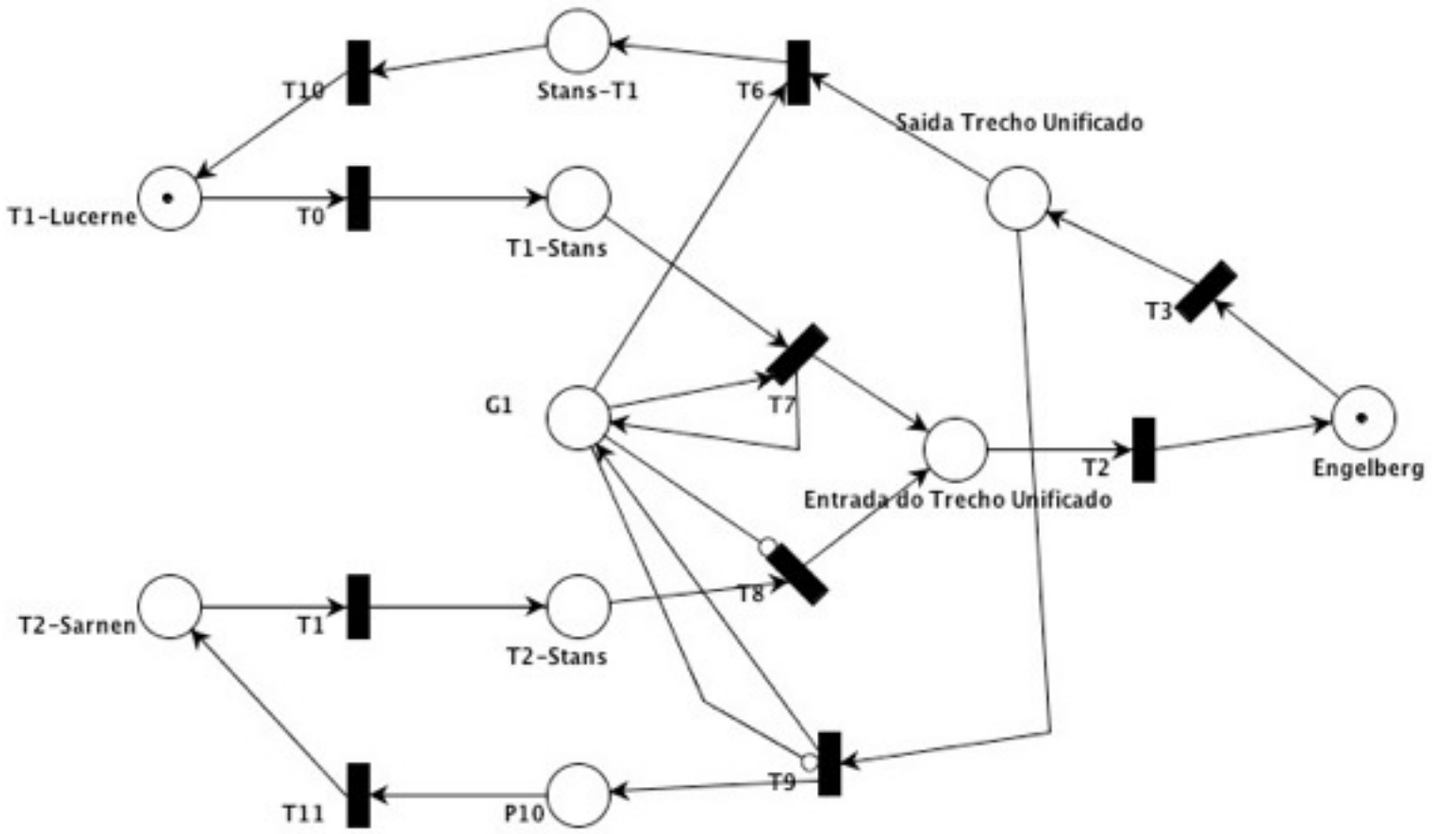
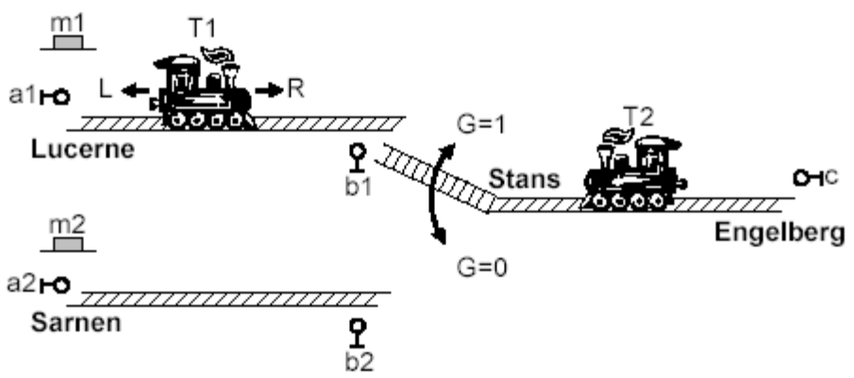
PMR 5237

Modelagem e Design de Sistemas Discretos em Redes de Petri

Aula 5: Análise de propriedades das redes P/T

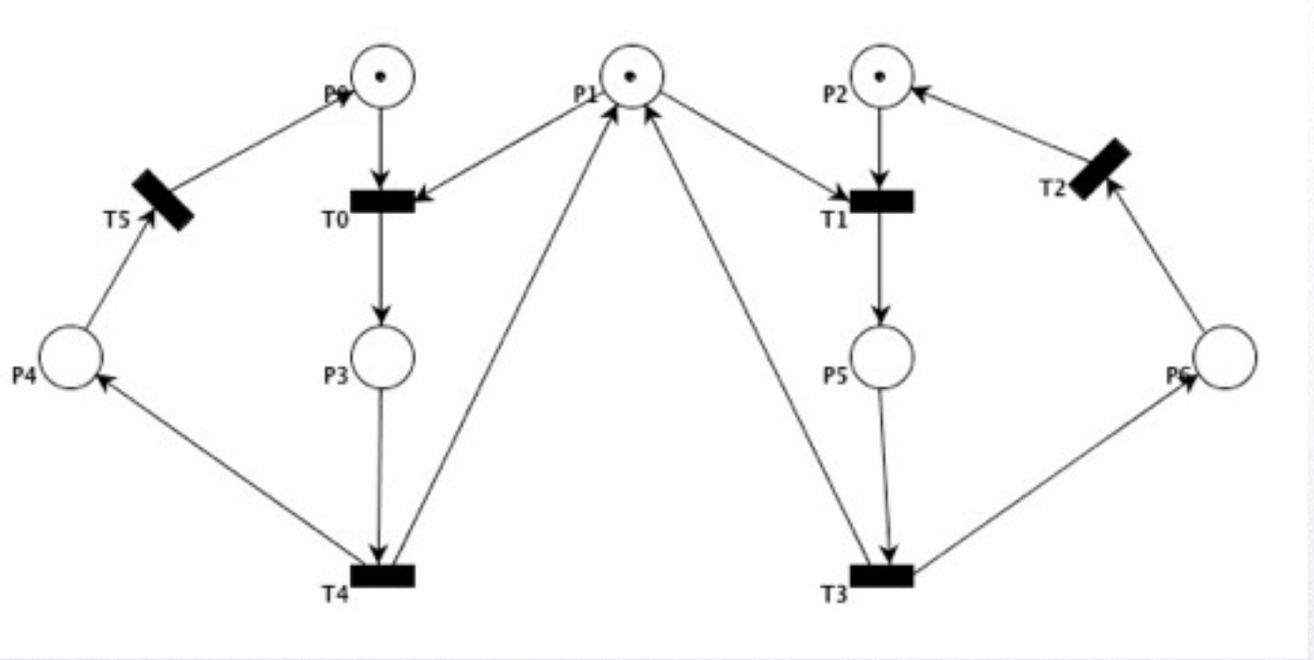
Prof. José Reinaldo Silva
reinaldo@usp.br


