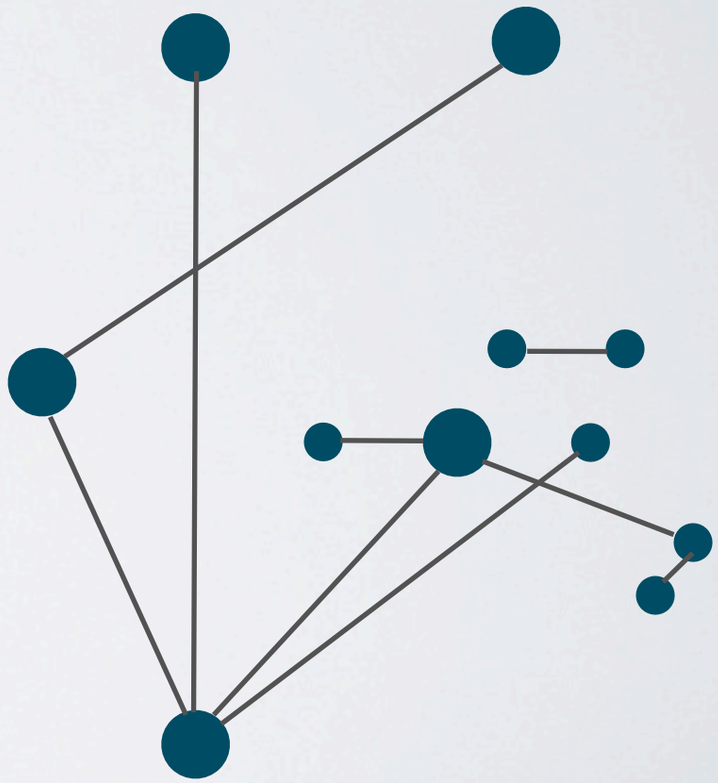
LaBRI

# MÉTHODES FORMELLES

2009-2014

Anca Muscholl, 15/01/15

cnrs université de BORDEAUX Bordeaux INP AQUITAINE



# Méthodes Formelles

# DOMAINES DE RECHERCHE

Vérification

Automates

Logique

Systèmes infinis

Algèbre

Programmes

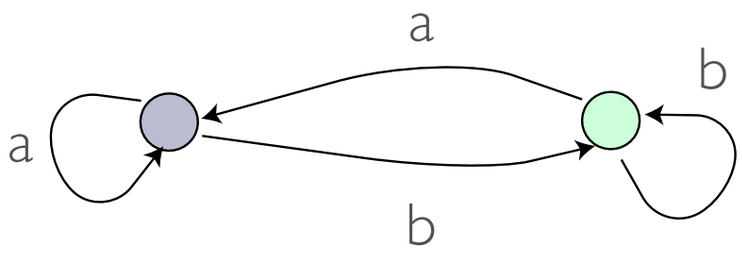
Jeux

Graphes

# Exemple 1: Logique et mots

abbaab

# Comment décrire des langages de mots:




Automates

$\forall x.\ (a(x) \Rightarrow \exists y{>}x.\ b(y))$

Chaque *a* est suivi par *un b*.

Logique du premier ordre (FOL)

Question 1:
Quand est-ce que le langage d'un automate peut être décrit en FOL ?

Question:
Est-ce qu'on peut décrire (ab)* ou (aa)* en FOL ?

Question 1:
Quand est-ce que le langage d'un automate peut être décrit en FOL ?

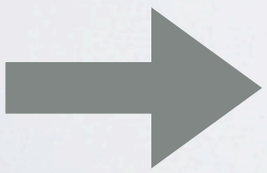
**Thm** [Schützenberger'65]:
Réponse donnée par l'algèbre :
semigroupe associé au langage.

Question 2 : Quelle est la formule la plus "simple" pour décrire un langage en FOL ?

Quelle est la formule la plus “simple” pour décrire un langage en FOL ?

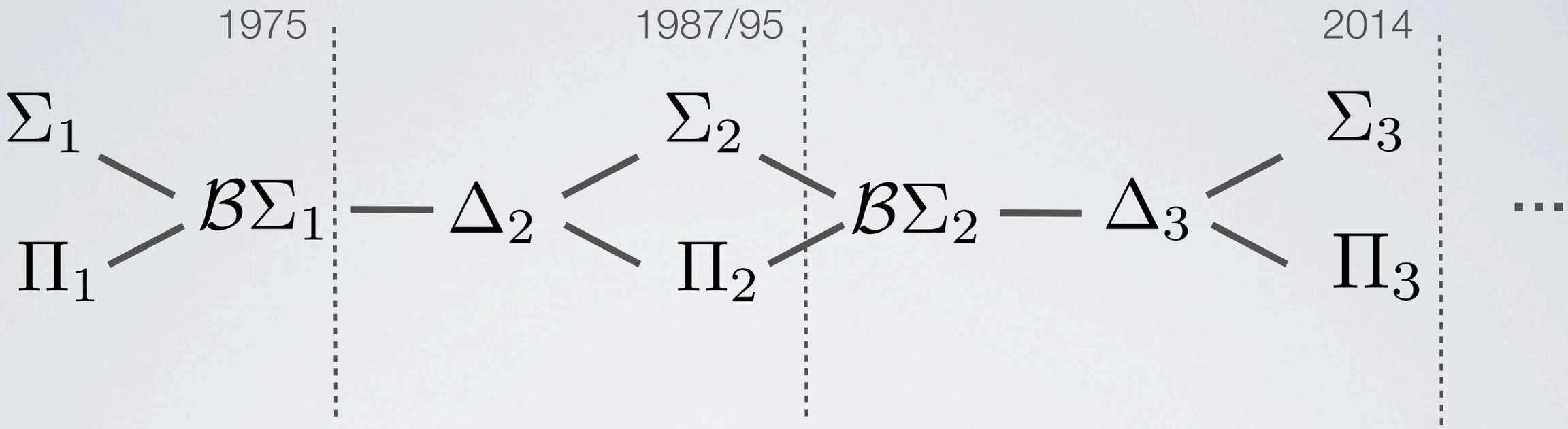
“Simple”:  nombre d’alternances des quantificateurs ∀ et ∃

Exemple:  Une alternance pour ∀x. (a(x) ⇒ ∃y>x. b(y))



Hiérarchie à l’intérieur de FOL

# Hiérarchie des quantificateurs dans FOL




Question 2: décider les niveaux de cette hiérarchie.

