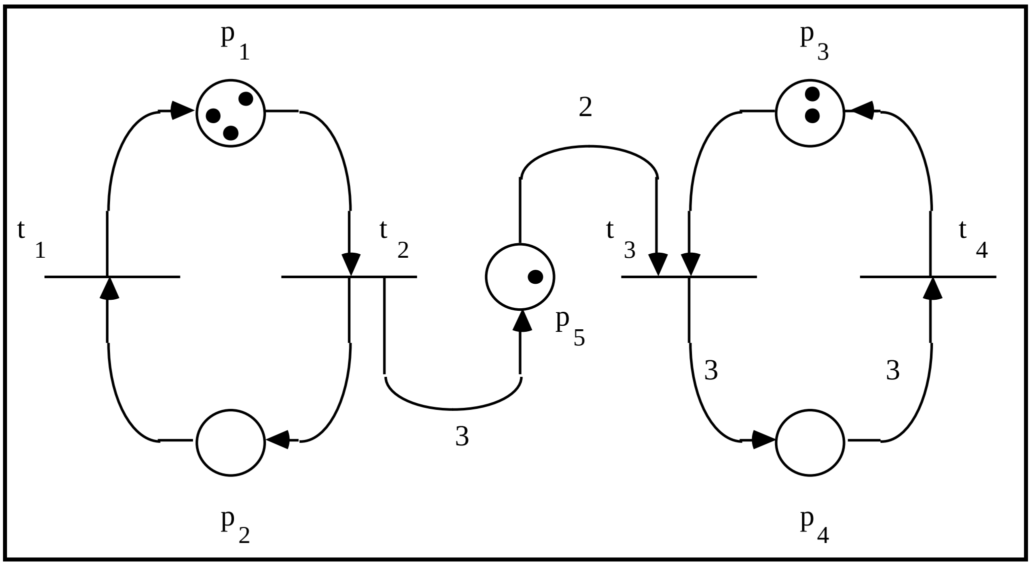
- Variazione data dalla differenza tra i due vettori colonna rispettivamente delle matrici O e I corrispondenti a t(j)

- Matrice d'incidenza della rete:

$$C = O - I$$

rappresenta la variazione di marcatura che si verifica a causa dello scatto di una qualunque transizione