T10
Stans-T1
T6
Saida Trecho Unificado
T1-Lucerne
T0
T1-Stans
T3
G1
T7
T2
Engelberg
Entrada do Trecho Unificado
T8
T2-Sarnen
T1
T2-Stans
T9
T11
P10

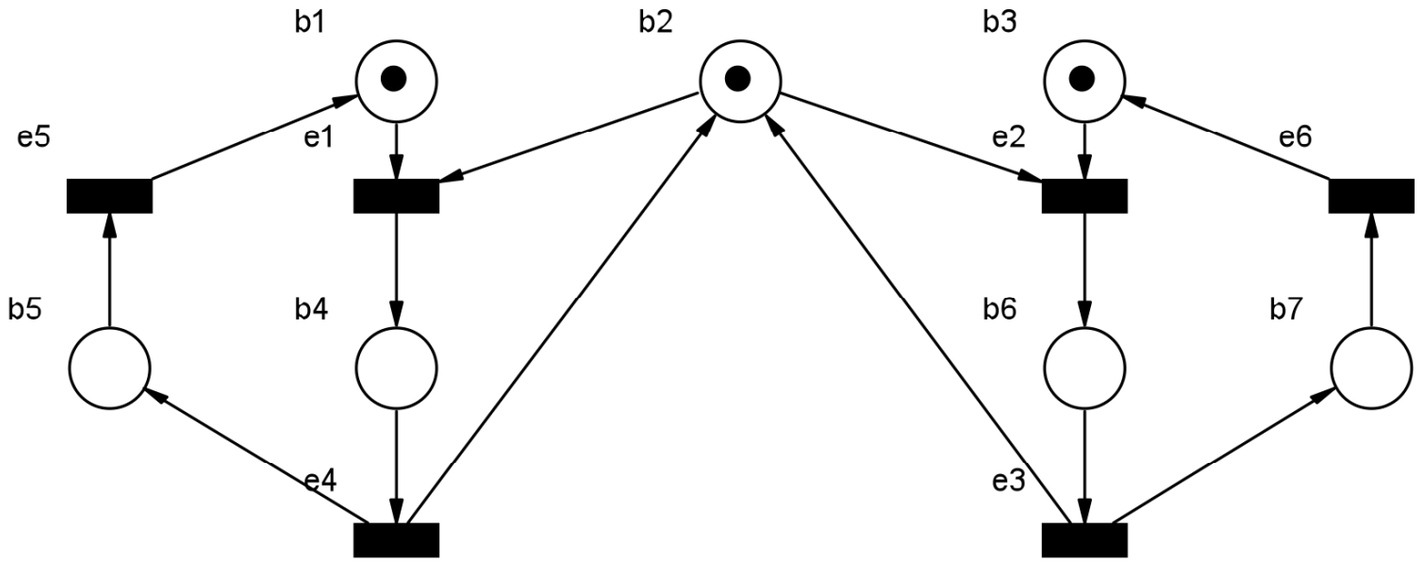

m1
T1
a1
L
R
Lucerne
G=1
T2
b1
Stans
c
Engelberg
m2
G=0
a2
Sarnen
b2

Exercicio

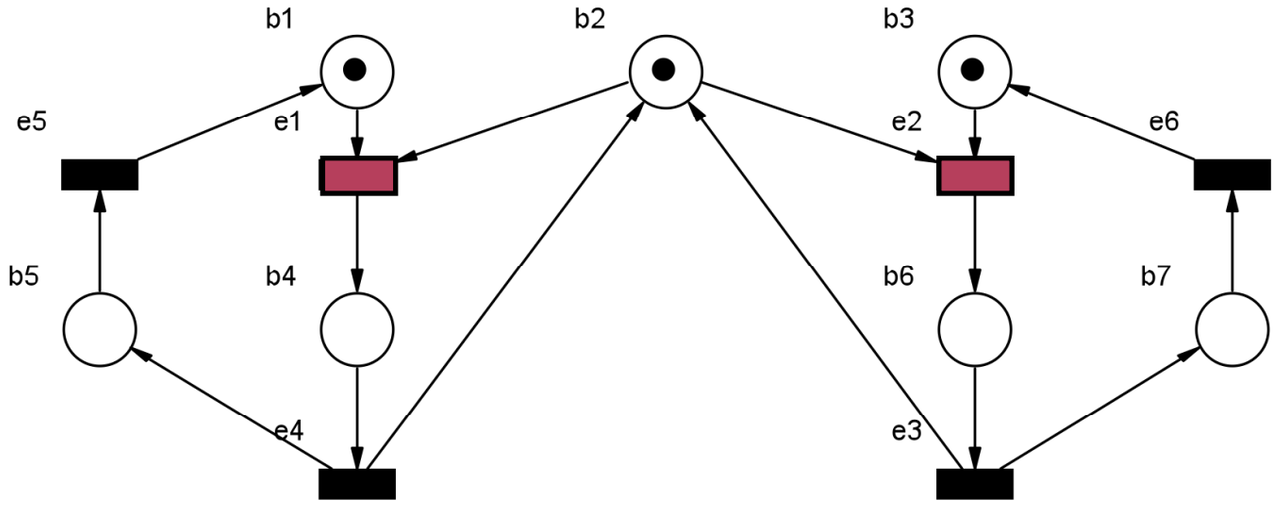
Dada a rede abaixo que representa um mutex clássico, faça com que o farol de dois tempos abra uma vez para cada rua alternadamente.



Exercício 3:



Trata-se de uma rede normal, sem loops e portanto a equação de estado pode ser plenamente determinada.



A marcação corrente é

$$M = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$A = \begin{pmatrix} -1 & -1 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 1 \\ 0 & 1 & 0 & -1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 \end{pmatrix} \quad (1)$$

Um algoritmo para determinar o vetor de habilitação pode ser especificado do seguinte modo:

- verificar a independencia das transições duas a duas, tomando o produto direto entre os vetores coluna da matriz A^T (ou as linhas da matriz A);
- determinar o conjunto de passos admissiveis do resultado acima;
- determinar, para a marcação corrente, quais as transições habilitadas e o vetor de habilitação.