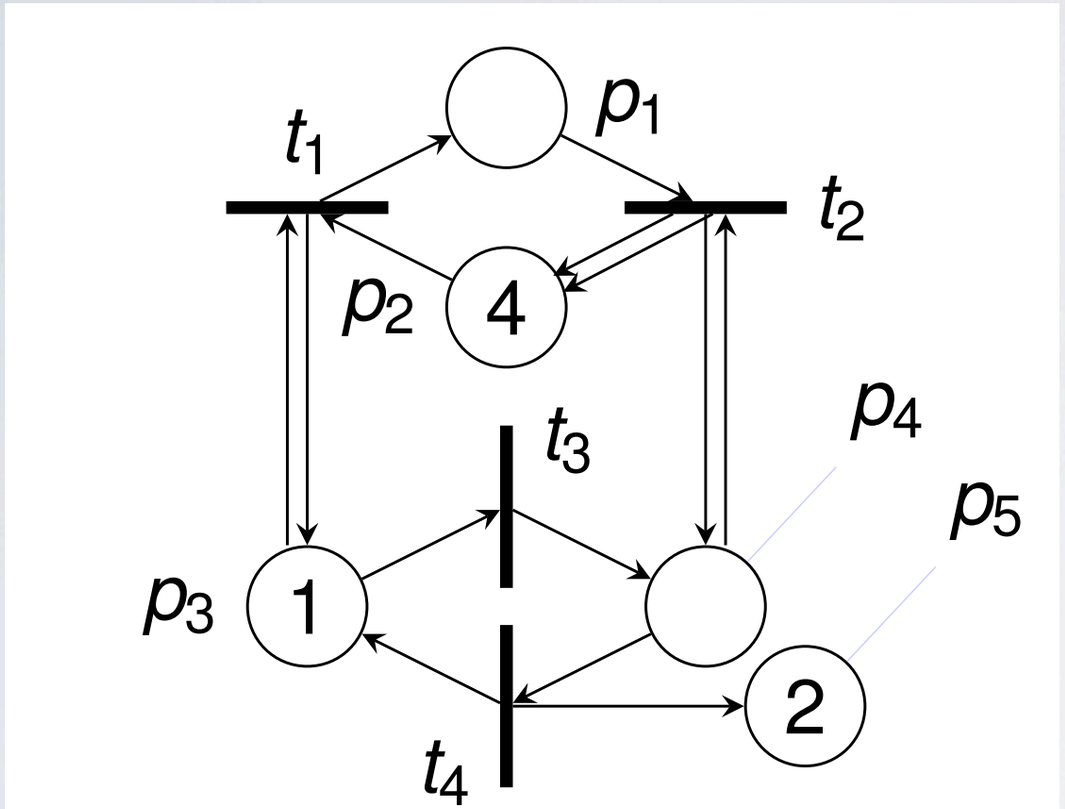
Résultat:

Décidabilité pour les niveaux $\mathcal{B}\Sigma_2\,,\ \Delta_3, \Sigma_3\,.$

# Exemple 2: Réseaux de Petri

1,2,3,...

# Vector Addition Systems (VAS)




| | | | |
|---|---|---|---|
| 0 | | | n-2 |
| 1 | | | $2^{n-3}$ |
| 1 | ✳ | | 0 |
| 0 | | | 1 |
| 0 | | | n |

?

Question :
Peut-on accéder à une configuration donnée ?

Problème de l'accessibilité dans les réseaux de Petri.

Problème de l'accessibilité dans les réseaux de Petri:

E.W. Mayr, R. Kosaraju 81/82: algorithme non primitif-récursif.

Question : arriver à une meilleure compréhension.

Résultat:
Première description structurelle des ensembles des configurations accessibles.

La non-accessibilité peut être attestée par un invariant dans la logique de Presburger FO(Nat,+).

# Vérification d’ordre supérieur

Sylvain Salvati

# PROPRIÉTÉS DE PROGRAMMES

## Propriétés comportementales

le service est toujours disponible
toute requête est traitée
etc...

## Propriétés de sûreté

bornes de vecteurs
division par 0
etc...