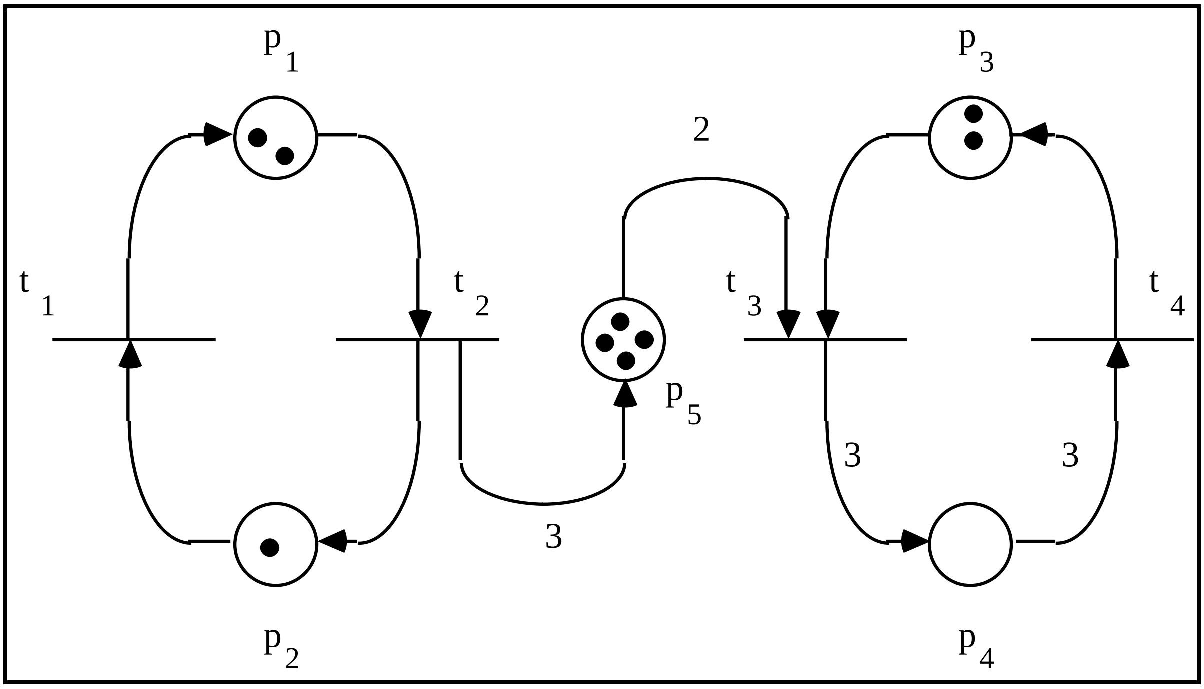
Esempio produttori/consumatori



$$O = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 3 & 0 \\ 0 & 3 & 0 & 0 \end{vmatrix} \qquad I = \begin{vmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 2 & 0 \end{vmatrix}$$

$$C = O - I = \begin{vmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 3 & -3 \\ 0 & 3 & -2 & 0 \end{vmatrix}$$

$$m = \begin{vmatrix} 3 \\ 0 \\ 2 \\ 0 \\ 1 \end{vmatrix} \qquad \text{Scatta t2:} \qquad m' = \begin{vmatrix} 2 \\ 1 \\ 2 \\ 0 \\ 4 \end{vmatrix}$$



$$m' = \begin{vmatrix} 2 \\ 1 \\ 2 \\ 0 \\ 4 \end{vmatrix}$$

- In generale non è possibile decidere correttamente sull'abilitazione di una transizione sulla base delle informazioni contenute nella sola C

- Esiste però un caso in cui la matrice C mantiene le stesse informazioni delle matrici I e O e si verifica per le cosiddette reti pure, nelle quali si esclude che un posto sia d'ingresso e di uscita a una medesima transizione

- Una rete pura è una rete P/T in cui

$$\forall t \quad T, Pre(t) \leftrightarrow Post(t) = Ø$$

Ad esempio la rete precedente è pura

Sequenze di scatti

- La sequenza di scatti $t_1 t_2$ è abilitata in M se t_1 e\` abilitata in M e, a sua volta, $t_2$ e\`abilitata in M' marcatura raggiunta dopo lo scatto di t1:

$$M\,[t_1\!> M' \quad M'\,[t_2\!> M'' \quad M\,[t_1 t_2\!> M''$$

- Per ricorsione, considerata una sequenza di scatti $S^{(n)} = t_1 \ldots t_n$ di lunghezza n arbitraria, si utilizza la notazione:

$$M[t_1 \ldots t_n\!>M^{(n)} \quad M[S^{(n)}\!> M^{(n)}$$

- L'evoluzione di una rete P/T consiste quindi di una sequenza di eventi discreti

- Tramite la notazione matriciale è possibile calcolare, note una marcatura M e una sequenza di scatti S ammissibile a partire da M, la marcatura che ne consegue

- Data una sequenza di scatti S ammissibile, si definisce allora un vettore s, di dimensione (|T| ∞ 1), le cui componenti riportano il numero di scatti delle singole transizioni t(j) nella sequenza S

- Si può dimostrare quindi che se M[S>M' allora

$$\boxed{m' = m + C s}$$

- Tale formula, detta equazione fondamentale, mostra la linearità intrinseca all'evoluzione delle reti P/T

Scelta della transizione

- Il meccanismo utilizzato per individuare la transizione che scatta è del tutto non-deterministico

- L'abilitazione e il conseguente scatto di una transizione non devono dipendere da altre circostanze al di fuori della marcatura dei posti d'ingresso alla transizione

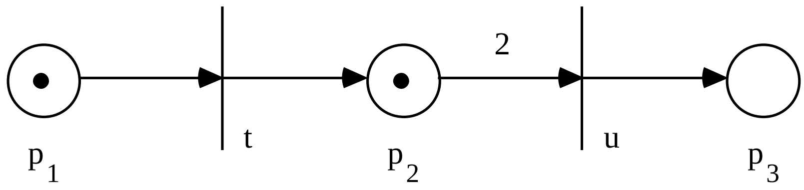
- Nell'esempio produttori e consumatori l'unica interazione si limita alla ricezione da parte dei consumatori degli oggetti creati dai produttori (nel modello a rete P/T i produttori in linea teorica potrebbero continuare a depositare token in p_5 indefinitamente anche prima che una sola coppia di oggetti venga presa da un consumatore)

- Qualsiasi limitazione e sincronizzazione alle attività deve comparire esplicitamente

- Si prescinde inoltre totalmente dalla nozione di tempo: tutto ciò che interessa sono le dipendenze di ordinamento parziale tra gli eventi.