Da matriz

$$A^T = \begin{pmatrix} -1 & 0 & 0 & 0 & 1 & 0 \\ -1 & -1 & 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 \end{pmatrix}$$

é possivel ver que

$e_1 \cdot e_2 = 1,\ e_1 \cdot e_3 = -1,\ e_1 \cdot e_4 = -2,\ e_1 \cdot e_5 = -1,\ e_1 \cdot e_6 = 0;$

$e_2 \cdot e_3 = -2,\ e_2 \cdot e_4 = -1,\ e_2 \cdot e_5 = 0,\ e_2 \cdot e_6 = -1;$

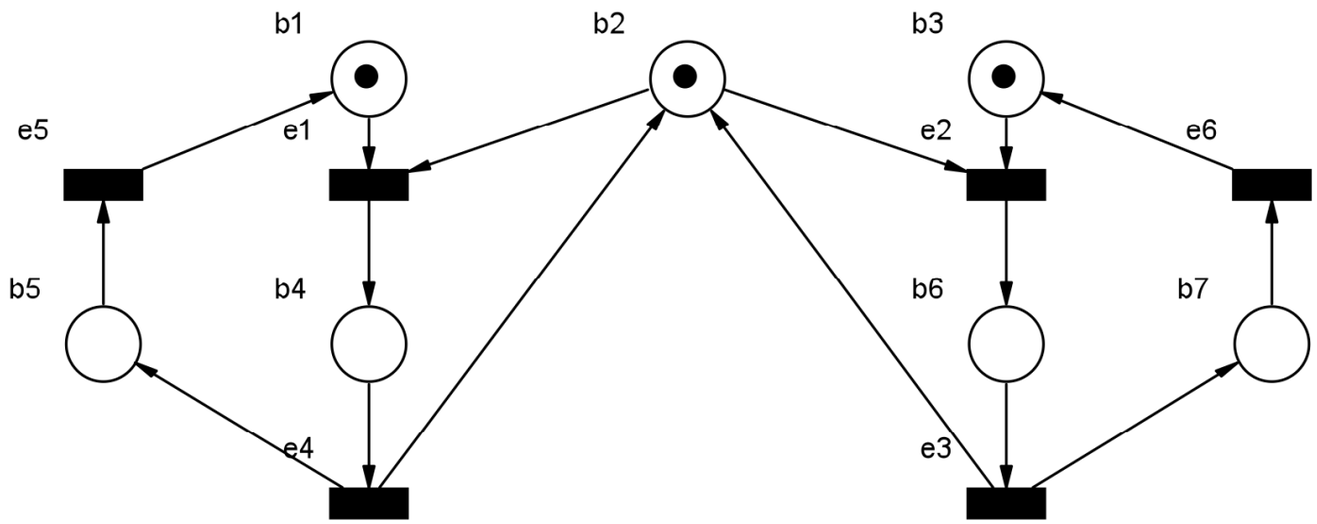
$e_3 \cdot e_4 = 1,\ e_3 \cdot e_5 = 0,\ e_3 \cdot e_6 = -1;$

$e_4 \cdot e_5 = -1,\ e_4 \cdot e_6 = 0;$

$e_5 \cdot e_6 = 0.$

os passos admissiveis são dados pelo conjunto de transições independentes duas a duas, que no caso se restringe a,

$\{e_1, e_6\},\ \{e_2, e_5\},\ \{e_3, e_5\},\ \{e_4, e_6\},\ \{e_5, e_6\}$

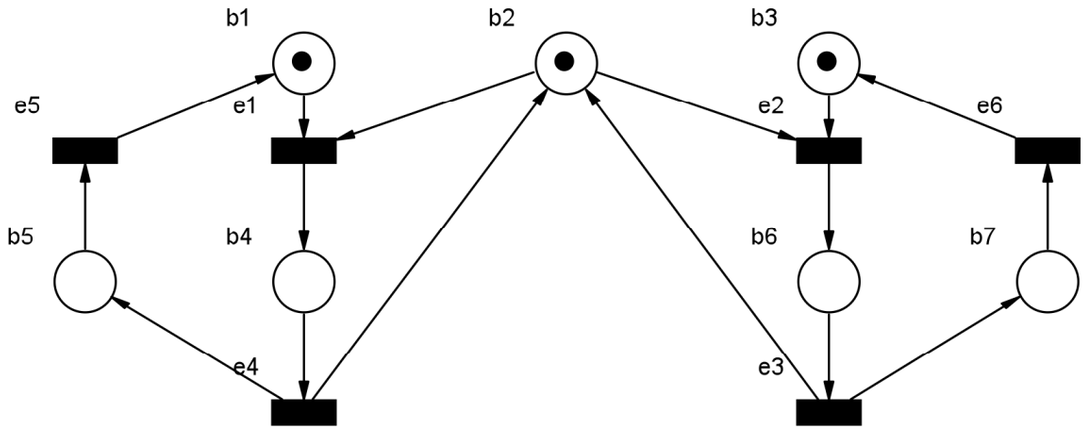


$e_1 \cdot e_2 = 1,\ e_1 \cdot e_3 = -1,\ e_1 \cdot e_4 = -2,\ e_1 \cdot e_5 = -1,\ e_1 \cdot e_6 = 0;$
$e_2 \cdot e_3 = -2,\ e_2 \cdot e_4 = -1,\ e_2 \cdot e_5 = 0,\ e_2 \cdot e_6 = -1;$
$e_3 \cdot e_4 = 1,\ e_3 \cdot e_5 = 0,\ e_3 \cdot e_6 = -1;$
$e_4 \cdot e_5 = -1,\ e_4 \cdot e_6 = 0;$
$e_5 \cdot e_6 = 0.$

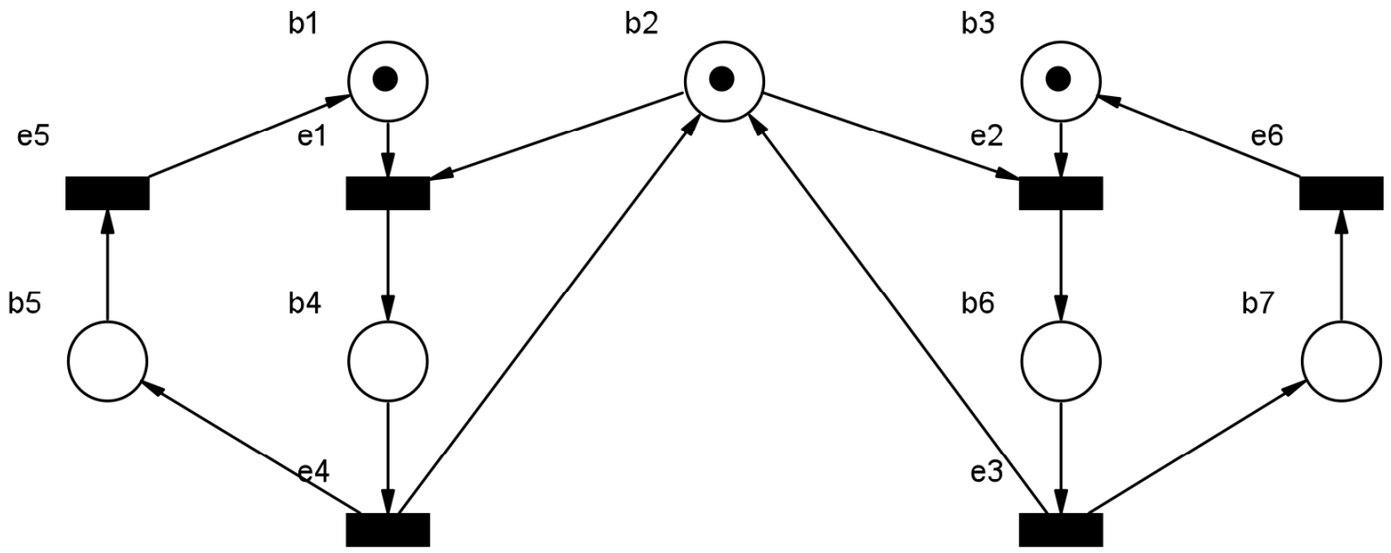
Se o produto escalar é nulo, isto é, se os vetores são ortogonais, então estes representam transições independentes. Se o produto escalar é negativo então as transições estão em contato, se for positivo então há um conflito.

