

# Le problème de la vérification : des systèmes à événements discrets aux systèmes hybrides

Robert Valette

LAAS-CNRS, F-31077 Toulouse Cedex 4  
France

Reims 25 Novembre 2005

# Plan de l'exposé

- 1 **Épigraphe**
- 2 Introduction
- 3 Modélisation
- 4 Vérification
- 5 Aspect logique et notion de scénario
- 6 Conclusion



Caminante, no hay camino,  
Se hace camino al andar

Antonio Machado Ruiz (Sevilla 1875, Colliure 1939)

Caminante, no hay camino,  
Se hace camino al andar

Pèlerin, il n'y a pas de chemin,  
C'est en marchant que l'on fait le chemin

Discurso del académico Excmo Sr. Manuel Silva Suárez  
De la ingeniería y de los sistemas de eventos discretos  
14 de noviembre de 2000



Devia ser proibido debochar  
de quem se aventura em língua estrangeira

Francisco Buarque de Hollanda (Chico)  
dans le roman  
*Budapeste*

Il devrait être interdit de se gausser  
de celui qui s'aventure en langue étrangère

Emplearé como hilo conductor la lengua y su tesoro

J'utiliserai comme fil conducteur la langue et son trésor

Discurso del académico Excmo Sr. Manuel Silva Suárez  
De la ingeniería y de los sistemas de eventos discretos  
14 de noviembre de 2000

# Plan de l'exposé

- 1 Épigraphe
- 2 **Introduction**
- 3 Modélisation
- 4 Vérification
- 5 Aspect logique et notion de scénario
- 6 Conclusion

# Introduction 1

- Le problème de la vérification des systèmes à événements discrets et des systèmes hybrides.
  - Qu'est-ce que la vérification ?
  - Qui conçoit ces systèmes et qui vérifie ?
- 
- La vérification est une **technique** utilisée par des **ingénieurs**.
  - Commençons donc notre réflexion par le commencement : qu'est ce qu'un ingénieur et qu'est ce qu'une technique ?

## Ingénieur ?

Ingeniero deriva de ingenio (lat. ingenium). Ello lleva a genio (lat. genius), que proviene de gignere (gigno, genui, genitum), engendrar, dar a luz ; crear, producir, causar.

Manuel Silva : De la ingeniería y de los sistemas de eventos discretos

engendrar : engendrer

dar a luz : donner le jour

crear : créer

producir : produire

causar : causer

La actividad del ingeniero se articula a través

- de su intuición
- de sus conocimientos profundos - científicos,
- de su experiencia,
- de su arte

Un ingénieur ne fonde pas uniquement son activité sur la science, sur un **langage scientifique formel**, c'est également un **créateur**.

## Technique ?

Técnica deriva del griego téchne : arte

On retrouve le mot **art** avec **artiste** et **artisan**.

L'idée de création est encore présente.

Mediante la técnica la Humanidad ha creado una sobrenaturaleza, un paisaje artificial

Par l'intermédiaire de la technique, l'humanité a créé une sur-nature, un paysage artificiel.

## Technique ?

Técnica deriva del griego téchne : arte

On retrouve le mot **art** avec **artiste** et **artisan**.

L'idée de création est encore présente.

Mediante la técnica la Humanidad ha creado una sobrenaturaleza, un paisaje artificial

Par l'intermédiaire de la technique, l'humanité a créé une sur-nature, un paysage artificiel.

Pour analyser :

Le problème de la vérification :  
des systèmes à événements discrets  
aux systèmes hybrides

Il faut donc à la fois s'appuyer sur un **langage** scientifique et sur tout ce qui peut aider le processus **créatif**.

Ce n'est pas facile, c'est contradictoire : formel X 1/2 formel

Devia ser proibido debochar de quem se aventura em língua estrangeira

Pour analyser :

Le problème de la vérification :  
des systèmes à événements discrets  
aux systèmes hybrides

Il faut donc à la fois s'appuyer sur un **langage** scientifique et sur tout ce  
qui peut aider le processus **créatif**.

Ce n'est pas facile, c'est contradictoire : formel X 1/2 formel

Devia ser proibido debochar de quem se aventura em língua  
estrangeira

Pour analyser :

Le problème de la vérification :  
des systèmes à événements discrets  
aux systèmes hybrides

Il faut donc à la fois s'appuyer sur un **langage** scientifique et sur tout ce qui peut aider le processus **créatif**.

Ce n'est pas facile, c'est contradictoire : formel X 1/2 formel

Devia ser proibido debochar de quem se aventura em língua estrangeira

Pour analyser :

Le problème de la vérification :  
des systèmes à événements discrets  
aux systèmes hybrides

Il faut donc à la fois s'appuyer sur un **langage** scientifique et sur tout ce  
qui peut aider le processus **créatif**.