Situazioni riguardanti coppie di transizioni

- Sequenza



Nell'esempio, l'unica transizione abilitata è t, visto che u, il cui scatto richiede la presenza di due token in p_2, può scattare solo dopo che è scattata t

- Conflitto

Due transizioni abilitate nella marcatura corrente hanno almeno un posto d'ingresso in comune

- Conflitto strutturale

Si verifica quando due transizioni t e u hanno almeno un posto d'ingresso in comune, ovvero quando

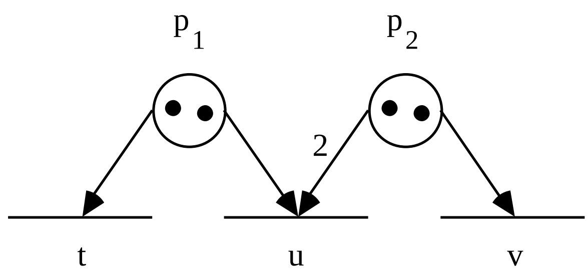
$$Pre(t) \leftrightarrow Pre(u) \ ? \ Ø$$

• Conflitto effettivo

Due transizioni t e u si dicono in conflitto effettivo nella marcatura M se sono in conflitto strutturale, sono entrambe abilitate in M e il numero di token che i loro posti d'ingresso contengono non è sufficiente a soddisfare tutti i pesi degli archi che li collegano alle due transizioni

M[t>   M[u>

$$\exists\, p \quad Pre(t) \leftrightarrow Pre(u)\ (M(p) < W(<p,t>) + W(<p,u>))$$



Conflitto strutturale, rispettivamente tra le transizioni t e u e tra le transizioni u e v

Solo il conflitto tra u e v è però un conflitto effettivo: se infatti scatta t, u permane abilitata e viceversa, mentre lo scatto di u rende impossibile lo scatto di v e viceversa

Reti Condizioni/Eventi (C/E)

- Tre limitazioni rispetto alle RdP:

  - Sono reti con archi di peso unitario

  - Tutti i posti hanno capacità unitaria, ossia non possono contenere più di un token, e ciò implica che

  - Una transizione è abilitata se e solo se tutti i suoi posti d'ingresso contengono un token e tutti i suoi posti d'uscita sono vuoti

- Con l'interpretazione:

  Transizione ❸ Evento

  Posto ❸ Condizione

  un evento può avere luogo se e solo se tutte le sue precondizioni valgono (i posti d'ingresso sono pieni) e tutte le sue postcondizioni non sono soddisfatte (i posti d'uscita sono vuoti)

- Scatto della transizione: le precondizioni dell'evento cessano di valere mentre cominciano a valere le sue postcondizioni

Vantaggi:

- Non vi è distinzione tra conflitto strutturale e conflitto effettivo: ciò rende l'analisi statica della rete molto più efficace che nel caso delle reti P/T

- Qualunque rete P/T (con numero massimo di token in ogni posto limitato) è trasformabile in una rete C/E equivalente

- Modellare un sistema tramite una rete di Petri è utile poiche` sulla rete possono essere svolte svariate analisi che diano un'indicazione sull'effettivo comportamento del sistema, anche se ...

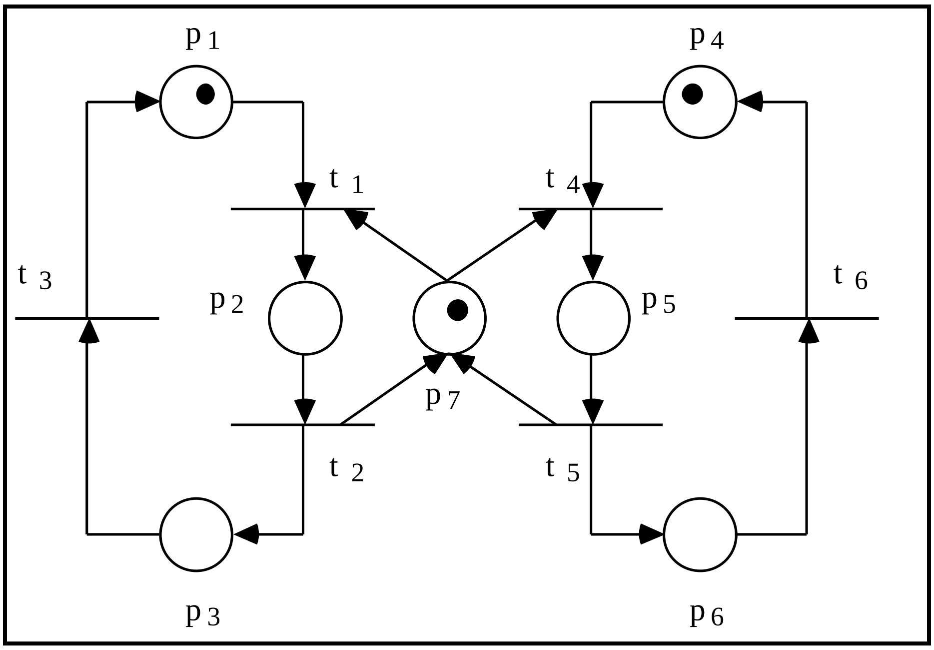
- ... alcune proprietà di interesse sono nel caso generale indecidibili o comunque decidibili, ma a prezzo di una complessità assai elevata