A marcação M habilita somente os estados $\{e_1, e_2\}$ que não constituem um passo - ao contrario estão em conflito - portanto somente uma destas transições poderá ocorrer, digamos e_1, e o vetor de habilitação neste estado é o seguinte,

$$\sigma_M = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$



Como vimos na lista de exercícios 1, se admitirmos que ao invés do mutex fosse possível na rede acima disparar simultâneamente e_1 e e_2 teríamos a marcação $m^T = (\ 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \ 0)$, com b_4 e b_6 marcados. Esta certamente é uma marcação impossível (embora não tenhamos uma marcação negativa). Na verdade o mutex garante que sempre b_4 ou (exclusivo) b_6 está marcado, portanto $M(b_4) + M(b_6) \leq 1$, que é o que caracteriza o mutex.



Podemos verificar ainda que o passo $|e_1 e_4 e_5\rangle$ aplicado ao estado inicial reproduz este mesmo estado. Similarmete, o passo $|e_2 e_3 e_6\rangle$ também reproduz o estado inicial e temos portanto dois vetores invariantes (de transição):

.

$$i_1^T = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} \quad \text{e} \; i_2^T = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Redes P/T: Definição

Definition 16

Uma rede Place/Transition P/T, é uma n-upla, $N = (S, T; F, W, K, M_0)$, onde,

- S é um conjunto finito de lugares;
- T é um conjunto finito de trasições;
- $F = (S \times T) \cup (T \times S)$ representa as relações de fluxo (arcos);
- $W : F \rightarrow \mathbb{N}^+$ representando o peso, isto é, a quantidade de marcas que flui em cada arco;
- $K : S \rightarrow \mathbb{N}$ é um mapeamento que atribui a cada lugar uma capacidade máxima para o armazenamento de marcas.
- M_0 é a marcação inicial.

Redes Limitadas

Definition 17

Uma rede $N = (S, T; F, W, K, M_0)$ é dita k-limitada se existe um número inteiro positivo k tal que

.

$\forall s \in S, M(s) \leq k,$

.

onde

.

$M : S \rightarrow \mathbb{N}$ é a função de marcação da rede.

.

O inteiro k é também chamado capacidade máxima de S, ou $max[K(s)]$.

Condição de Habilitação

Definition 18

Seja uma rede $N = (S, T; F, W, K, M_0)$. Uma transição $t \in T$ é dita habilitada em uma marcação M se e somente se,
$\forall s \in \bullet t, M(s) \geq W(s,t) \wedge \forall s \in t\bullet, M(s) \leq K(s) - W(t,s)$.

A Def.18 é chamada de condição de disparo estrita, e é aplicada a redes k-limitadas, isto é, onde mas{K(s)] é finito.

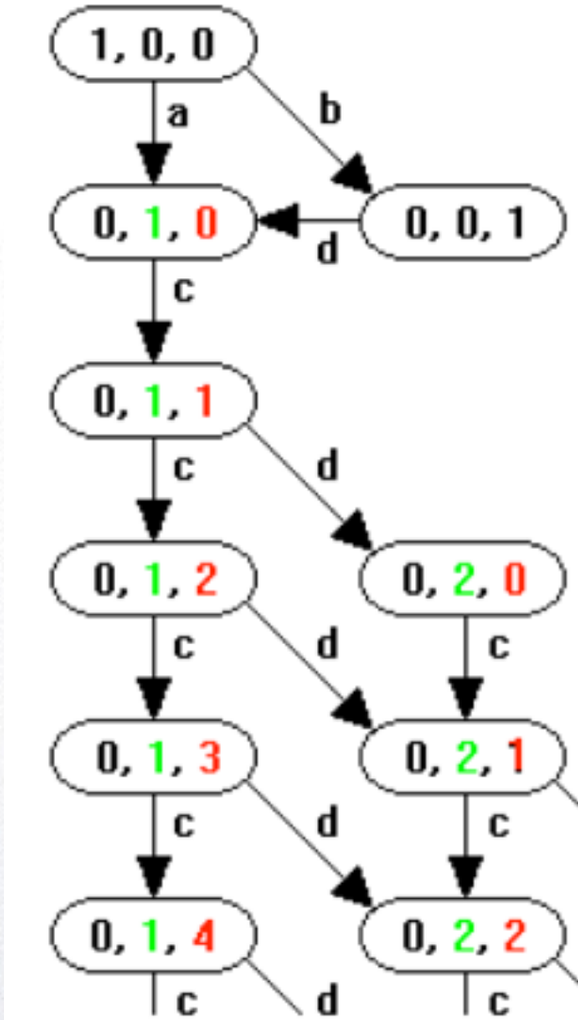
Redes Ilimitadas

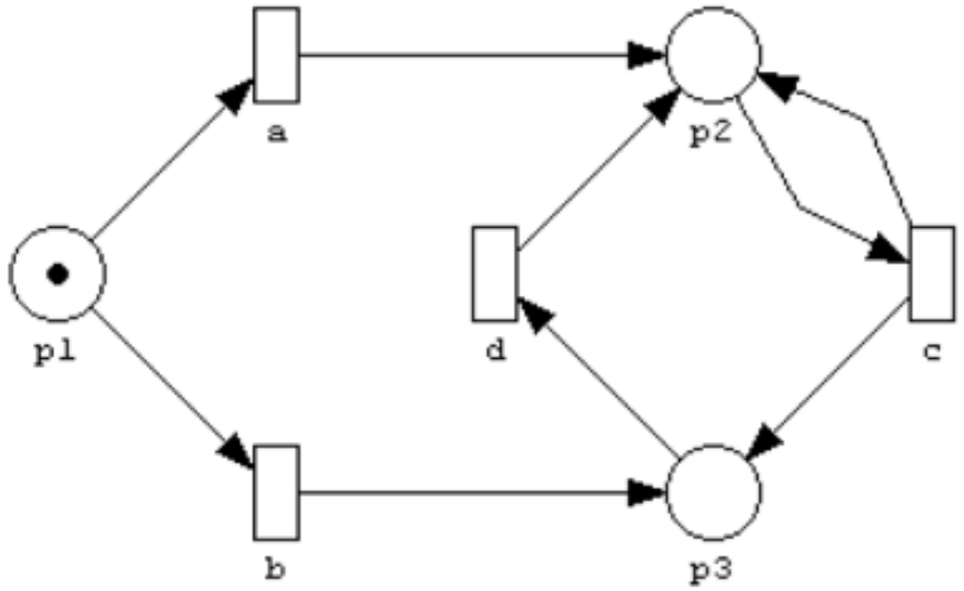
Definition 19

Uma rede $N = (S, T; F, W, K, M_0)$ é dita de capacidade infinita se e somente se,
$\exists s \in S | K(s) = w$, onde w é o inteiro ilimitado aleph-zero.

Uma rede de capacidade ilimitada tem também um grafo de atingibilidade infinito.