Ce n'est pas facile, c'est contradictoire : formel X 1/2 formel

Devia ser proibido debochar de quem se aventura em língua  
estrangeira

# Plan de l'exposé

- 1 Épigraphes
- 2 Introduction
- 3 **Modélisation**
- 4 Vérification
- 5 Aspect logique et notion de scénario
- 6 Conclusion

## Modélisation des systèmes hybrides :

Quels langages formels utiliser ?

Sur quels domaines scientifiques fonder sa démarche ?

Optimiste : créer une nouvelle langue

Étudier les relations entre les langages adaptés aux systèmes à événements discrets et ceux adaptés aux systèmes continus

Pessimiste : polyglotte

Avoir un formalisme séparé pour chaque aspect et passer de l'un à l'autre au gré des besoins

## Modélisation des systèmes hybrides :

Quels langages formels utiliser ?

Sur quels domaines scientifiques fonder sa démarche ?

## Optimiste : créer une nouvelle langue

Étudier les relations entre les langages adaptés aux systèmes à événements discrets et ceux adaptés aux systèmes continus

## Pessimiste : polyglotte

Avoir un formalisme séparé pour chaque aspect et passer de l'un à l'autre au gré des besoins

## Modélisation des systèmes hybrides :

Quels langages formels utiliser ?

Sur quels domaines scientifiques fonder sa démarche ?

## Optimiste : créer une nouvelle langue

Étudier les relations entre les langages adaptés aux systèmes à événements discrets et ceux adaptés aux systèmes continus

## Pessimiste : polyglotte

Avoir un formalisme séparé pour chaque aspect et passer de l'un à l'autre au gré des besoins

## Mais

- Pour favoriser la créativité il faut plus qu'un **langage** formel défini par un lexique et une grammaire
- Une **langue** c'est plus que cela
- Pour l'ingénieur il faut des méthodes, des approches permettant de raisonner.

Le formalisme adapté au discret et au continu doit être plus qu'un langage formel. Il doit venir avec une panoplie d'outils et de méthodes permettant non seulement de décrire, mais également de **raisonner** pour **créer** et **innover**.

La caricature de la vérification de modèle :

- Une logique pour **décrire** la propriété
- Un langage formel pour **décrire** le système de façon à pouvoir générer tous ses états
- L'outil informatique presse bouton qui vérifie par énumération

La caricature de UML

- Que chacun amène ses méthodes et langages adaptés à chaque métier
- Avec les concepts d'objet, de relation entre objets et la possibilité de travailler avec diverses vues ; on arrivera bien à tout **unifier**.

Pourquoi cela marche ? :

- Il faut construire une **abstraction** du système et de la propriété pour pouvoir vérifier effectivement
- Il faut réussir effectivement à construire les diverses vues UML (les divers types de diagramme)

Il y a un travail préalable d'**abstraction**, de **modélisation** et d'**interaction** entre des points de vue.

Choisir les langages les plus riches et les plus adaptés au raisonnement pour décrire les aspects discrets et continus des systèmes hybrides

Pourquoi cela marche ? :

- Il faut construire une **abstraction** du système et de la propriété pour pouvoir vérifier effectivement
- Il faut réussir effectivement à construire les diverses vues UML (les divers types de diagramme)

Il y a un travail préalable d'**abstraction**, de **modélisation** et d'**interaction** entre des points de vue.

Choisir les langages les plus riches et les plus adaptés au raisonnement pour décrire les aspects discrets et continus des systèmes hybrides

## Et les objets représentés ?

### → Le continu :

- il représente le plus souvent des lois de la physique ou au moins leur expression au sein de systèmes artificiels

### → Le discret :

- il représente un monde artificiel construit par les ingénieurs.
- ou bien une abstraction du monde physique

Mediante la técnica la Humanidad ha creado una sobrenaturaleza, un paisaje artificial

Interaction entre nature et "sur-nature" est une caractéristique de bien des systèmes hybrides

## Et les objets représentés ?

→ Le continu :

- il représente le plus souvent des lois de la physique ou au moins leur expression au sein de systèmes artificiels

→ Le discret :

- il représente un monde artificiel construit par les ingénieurs.
- ou bien une abstraction du monde physique

Mediante la técnica la Humanidad ha creado una sobrenaturaleza, un paisaje artificial

Interaction entre nature et "sur-nature" est une caractéristique de bien des systèmes hybrides