# PROPRIÉTÉS DE PROGRAMMES

## Propriétés comportementales

propriétés infinitaires

### Propriétés de sûreté

accessibilité

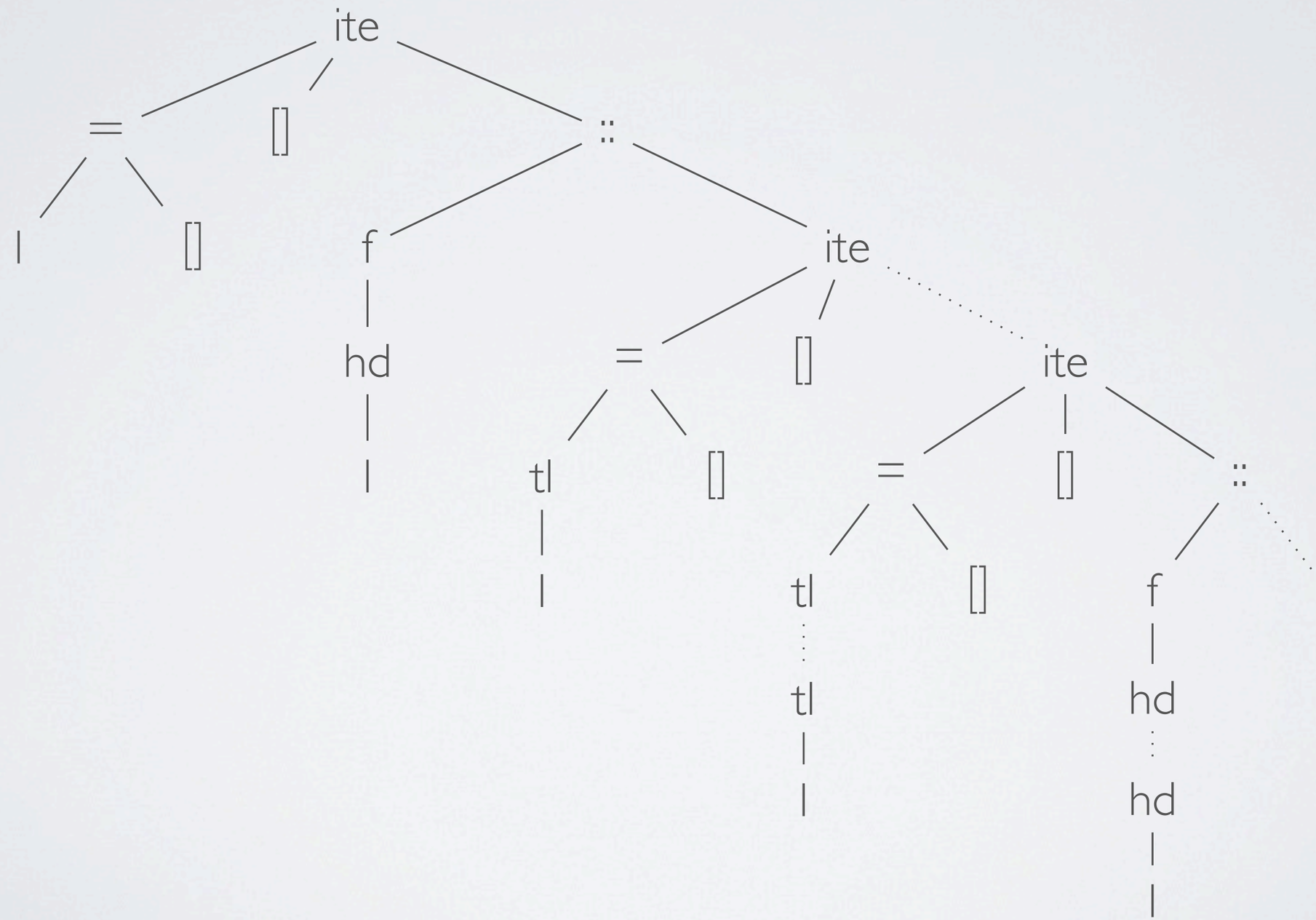
# ABSTRACTIONS FINIES

Accessibilité → Automates d'états finis

Propriétés infinitaires → Automates de parité
Logique monadique
du second ordre (MSO)