Exemplo





O grafo de atingibilidade à esquerda é infinito

Flexibilizando a regra de transição

Definition 21

Seja uma rede $N = (S, T; F, W, K, M_0)$, uma transição $t \in T$ é dita fracamente habilitada se e somente se
$\forall s \in \bullet t, M(s) \leq W(s, t)$.

Uma regra de transição fraca é sempre aplicável a uma rede de capacidade infinita.

Teorema 2

Seja uma rede P/T $< N, M_0 >$, onde se aplica a regra de transição estrita, e seja $< N', M'_0 >$ a sua rede dual, onde se aplica a regra de transição fraca. O grafo de atingibilidade destas duas redes são isomorfos.
Dem] (Lista de exercícios 2)

Portanto, para um ambiente de modelagem que trabalhe sempre com a rede dual não é preciso usar a regra de transição estrita.

Proposição 2] Para toda análise de rede Place/Transition é possível utilizar a regra de transição fraca, dado que toda rede de capacidade finita, onde se pode aplicar a regra de disparo estrita, é de fato equivalente à sua rede dual onde se pode aplicar a regra de transição fraca.

$$\mathbf{M}_{i+1} = \mathbf{M}_0 + \mathbf{A}^T \sum_{j=0}^{i} \sigma_j$$

Fazendo $\sum_{j=0}^{i} \sigma_j = \overline{\sigma}$, temos a equação não - homogênea,

$\mathrm{A}^{\mathrm{T}}\overline{\sigma} = \Delta M$. Se esta equação tiver solução não saberemos de fato se existe uma permutação de σ's que seja exequivel na prática, e que tornaria o estado de fato atingível. Entretanto, se a equação não tem solução, então o estado em questão NÃO é atingível. Temos assim uma condição necessária para a atingibilidade, obtida diretamente da equação de estado.

Árvore de Cobertura

Definition 22

Seja uma rede P/T $< N, M_0 >$, e seja uma marcação $M \in |M_0\rangle$. A marcação M é dita emcampável (coverable) se e somente se existir uma marcação $M' \in |M_0\rangle$ tal que $M' \geq M$, isto é,
$\forall s \in S, M'(s) \geq M(s)$.

Uma árvore de cobertura é uma estrutura que tem a marcação inicial como raiz e cada ramo representando os diferentes processos ou sequencia de disparos até encontrar um “dead end” ou uma marcação já visitada.

Algorítimo de Construção

1) Tome M_0 como raiz e rotule este estado como “new”

2) Enquanto existir uma marcação denotada por “new” faça
   2.1) Selecione uma nova marcação M (apontada por “new”);
   2.2) Se M for idêntica a alguma marcação já visitada, rotule esta marcação como “old” e procure uma nova marcação.
   2.3) Se nenhuma transição está habilitada então rotule M como um “final trap”;
   2.4) Enquanto existirem transições habilitadas em M, faça
      2.4.1) Obtenha a marcação resultante do firing de $t \in M^{\bullet}$;
      2.4.2) Se a nova marcação é superável substitua M´por *w*
      2.4.3) Faça um novo nó com M´, desenhe um arco com rótulo t de M para M´ e rotule M´ como “new”.

Redefinindo propriedades

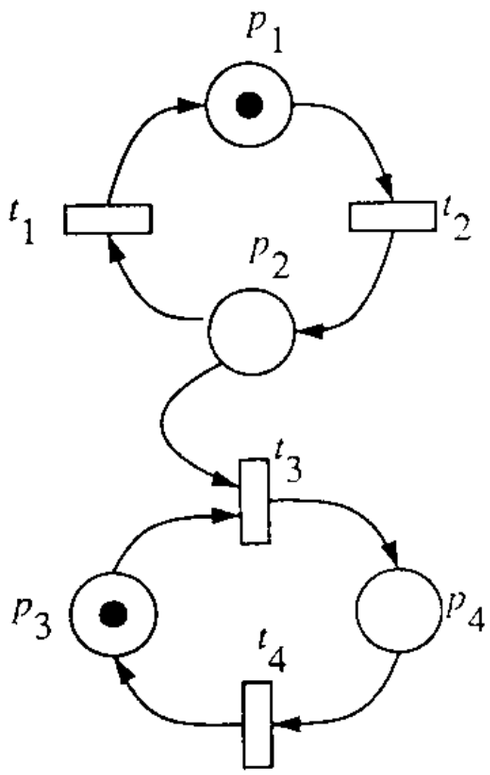
Para as redes de Petri clássicas, a análise de comportamento dos sistemas (discretos, distribuídos) é baseada em propriedades como:

Deadlock-freedon (ausência de deadlock) – a rede não atinge um deadlock total
Liveness (vivacidade) – a rede não atinge uma situação de deadlock parcial
Boundness (limitação) - nenhum lugar tem marcação monotonicamente crescente
Reversibility (reversibilidade) – o estado inicial é alcançável de qualquer marcação

Coverability Tree

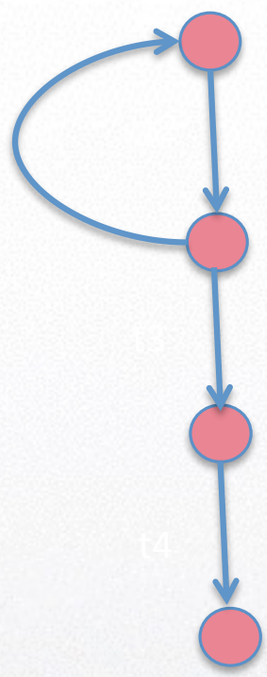
Exemplo de deadlock

Uma rede limitada



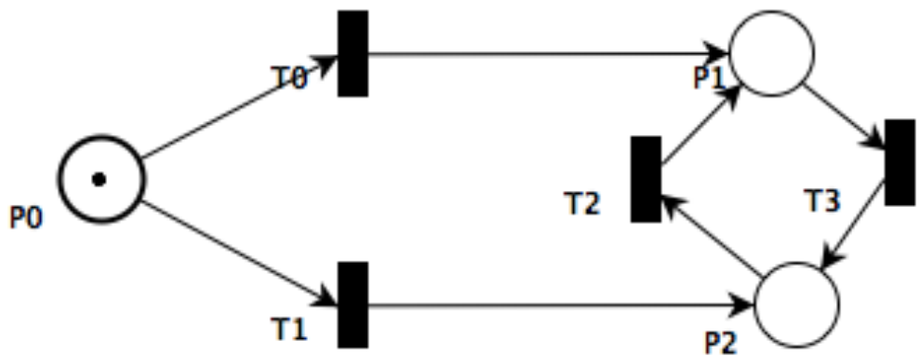
Murata, 1989, pag. 549

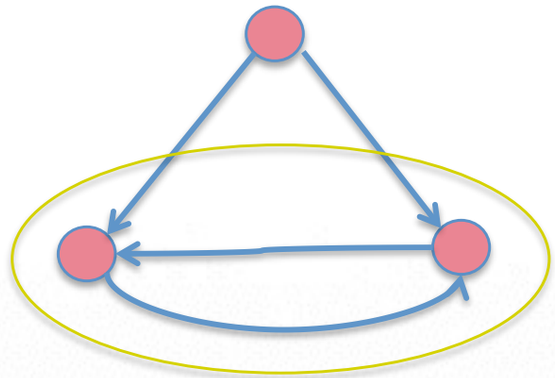
E seu grafo de atingibilidade



deadlock

Exemplo de Trap





Trap (armadilha)

Caminhos para modelagem

Possíveis estratégias :

- Classificação (fazer um estudo prévio de certas classes de rede e simplesmente identificar cada caso prático com uma das classes)

- Identificar propriedades “desejáveis” nas redes associadas a casos práticos, implicando que já existe uma associação destas propriedades com comportamento ou estrutura do sistema.