- ➔ Ne pas discrétiser le continu
  - On perd l'**explication** de la valeur d'une variable à  $t + \Delta t$  en connaissant sa valeur et celle de sa dérivée à  $t$

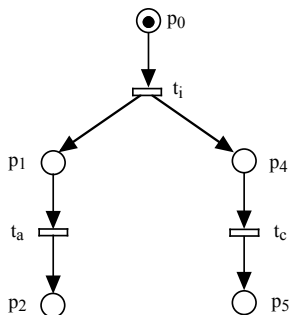
### Systemes d'équations algébro-différentielles

- ➔ Préserver l'ordre partiel entre les événements
  - L'événement  $e_1$  précède  $e_2$  doit pouvoir être interprété comme  $e_1$  est la **cause** de  $e_2$  et non la simple conséquence de la valeur numérique de certaines durées.

### Réseaux de Petri et parallélisme vrai plutôt qu'automates

## Réseaux de Petri Prédicats Transitions Différentiels

Travail avec  
les collègues et les doctorants du LAAS-CNRS et du LGP-CNRS  
et la communauté nationale (RdP+SDH) et le Brésil (USP)  
sans oublier l'Université de Saragosse



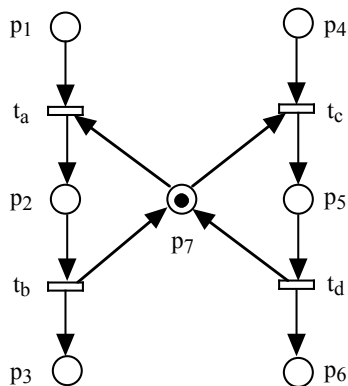
$$F(p_1) : dV/dt = f_1(V, \dots)$$

$$G(t_a) : \text{Si } V = K_{30}$$

# Plan de l'exposé

- 1 Épigraphe
- 2 Introduction
- 3 Modélisation
- 4 **Vérification**
- 5 Aspect logique et notion de scénario
- 6 Conclusion

# Vérification : Propriété / événements discrets



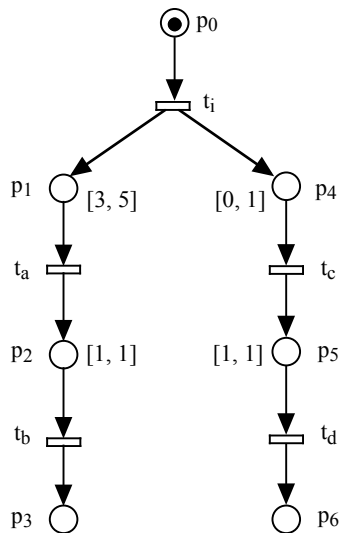
Quelles que soient les dynamiques continues associées aux places et les seuils associés aux transitions

$$M(p_2) + M(p_5) + M(p_7) = 1 \text{ et}$$

$$M(p_2) + M(p_5) \leq 1 \text{ et}$$

$p_2 \otimes p_5$  est inaccessible

# Vérification : Propriété temporelle 1



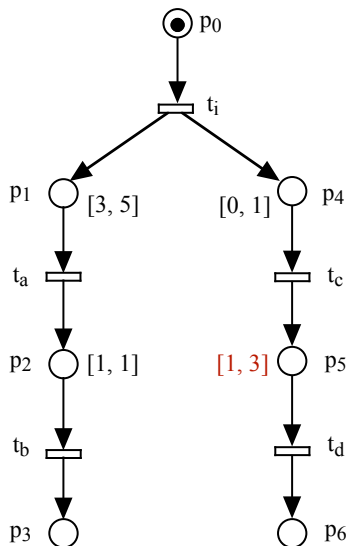
## Abstraction temporelle numérique

Si les dynamiques continues associées aux places et les seuils associés aux transitions sont cohérents avec les contraintes temporelles

$t_d$  est franchie au plus tard à la date 2

$t_a$  est franchie au plus tôt à la date 3

$p_2 \otimes p_5$  est inaccessible



## Abstraction temporelle numérique

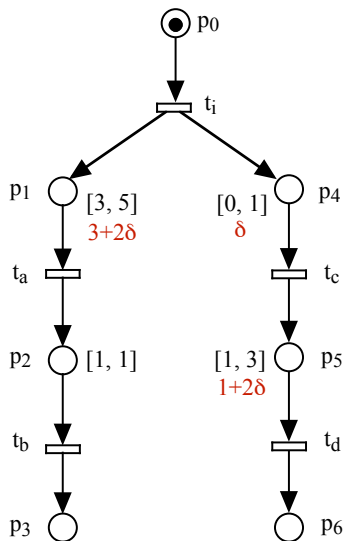
Avec ces nouveaux domaines pour les durées opératoires