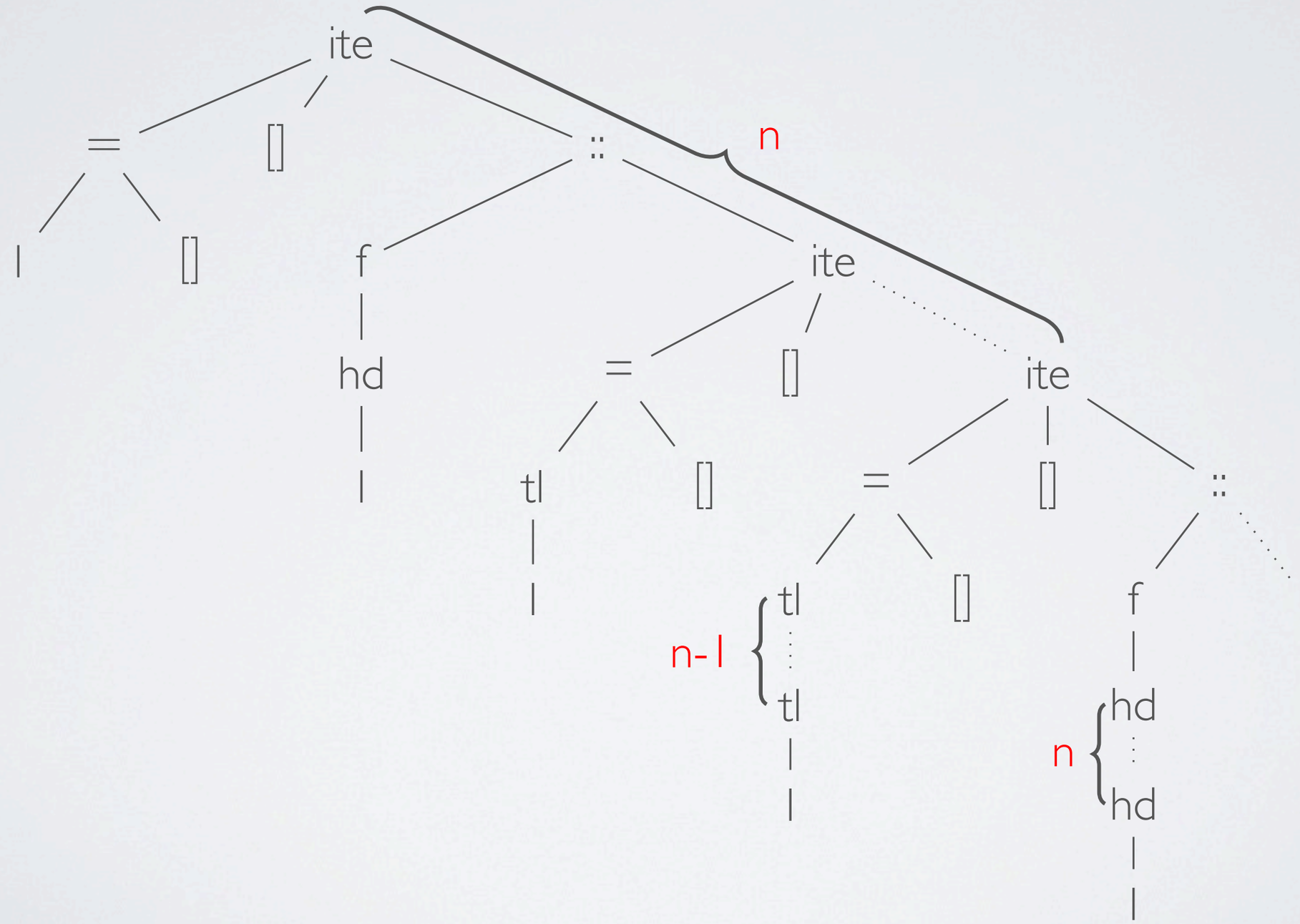
# ORDRE SUPÉRIEUR

map f l = if l=[ ] then [ ] else (f(hd l))::(map f (tl l))



# ORDRE SUPÉRIEUR

map f l = if l=[ ] then [ ] else (f(hd l))::(map f (tl l))