- Reproduzir a rede de cobertura e fazer a análise sobre esta rede

Propriedades das Redes de Petri

As propriedades comportamentais das redes de Petri são :

- atingibilidade (já discutida brevemente)
- limitação (já discutida)
- vivacidade
- reversibilidade
- cobertura (já discutida)
- persistência
- invariantes (já discutida)
- distância síncrona
- equacidade

Vivacidade

Definition 23

Seja uma rede P/T $< N, M_0 >$, e seja uma transição genérica $t \in T$. Seja $\ell(M_0)$ o conjunto de sequencias de disparo definidas sobre $|M_0\rangle$. A transição t é dita :

i) L-0 viva (morta), se t nunca é disparada em nenhuma sequencia de $\ell(M_0)$;

ii) L-1 viva, se t é disparada pelo menos uma vez em alguma sequencia de $\ell(M_0)$;

iii) L-2 viva, se, dado um inteiro positivo k, t é disparada k-vezes em alguma sequencia de $\ell(M_0)$;

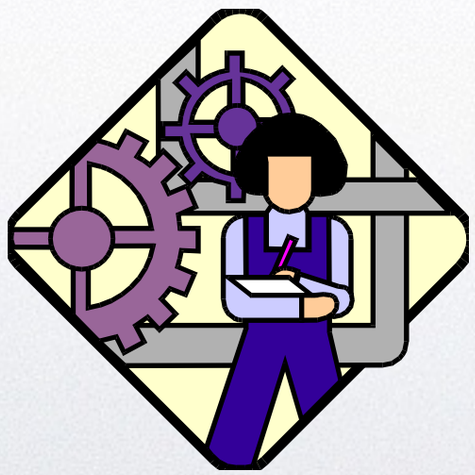
iv) L-3 viva, se t é disparada infinitas vezes em alguma sequencia de $\ell(M_0)$;

v) L-4 viva, se t é disparada pelo menos uma vez em todas as sequencias de $\ell(M_0)$.

Reversibilidade

Definition 24

Seja uma rede P/T $< N, M_0 >$, e seja uma transição genérica $t \in T$. Seja $|M_0\rangle$ o conjunto de todas as marcações atingíveis a partir de M_0 (ou forward case class de M_0). A rede é dita reversível se e somente se, para toda marcação $M \in |M_0\rangle$, M_0 é atingível a partir de M.



Ciclo de produção

Persistencia

Definition 25

Seja uma rede P/T $< N, M_0 >$, é dita persistente se e somente se, dadas duas transições genéricas da rede, o disparo de uma delas não desabilita a outra.

Persistência $\Leftrightarrow$ Livre de conflito

Equacidade

B–fairness

Definition 26

Seja uma rede P/T $< N, M_0 >$, duas transições genéricas desta rede podem ser ditas equânimes (B-fair) se e somente se o número de vezes que uma delas pode ocorrer sem que a outra ocorra é finito.
Uma rede é dita equânime (B-fair) se é equânime para todo par de transições $t_1, t_2 \in T$.

Corolário

Seja uma rede Place/Transition P/T,dadas duas transições genéricas desta rede são ditas infinitamente equânimes se uma delas pode ocorrer infinitas vezes sem que a outra ocorra.
Uma rede é dita infinitamente equânime se é infinitamente equânime para todo par de transições $t_1, t_2 \in T$.

Propriedades estruturais

São ditas propriedades estruturais das Redes de Petri, as propriedades que não dependem da marcação inicial mas somente da estrutura topológica da rede.

Vivacidade estrutural
Controlabilidade
Limitação estrutural
Conservabilidade
Consistência

Definition 27

Seja uma rede P/T $< N, M_0 >$, esta rede é estruturalmente viva se existe pelo menos uma marcação inicial para a qual a rede é viva (L-4 viva).

Definition 28

Seja uma rede P/T $< N, M_0 >$, esta rede é dita completamente controlável se e somente se qualquer marcação da rede for atingível a partir de uma marcação dada M, para todo M.

Teorema 3

Seja uma rede Place/Transition P/T com m lugares e n transições. Se esta rede é completamente controlável, então $Posto(A) = m$, onde A é a matriz de incidência da rede,

Dem} Se a rede é completamente controlável, existe um x tal que $A^T x = \Delta M$, dado que qualquer estado é atingível a partir de uma marcação dada M_0. Assim, $Posto(A) = Posto([A : \Delta M]) = Posto(A^T) = m$.

Definition 29

Seja uma rede P/T $< N, M_0 >$, esta rede é dita limitada estruturalmente se e somente se é k-limitada para qualquer marcação inicial escolhida.

Definition 30

Seja uma rede P/T $< N, M_0 >$, esta rede é dita parcialmente conservativa se e somente se existe um inteiro positivo y_s para alguns lugares, de modo que o vetor $y = [y_s]$, tal que $M(s)^T y = M_0^T(s) y = cte$.

Definition 31

Seja uma rede P/T $< N, M_0 >$, esta rede é dita (totalmente) conservativa se e somente se existe um inteiro positivo y_s para todo lugar s, de modo que o vetor $y = [y_s]$, é tal que $M(s)^T y = M_0^T(s) y = cte$.

Fica claro que se uma rede é parcialmente conservativa então existe um invariante de lugar com algumas posições nulas. Portanto, o invariante de lugar está diretamente ligado à propriedade da rede de conservar as marcas pelo menos em um sub-conjunto próprio de lugares (parcialmente conservativa).

Consistência

Definition 32

Seja uma rede P/T $< N, M_0 >$, esta rede é dita parcialmente/totalmente consistente se existe uma marcação M_0 e uma sequencia de disparos σ que leva ciclicamente a M_0 de modo de algumas/todas as transições ocorrem pelo menos uma vez em σ.

Aplicações estratégicas

Sistemas supervisórios inteligentes

$$m_1 \xrightarrow{t_1} m_2 \xrightarrow{t_2} \cdots \xrightarrow{t_k} m_k \quad \Rightarrow$$

$$\Rightarrow \; m_1 \xrightarrow{\sigma} m_k$$

$$\text{onde } \sigma = t_1 t_2 \cdots t_k$$

Teoria de Sistemas Supervisórios (TSS)

Os processos de um sistema discreto podem ser representados por strings de eventos ou passos. Tais strings formam uma suprema linguagem controlável e pode incluir eventos não controláveis, desde que observáveis e preditiveis.

O supervisório em malha fechada é um parser para esta suprema linguagem controlável.

Ramadge, P.J. and Wonham, W.M.; The Control of Discrete Event System, Proc. of the IEEE, Vol. 77, no. 1, 1989

Verificação de sistemas

- uma técnica de verificação é um algorítmo procedural que prova que uma dada propriedade vale em um caso específico;

- uma técnica de prova visa demonstrar a propriedade em um caso geral (em geral lida com métodos simbólicos, declarativos);

- uma técnica de análise agrupa um conjunto de propriedades de uma rede como sendo isomorfas às de um modelo ou artefato em fase de design (sistema em geral).