$t_d$  est franchie au plus tard à la date 4

$t_a$  est franchie au plus tôt à la date 3

$p_2 \otimes p_5$  est accessible

On ne peut pas montrer la propriété



## Abstraction temporelle symbolique

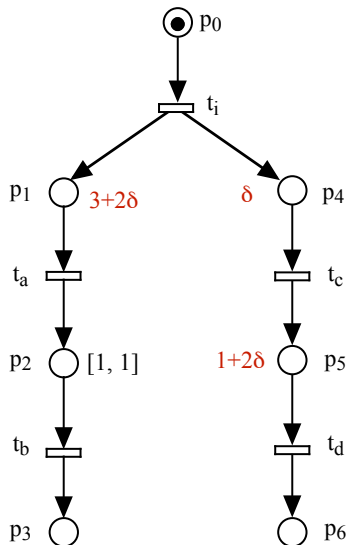
Les variations des durées opératoires ne sont pas indépendantes

$t_d$  est franchie à la date  $1 + 3.\delta$

$t_a$  est franchie à la date  $3 + 2.\delta$

$p_2 \otimes p_5$  est inaccessible pour  $\delta \in [0, 1]$

**Remarque :** l'abstraction temporelle numérique est la même que précédemment



## Abstraction temporelle symbolique

$t_d$  est franchie à la date  $1 + 3.\delta$

$t_a$  est franchie à la date  $3 + 2.\delta$

$p_2 \otimes p_5$  est inaccessible

si  $1 + 3.\delta < 3 + 2.\delta$

Soit  $\delta < 2$   $\delta \in [0, 2)$

On ne se contente pas de vérifier si la propriété est vraie où non, on donne le domaine du paramètre qui permet de prouver la propriété.

On ne vérifie pas la propriété pour un jeu de valeurs

On donne le domaine du paramètre qui permet de **prouver** la propriété

Ce n'est plus automatique ?

Caminante, no hay camino,  
Se hace camino al andar

Pèlerin, il n'y a pas de chemin,  
C'est en marchant que l'on fait le chemin

## Vérification : Propriété hybride 4

Les relations de **causalité** entre certaines propriétés et certains domaines de paramètres critiques me semblent essentiels pour favoriser l'aspect **conception** et **création** qui est, peut être, mal pris en compte par les méthodes formelles classiques qui privilégient l'aspect **scientifique** du travail de l'ingénieur dans le domaine de l'informatique industrielle (systèmes embarqués).

La actividad del ingeniero se articula a través

- de su intuición
- de sus conocimientos profundos - científicos,
- de su experiencia,
- de su arte

# Plan de l'exposé

- 1 Épigraphe
- 2 Introduction
- 3 Modélisation
- 4 Vérification
- 5 Aspect logique et notion de scénario
- 6 Conclusion

# Scénario : Logique linéaire 1

La démarche que nous avons prôné pour la vérification de propriété dans les systèmes hybrides est en fait une démarche de **preuve** fondée sur l'analyse des relations de **causalité** entre les événements

Elle n'est possible que parce qu'il existe une logique adéquate

La logique linéaire de J.Y. Girard

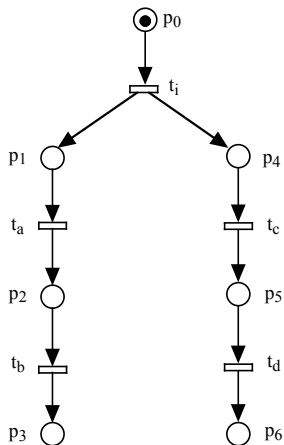
Équivalence entre accessibilité dans un réseau de Petri et preuve de certains séquents de Logique linéaire

Extraire les relations de causalité/précédence de l'arbre de preuve et non chercher à les décrire

Travail avec  
les collègues et les doctorants du LAAS-CNRS

- ➔ L'ordre partiel est conservé mais
  - il **n'est pas** dans le séquent (la formulation logique de l'accessibilité)
  - il **est** dans la preuve du séquent.

# Scénario : Logique linéaire 3



Nous avons associé :

- scénario dans un réseau de Petri = ens. tirs et ordre partiel
- séquent de logique linéaire à prouver

Un scénario encapsule beaucoup de séquences :

A gauche : un scénario

Mais six séquences

abcd, acbd, acdb, cadb, cabd, cdab

## Scénario : Logique linéaire 4

À partir d'un scénario, dans un système temporisé on obtient :  
un ensemble de contraintes temporelles simple (STN)

C'est un système linéaire (max,+)

Étudier un système scénario par scénario est similaire à étudier un  
système non linéaire par des linéarisations par morceaux

Le plus important est sans doute la meilleure **compréhension** du  
système à travers les relations de causalité entre les événements.