# HISTORIQUE

Knapik Niwinski
Urzyczyn Walukiewicz 05

Walukiewicz 96

Ong 06

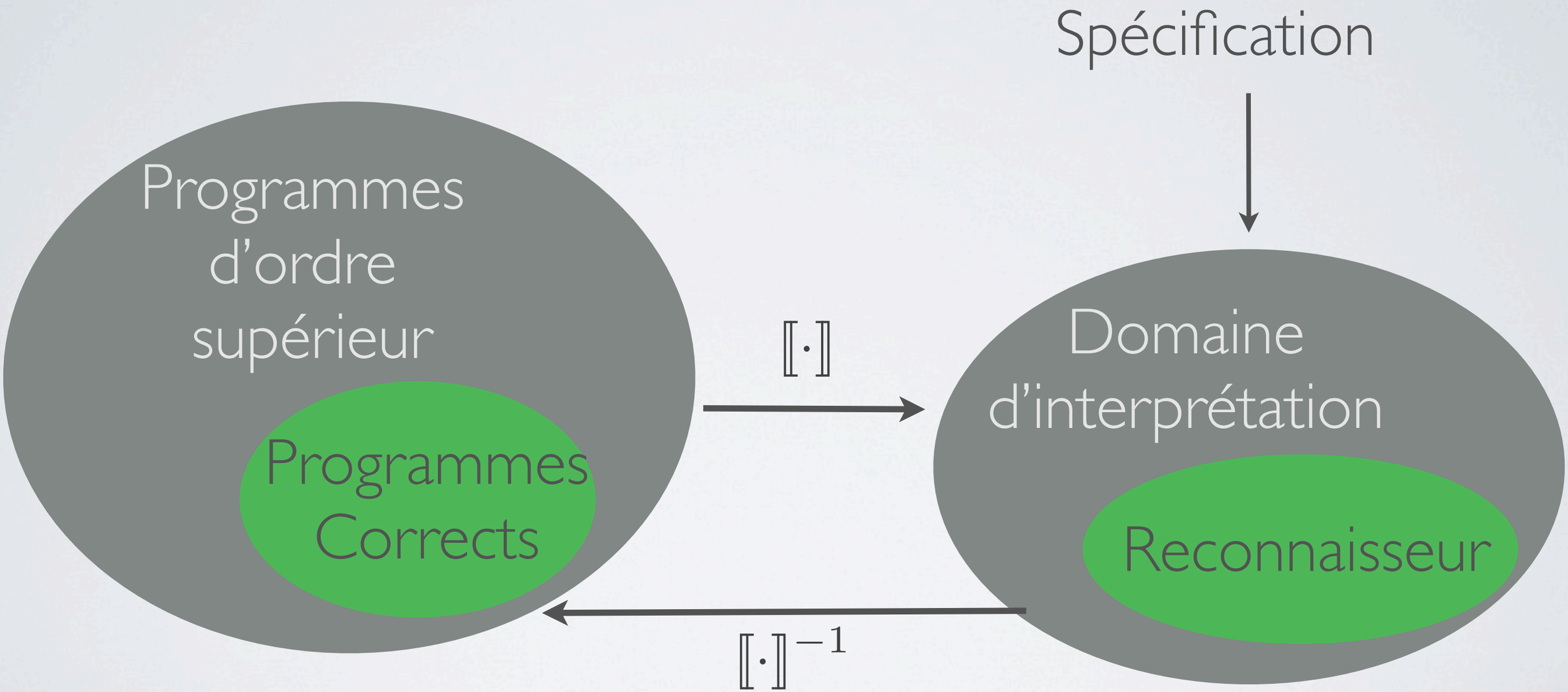
Rabin 69

Muller Schupp 85

Knapik Courcelle 02
Knapik Niwinski Urzyczyn 02

Courcelle 95
Courcelle Walukiewicz 95

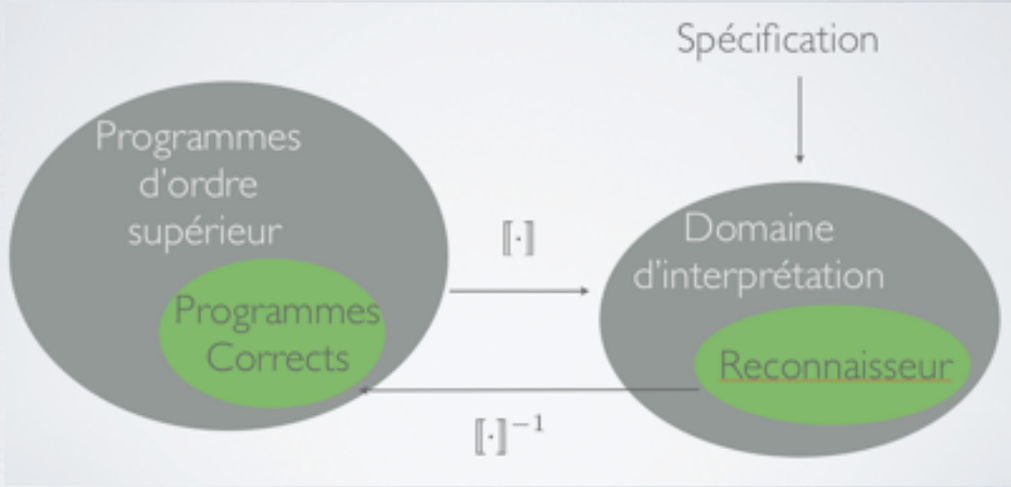
# RECONNAISSABILITÉ



# MOTIVATIONS

- Lien avec la sémantique dénotationnelle des programmes
- Révéler la structure des invariants
- Domaines finis => décidabilité

# RÉSULTATS




- Démonstration du théorème de Ong avec des outils standards du lambda calcul
- Sémantique de Scott finie = spécifications par automates triviaux
- Définition d'une sémantique qui capture les spécifications MSO dites «faibles»
- Définition d'une sémantique qui capture les spécifications MSO (en cours)

# APPLICATIONS

- Modularité de la vérification de programmes
- Synthèse de programmes à partir de modules
- Transformations de programmes pour rattraper les erreurs
- Descriptions uniformes des propriétés de sûreté et des propriétés comportementales

# PERSPECTIVES

- Affiner les algorithmes de décision
- Composer des spécifications comportementales (du local au global)
- Vers des domaines infinitaires et utilisation des méthodes d'interprétation abstraite

# Autres résultats

automates pondérés

automates à pile(s)