Proprieta` delle Reti di Petri:

- Binarietà (Safeness)

Una rete P/T si dice binaria (safe) se in ogni suo posto, quale che sia l'evoluzione della rete, non si può mai avere più di un token

Condizione sufficiente: marcatura iniziale binaria e che tutte le marcature raggiungibili siano anch'esse binarie



- Le reti C/E sono binarie per definizione

- I posti di una rete binaria possono essere rappresentati da bit

- Limitatezza (Boundedness)

Un posto di una rete P/T si dice k-limitato se in una qualunque marcatura raggiungibile della rete il numero di token non supera mai il valore intero prefissato k

Una rete P/T nel suo complesso si dice limitata se tutti i suoi posti sono limitati

- Se una rete è limitata, la rete stessa può avere un numero limitato di marcature distinte e risulta pertanto equivalente a un automa a stati finiti

- Qualunque rete può essere resa limitata con l'aggiunta di opportuni posti

- Vitalità (Liveness)

  Da` una misura dell'esistenza di transizioni che non possono (piu`) avvenire (situazioni di blocco critico, deadlock)

- Gradi di vitalità di una transizione

  Grado 0

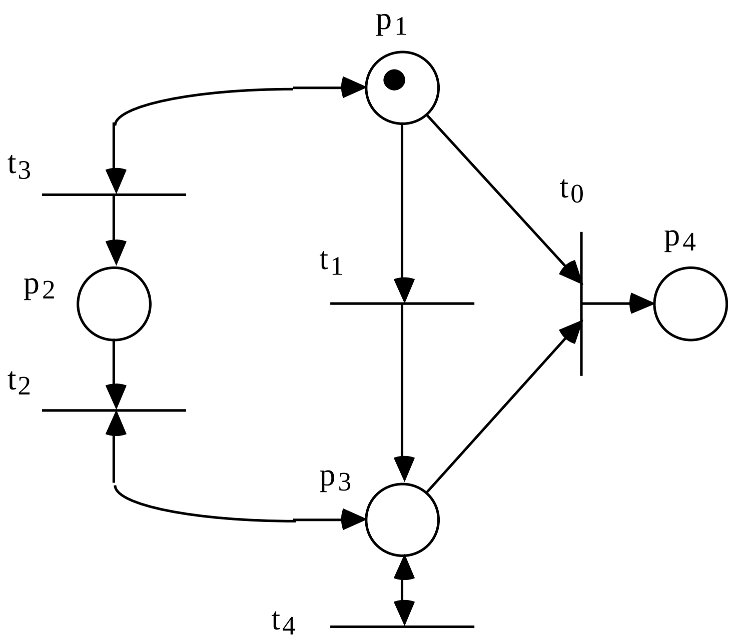
  Una transizione t è a grado 0 di vitalità se non può mai scattare in qualunque marcatura raggiungibile della rete (la transizione t è morta)

  ...