Favorise la réactivité/créativité de l'ingénieur lors du processus de  
conception

# Scénario : Logique linéaire 4

À partir d'un scénario, dans un système temporisé on obtient :  
un ensemble de contraintes temporelles simple (STN)

C'est un système linéaire (max,+)

Étudier un système scénario par scénario est similaire à étudier un  
système non linéaire par des linéarisations par morceaux

Le plus important est sans doute la meilleure **compréhension** du  
système à travers les relations de causalité entre les événements.

Favorise la réactivité/créativité de l'ingénieur lors du processus de  
conception

# Scénario : Règles de réduction 1

Dans ce cadre général :

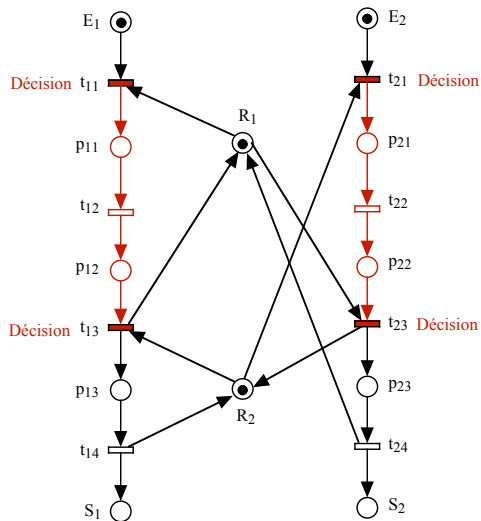
➔ Un travail commun avec Manuel Silva à l'occasion de la thèse de Juan Carlos Mugarza

La **règle de réduction** des réseaux de Petri consistant à fusionner deux transitions liées par une place peut être vue comme une déduction concernant une causalité **nécessaire** entre des événements.

Toute résolution de conflit en contradiction avec cette causalité doit être évitée :

- elle peut mener à un blocage mortel
- ou simplement à un comportement non désiré

# Scénario : Règles de réduction 2



Les décisions associées aux transitions  $t_{11}$  et  $t_{13}$  ( $t_{21}$  et  $t_{23}$  resp.) sont logiquement liées

➔ On évite le blocage mortel  $p_{12} \otimes p_{22}$  obtenu par  $t_{11}; t_{21}; t_{12}; t_{22}$

# Plan de l'exposé

- 1 Épigraphe
- 2 Introduction
- 3 Modélisation
- 4 Vérification
- 5 Aspect logique et notion de scénario
- 6 **Conclusion**

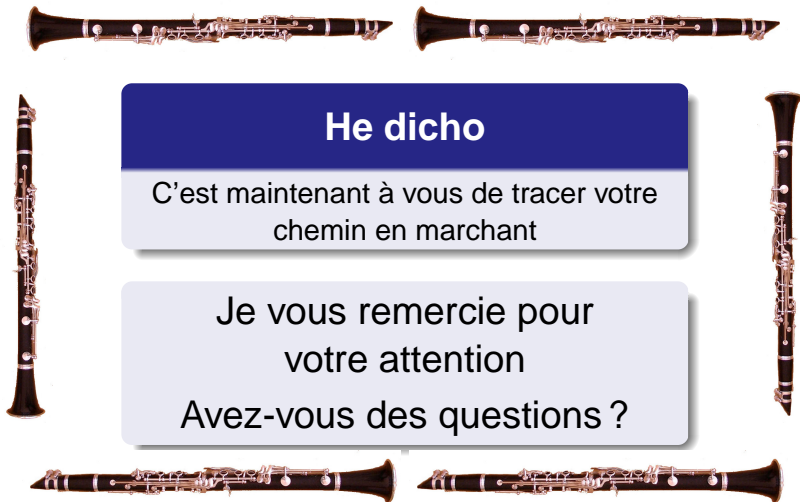
Faut-il conclure aujourd'hui ?

Je ne le pense pas.

➔ Une simple remarque pour illustrer la richesse du livre de Manuel Silva

De la ingeniería y de los sistemas de eventos discretos :

Bien que mon chemin en tant que chercheur ait été différent du sien, son livre a été un révélateur puissant qui m'a aidé à prendre conscience de mon cheminement.



## He dicho

C'est maintenant à vous de tracer votre chemin en marchant

Je vous remercie pour  
votre attention

Avez-vous des questions ?