## Automates

automates probabilistes

transducteurs

## Algèbre

forest algebras

monoïdes inversifs

systèmes finis

temps-réel

## Vérification

code binaire

machines communicantes

SAT

## Logique

Théorie de la démonstration

## Systèmes infinis

accélération

data

Presburger

## Jeux

synthèse distribuée

jeux stochastiques

## Graphes

décomposition de graphes

fly-automata

## Programmes

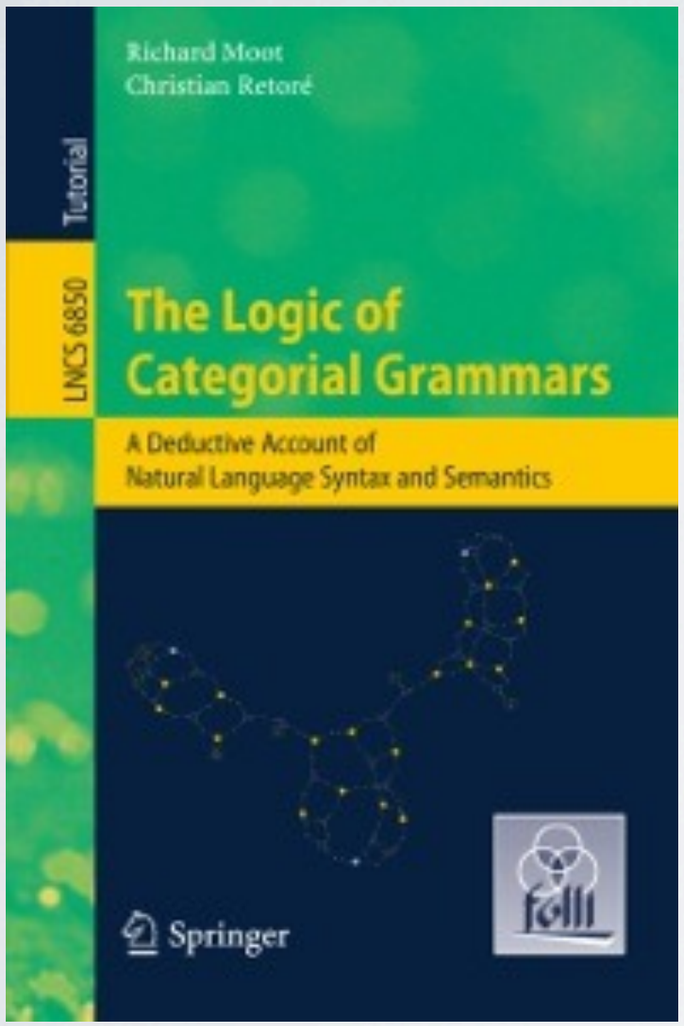
lambda-calcul

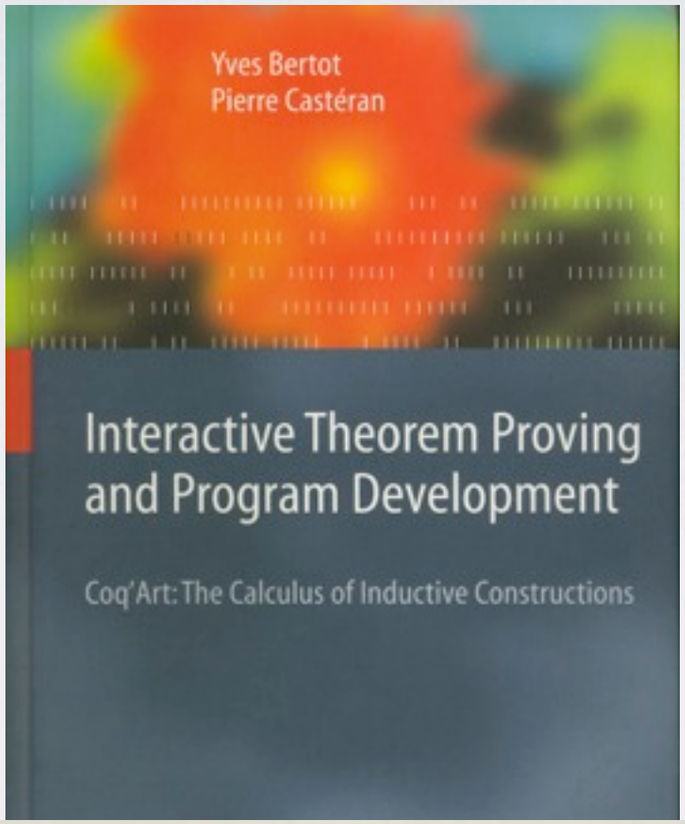
ordre supérieur

## Langages naturels

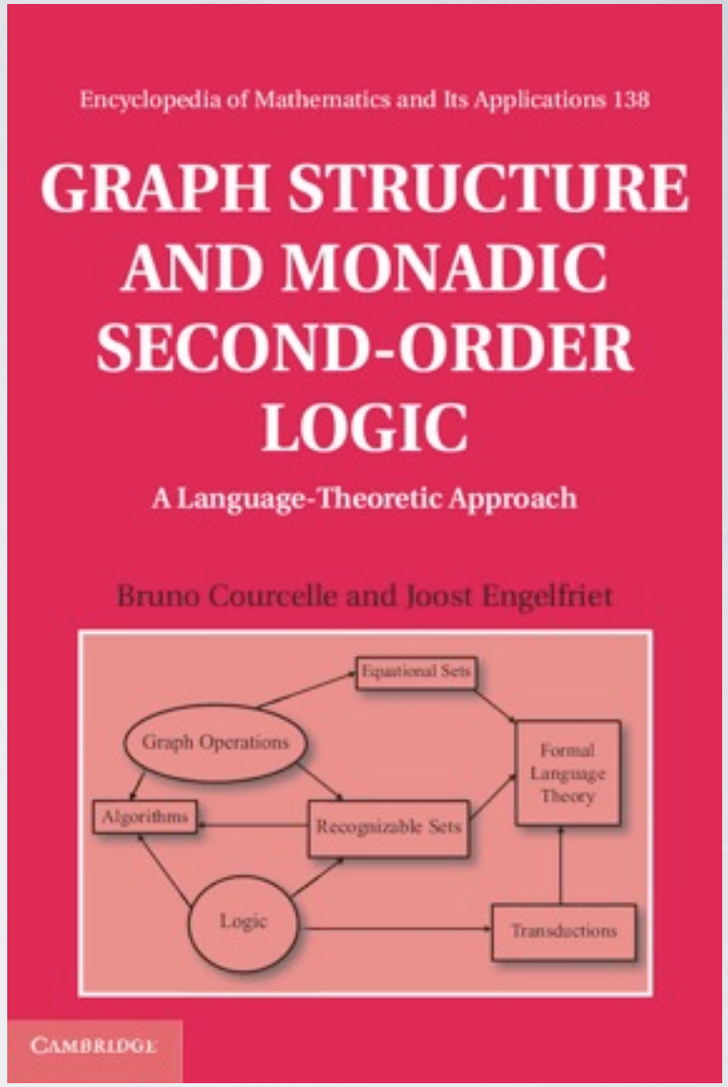
grammaires catégorielles

sémantique lexicale


Richard Moot
Christian Retoré
LNCS 6850
Tutorial
The Logic of Categorial Grammars
A Deductive Account of Natural Language Syntax and Semantics
Springer


Yves Bertot
Pierre Castéran
Interactive Theorem Proving and Program Development
Coq'Art: The Calculus of Inductive Constructions


ACM
Software System Award 2013
Presented to
Pierre Castéran, Thierry Coquand,
Gérard Huet, Christine Paulin-Mohring,
Bruno Barras, Jean-Christophe Filliâtre,
Hugo Herbelin, Chet Murthy,
Yves Bertot, and Pierre Castéran
For the Coq Proof Assistant System that provides interactive software for the development of formal proofs using a powerful logic known as the Calculus of Inductive Constructions.
ACM PRESIDENT
ACM AWARDS COMMITTEE CHAIR


Encyclopedia of Mathematics and Its Applications 138
GRAPH STRUCTURE AND MONADIC SECOND-ORDER LOGIC
A Language-Theoretic Approach
Bruno Courcelle and Joost Engelfriet
Equational Sets
Graph Operations
Formal Language Theory
Algorithms
Recognizable Sets
Logic
Transductions
CAMBRIDGE

# Logiciels et transfert

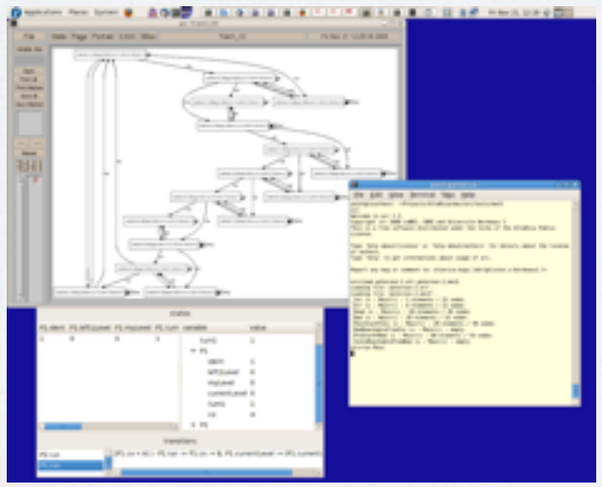
# AltaRica

Description hiérarchique de systèmes basée sur les automates.