  Grado 4

  Una transizione t è a grado 4 di vitalità se data una qualunque marcatura raggiungibile esiste una sequenza di scatti che a partire da tale marcatura abiliti t (la transizione t è viva)

- Una rete P/T si dice viva se e solo se ogni sua transizione è viva (è al quarto grado di vitalità)



- t_0 ha grado 0 di vitalità (non si puo` mai avere un token in p1 e uno in p3)

- t_1 può scattare solo una volta (grado di vitalità 1)

- t_3 può scattare a partire dalla marcatura iniziale un numero di volte che non è definito a priori (grado 3 di vitalità)

- t_2 può scattare tante volte quanto è il numero di token che si trovano in p_2, ovvero dal numero di scatti della transizione t_3 avvenuti in precedenza (grado 2 di vitalità)

- Da ogni marcatura raggiungibile esiste sempre una sequenza di scatti che rende abilitata la transizione t_4 (grado 4 di vitalità)

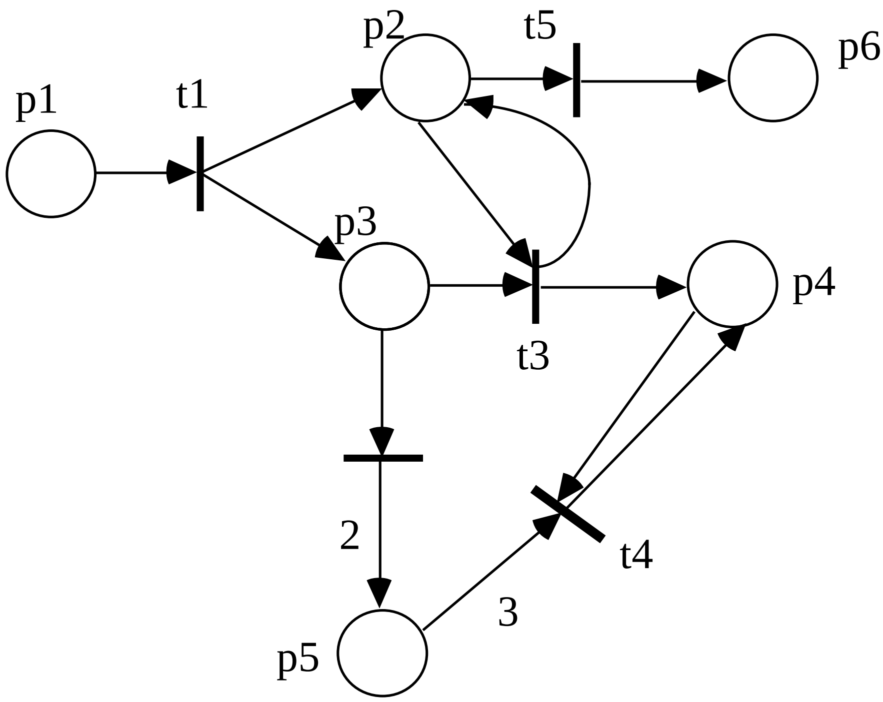
- Raggiungibilità (Reachability)

M' raggiungibile dalla marcatura M se e solo se esiste almeno una sequenza di scatti che a partire da M produca la marcatura M'

Consente di determinare se da una certa marcatura iniziale si possono raggiungere stati indesiderati

(Queste sono tutte proprieta` decidibili)

Esempio di analisi:



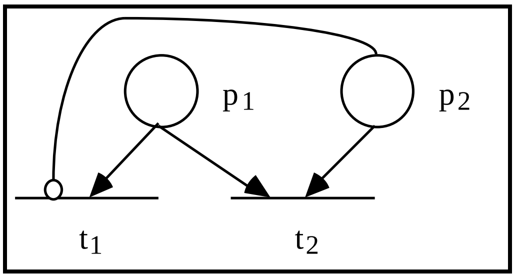
Data la marcatura iniziale:

$$m = \begin{vmatrix} 2 \\ 0 \\ 0 \\ 2 \\ 5 \\ 1 \end{vmatrix}$$

- il numero di token in p2 puo` essere > 2?
- il numero di token in un posto puo` diventare infinito?
- la rete puo` andare in stallo? (esiste una transizione che a un certo punto diventera` mai attivabile?)
- si puo` raggiungere la marcatura [0,1,1,3,5,2]?
- la sequenza t1,t2,t2,t3,t4,t5,t5,t5 e` possibile?

Estensioni alle Reti di Petri

- Archi inibitori (per disabilitare una transizione)



t_1 e` abilitata se e solo se la transizione t_2 non è abilitata

- Reti temporizzate e stocastiche

  Rappresentano gli intervalli di tempo che intercorrono tra gli eventi

- Reti di alto livello

  I token portano con sé delle informazioni, per cui non sono più completamente indistinguibili, come avviene nel caso delle reti P/T ordinarie