Usando Petri Nets para verificação

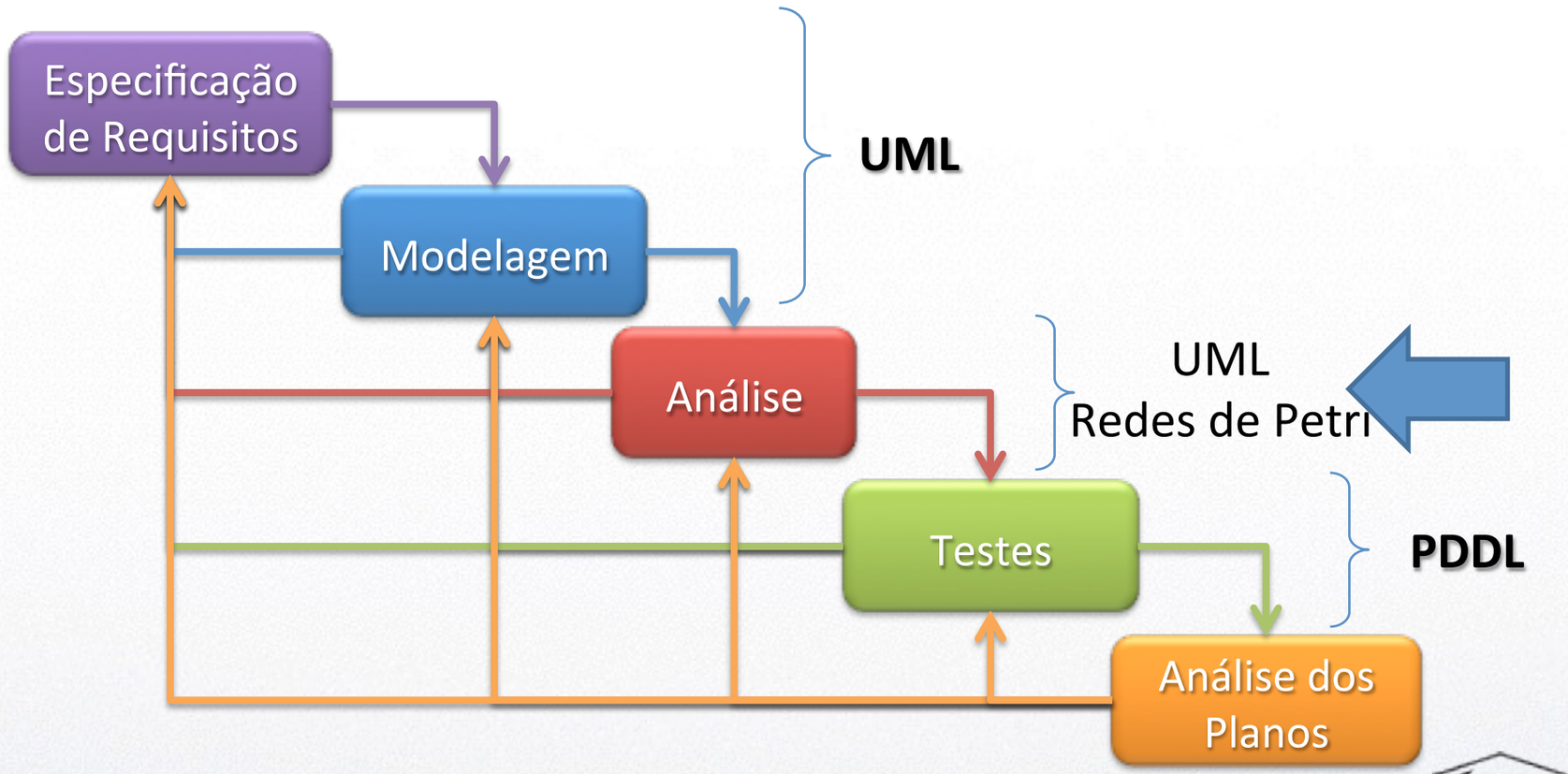
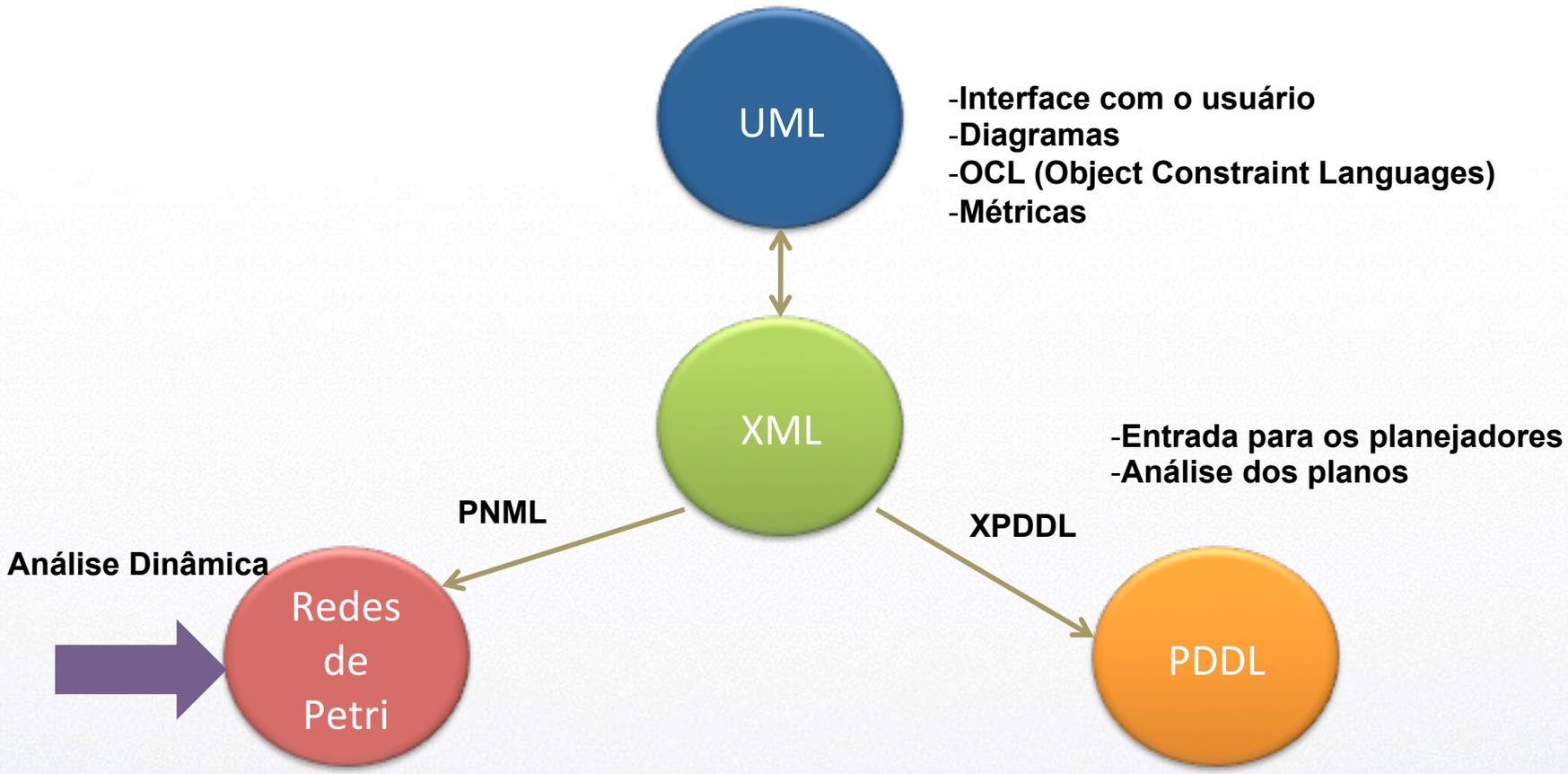


Figura retirada de (Vaquero et. al 2009)

O sistema itSIMPLE



A rede de Petri tem todos os elementos fundamentais à análise de sistemas?