Méthodologie: modélisation

Théorie : vérification

Implémentation: ARC et mecV



# AltaRica

Certification de commandes de vol du Falcon 7FX (Dassault Aviation)

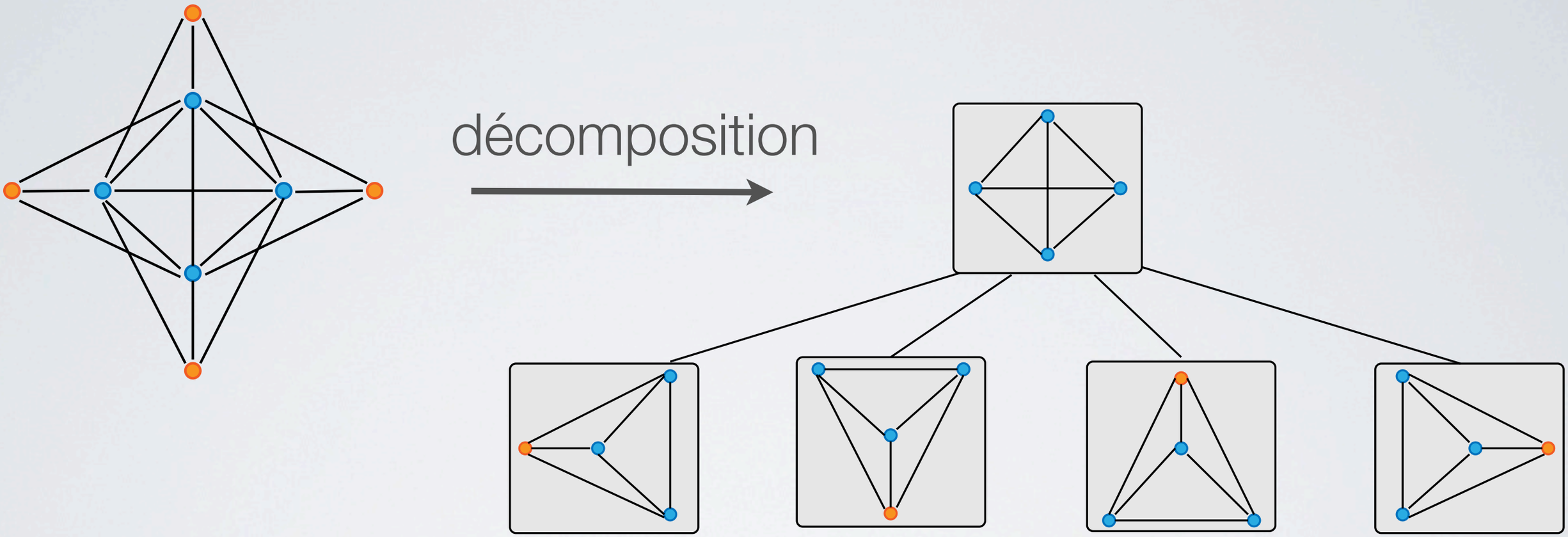
APSYS (Airbus Group) développe l'outil SIMFIA basé sur AltaRica

CERT-ONERA utilise AltaRica dans des études avioniques.

Thèse CIFRE + 2 contrats d'études sur le diagnostic de modèles AltaRica pour Thales Toulouse

# AutoWrite/AutoGraph

## Une approche pragmatique du théorème de B. Courcelle.




largeur 4

**Thm** L'évaluation d'une formule logique MSO se fait en <u>temps linéaire</u> sur des decompositions de graphes de largeur bornée.

# AutoWrite/AutoGraph

Objectif : Algorithmes pratiques pour valider des propriétés de graphes exprimables en Logique Monadique du Second Ordre

Problème : la taille des automates d'arbres explose en fonction de la borne.

Résultat : Fly-automata.
L'automate est construit au fur et à mesure qu'on évalue un arbre donné.

# Beaucoup plus...

INSIGHT : analyse de code binaire

TChecker : abstractions de systèmes temps-réel

TAPAS : arithmétique de Presburger

Glucose : SAT solver

LALBLC : équivalence d’automates à pile

Vaucanson : automates pondérés

GRAIL : analyseur syntaxique pour grammaires catégorielles

# Fonctionnement

# LGL + MV + Linguistique informatique (en 2009)

## LGL

Logique
Graphes
Langages

## MV

Modélisation et
Vérification

VISIDIA CA

POSET IS

RHOBAN

LGL (Mardi 11h)

MV (Jeudi 11h)

Petite école de Coq (Lundi 9h)

Algos distribués (Lundi 14h)

# Collaborations

LaBRI : CombAlgo, I&S, Progress

Labex CPU (LaBRI, IMB, IMS)

National:  projets ANR (5 en cours au 1/1/15)


International:

Inde: AVeRTS, LIA Informel + coopérations prévues

Allemagne-Portugal, Japon

Projet européen REACH (Europe-Inde, 2015-2018)

# Recrutements

2 PR (dont 1 mutation)

2 MdC

1 CR1 et 1 CR2 CNRS

Nouvelles thématiques avec fort potentiel, qui se marient parfaitement avec l’existant.

# Animation de la recherche

Comités de programme:

ICALP: 09, 11, 12
LICS : 10, 11, 13, 14
STACS : 12, 13

FOSSACS, FSTTCS, ICDT,
MFCS, TACAS, TALN,...

Présidence de comités de pilotage:

STACS, FoSSaCS, LIPIcs, IFIP WG

Organisation de conférences
et écoles :

ESSLLI ’09
EPIT ’11
RP ’12

# Coopérations industrielles

5 thèses CIFRE

Airbus
EADS
SERMA
THALES
2MORO

Contrats

RATP
Thales Toulouse

Projets

ANR VACSIM (Dassault, EDF)
SAFE (Dassault,...)
FUI MARSHAL (EADS,..)

Rhoban start-up

Workshops  et formations AltaRica (MBSAW ‘12)

JDEV’15 (Journées nationales du Développement Logiciel)

# Perspectives

Préserver la cohérence thématique

Maintenir un spectre large d’intérêts

S’ouvrir davantage aux coopérations

Théorème
de Courcelle

Autograph

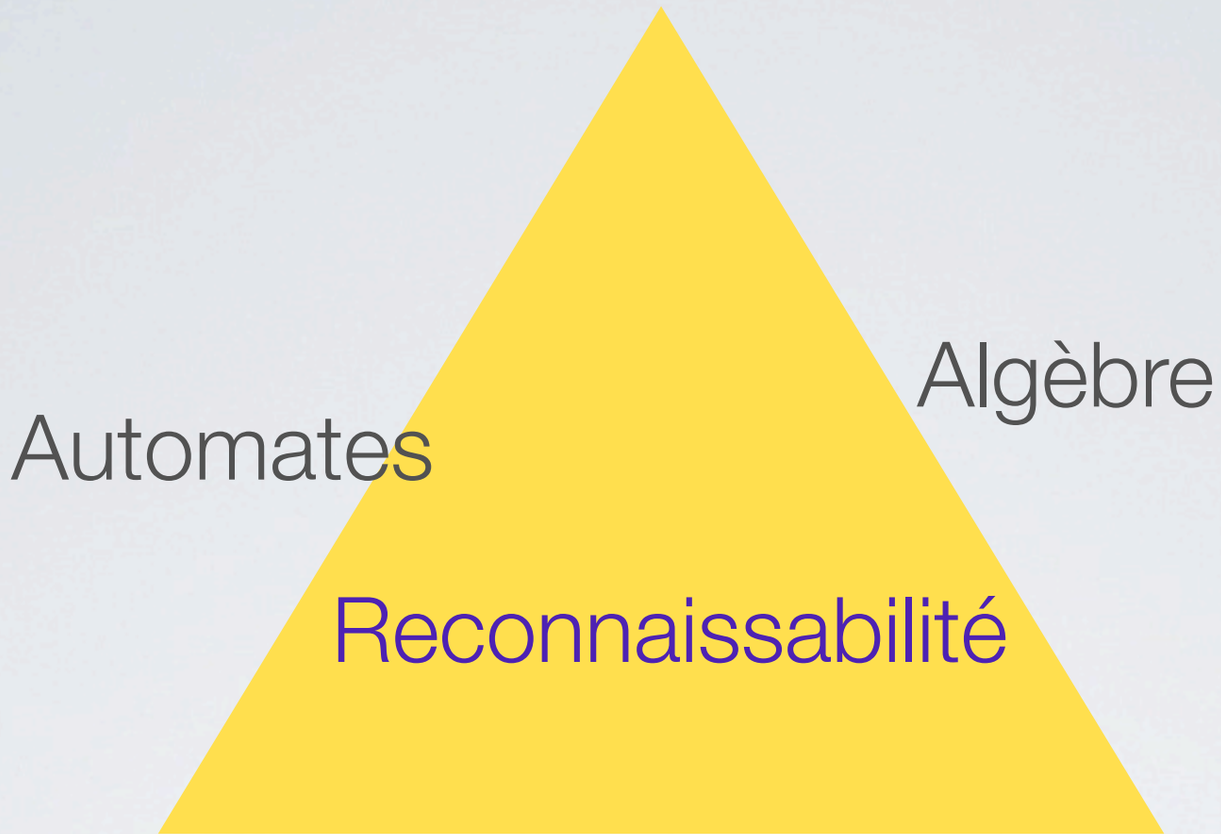
Arithmétique
de Presburger

TAPAS

Mise en œuvre de
résultats théoriques
d'envergure

Équivalence
d'automates à pile

LALBLC




Quid de cadres plus riches ? Transducteurs ?


transducteurs 2-way = transductions MSO-définissables

Parallélisation massive de techniques SAT

Vérification: Contrat avec la RATP

Thèse CIFRE (SafeRiver)

# SAT (Glucose)

Hybridation BDD/SAT dans ALTARICA

Applications transverses: bioinfo, I&S, graphes

# MÉTHODES FORMELLES

Michel Bauderon
Wafa Ben-Jaballah
Michel Billaud
Sébastien Bindel
Pierre Bourreau
Frédérique Carrère
Pierre Castéran
Lionel Clément
Bruno Courcelle
Anne Dicky
Etienne Dubourg
Irène Durand
Patrick Félix
Diego Figueira
Emmanuel Fleury
Olivier Gauwin
Thomas Geffroy
Hugo Gimbert
Paul Gloess
Alain Griffault
Pierre Halftermeyer
Frédéric Herbreteau
Ludovic Hofer
David Janin
Edon Kelmendi
Jérôme Kirman
Denis Lapoire
Jérôme Leroux
Sylvain Lombardy
Olivier Ly
Richard Moot
Mohamed Mosbah
Anca Muscholl
Kaninda Musumbu
Grégoire Passault
Thomas Place
Gérald Point
Gabriele Puppis
David Renault
Christian Rétoré
Antoine Rollet
Quentin Rouxel
Sylvain Salvati
Géraud Sénizergues
Laurent Simon
Marc Sylvestre
Grégoire Sutre
Lorijn Van Rooijen
Thanh Tung Tran
Aymeric Vincent
Igor Walukiewicz
Pascal Weil
Marc Zeitoun