Aplicações e extensões

Sistemas de telecomunicação

Redes de computadores

Sistemas de manufatura

Sistemas químicos de produção em batelada

Sistemas de transporte (inteligentes)

etc.

O projeto de padronização das Redes de Petri

IEC/ISO 15909

Parte 1 (2004): modelo semântico, definição teórica das redes clássicas e das redes de alto nível.

Parte 2 (2005-2008): definição do protocolo de importação/exportação, PNML.

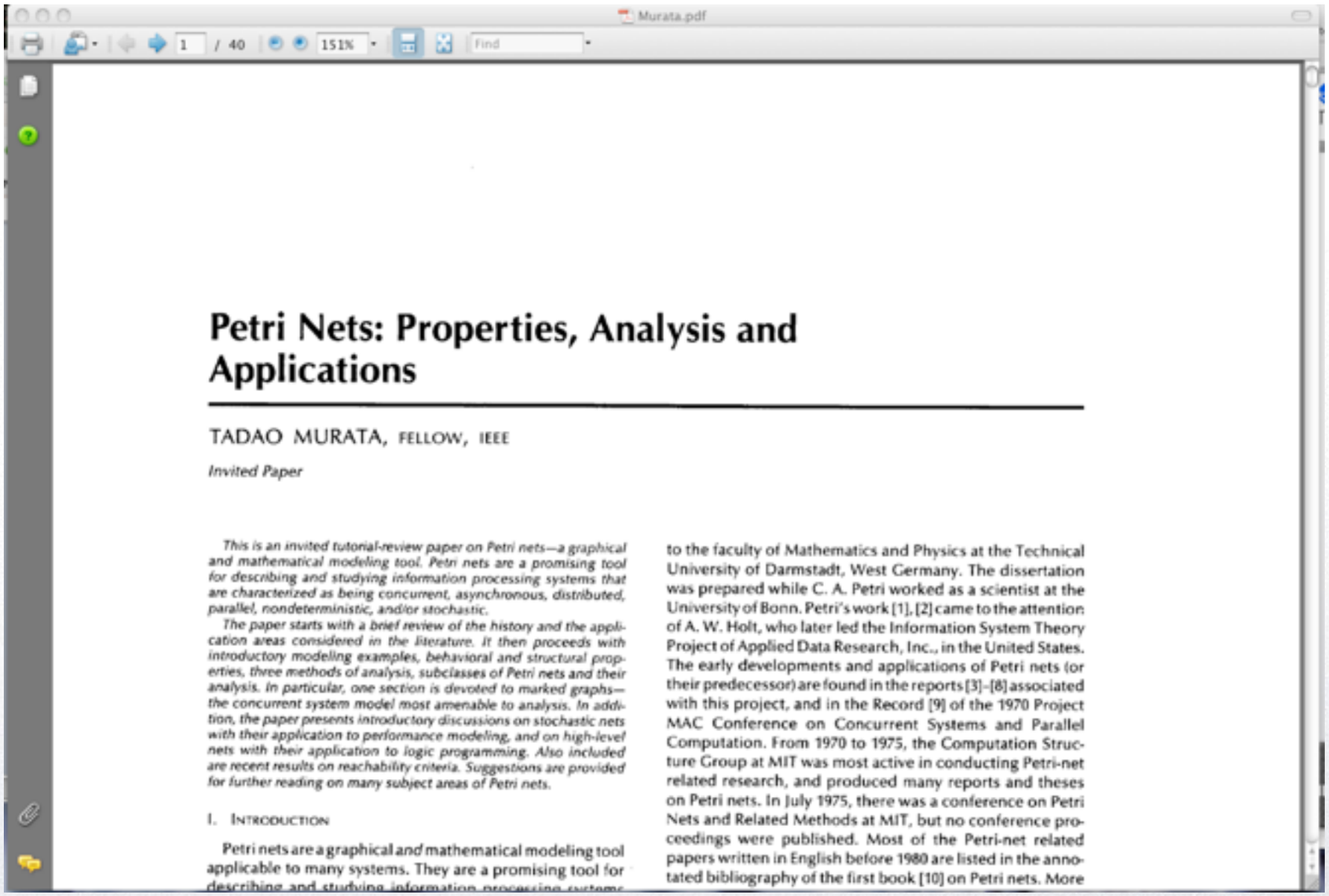
Parte 3 (?) : Extensões, Redes Temporizadas, modularidade, hierarquia.

Já está disponível a lista de exercícios 3 (no site) cujo upload deve ser feito até a próxima aula.

Todos devem tentar recuperar o atraso na definição do artigo e os que estão em dia devem avançar. A cada milestone todos deverão receber algum feedback sobre o trabalho e devem seguir as sugestões, primeiro dos respectivos orientadores, segundo do "revisor".

Leitura da Semana

Tadao Murata



Usando redes de Petri para análise de Use-Case

Verification of Use Case with Petri Nets in Requirement Analysis*

Jinqiang Zhao[1,2] and Zhenhua Duan[1,**]

[1] Institute of Computing Theory & Technology, Xidian University, Xi'an, 710071, P.R. China
[2] State Key Laboratory of Software Engineering, Wuhan University, 430072, P.R. China
jqzhao1985@gmail.com, zhenhua_duan@126.com

Abstract. Requirement analysis plays a very important role in reliability, cost, and safety of a software system. The use case approach remains the dominant approach during requirement elicitation in industry. Unfortunately, the use case approach suffers from several shortcomings, such as lacking accuracy and being difficult to analyze and validate the dynamic behavior of use cases for concurrency, consistency, etc. This paper proposes an approach for overcoming limitations of the use case approach and applies the approach in Model Driven Development (MDD). Timed and Controlled Petri Nets are used as the formal description and verification mechanism for the acquired requirements. Use cases are used to elicit the requirements and to construct scenarios. After specifying the scenarios, each of them can be transformed into its correspondent Petri-net model. Through analyzing these Petri-net models, some flaws or errors of requirements can be detected. The proposed approach is demonstrated by an E-mail client system.

Keywords: use case; Model Driven Development; Petri net; requirement analysis.

1 Introduction and Related Works

Software development usually consists of the following stages: requirement analysis, design, code and testing. Many research studies have shown the considerable influence of early requirement analysis on the reduction of the unnecessary costs, confusion and complexity in the later phases of software development [1].

Therefore, high quality of requirement analysis can most likely reduce some potential risk occurred in later phases of software development.

* This research is supported by the NSFC Grant No. 60433010, NSFC Grant No. 60873018 jointly sponsored by Microsoft Asia Research Academy, Defence Pre-Research Project of China No. 51315050105, SRFDP Grant 200807010012 and SKLSE20080713.
** Corresponding author.

O. Gervasi et al. (Eds.): ICCSA 2009, Part II, LNCS 5593, pp. 29–42, 2009.

Fim