Sur-approximations non régulières et terminaison pour l'analyse d'accessibilité

Vivien Pelletier

29 août 2018

Sommaire

1 Introduction

2 Analyse d'accessibilité

3 Sur-approximations d'ensemble de descendants

4 Méthode de complétion

Systèmes complexes

Système complexe

Un système complexe est un ensemble constitué d'un grand nombre d'entités en interaction qui empêchent l'observateur de prévoir sa rétroaction, son comportement ou évolution par le calcul.

Systèmes complexes

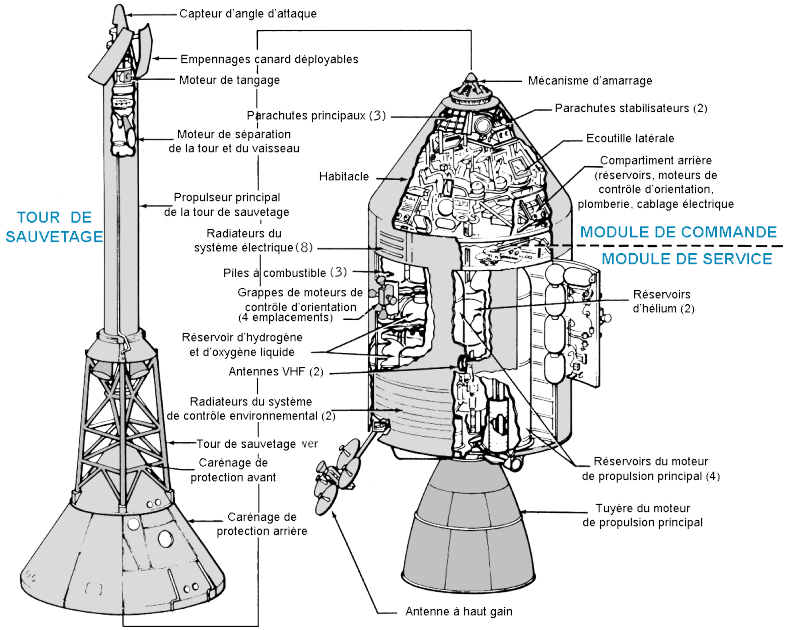
Système complexe

Un système complexe est un ensemble constitué d'un grand nombre d'entités en interaction qui empêchent l'observateur de prévoir sa rétroaction, son comportement ou évolution par le calcul.

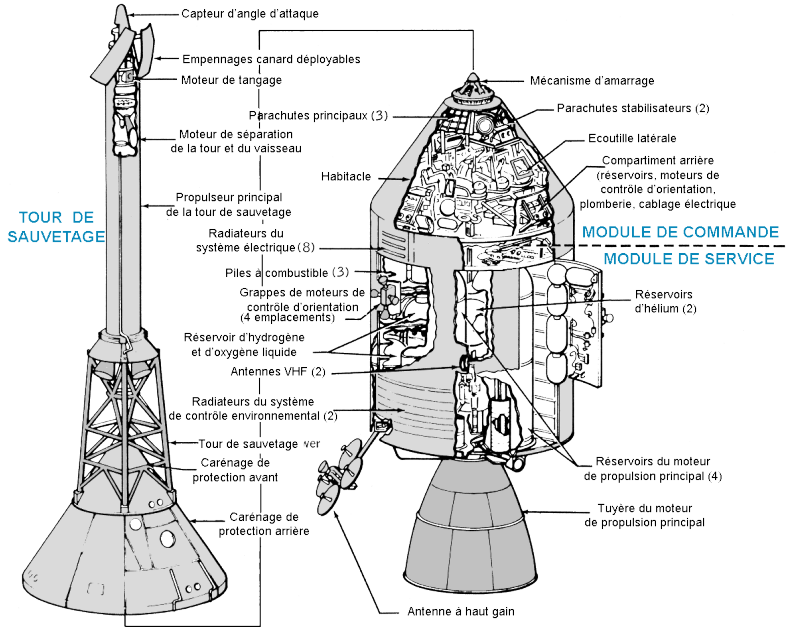
Exemples

- programmes informatiques
- protocoles de sécurité
- circuits logiques

Le génie logiciel



Le génie logiciel



Génie logiciel

L'ensemble des activités de conception et de mise en œuvre des produits et des procédures tendant à rationaliser la production du logiciel et son suivi.

Vérification

Conformité et fiabilité d'un système complexe ?

Vérification

Conformité et fiabilité d'un système complexe ?

- Les tests

Vérification

Conformité et fiabilité d'un système complexe ?

- Les tests
  - si l'ensemble d'entrées est trop grand ou infini ?

Vérification

Conformité et fiabilité d'un système complexe ?

- Les tests
  - si l'ensemble d'entrées est trop grand ou infini ?
- Les méthodes formelles

Vérification

Conformité et fiabilité d'un système complexe ?

- Les tests
  - si l'ensemble d'entrées est trop grand ou infini ?
- Les méthodes formelles
  - analyse statique par interprétation abstraite

Vérification

Conformité et fiabilité d'un système complexe ?

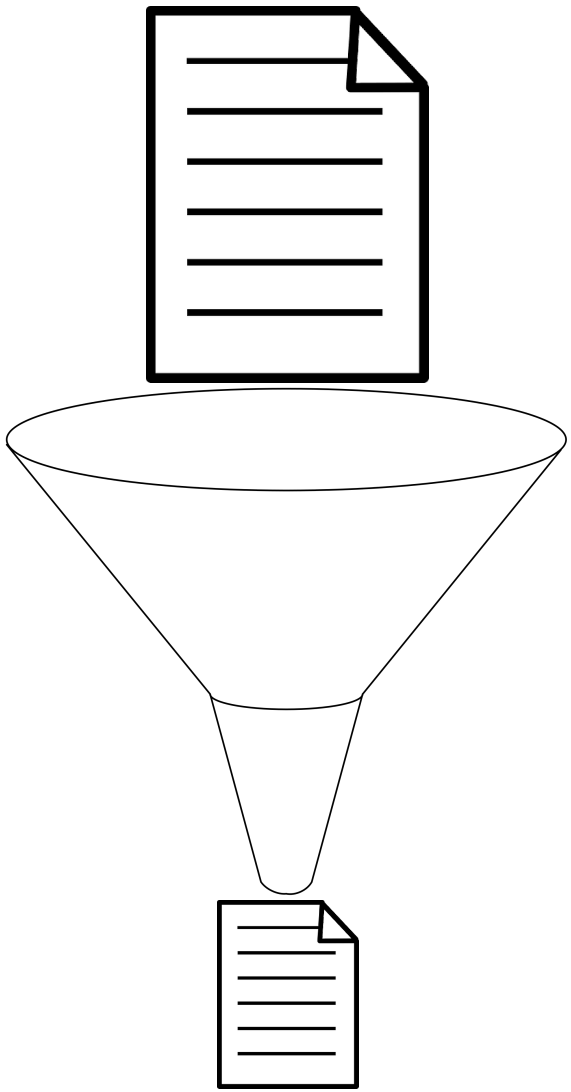
- Les tests
  - si l'ensemble d'entrées est trop grand ou infini ?
- Les méthodes formelles
  - analyse statique par interprétation abstraite
  - vérification déductive

Vérification

Conformité et fiabilité d'un système complexe ?

- Les tests
  - si l'ensemble d'entrées est trop grand ou infini ?
- Les méthodes formelles
  - analyse statique par interprétation abstraite
  - vérification déductive
  - vérification de modèles

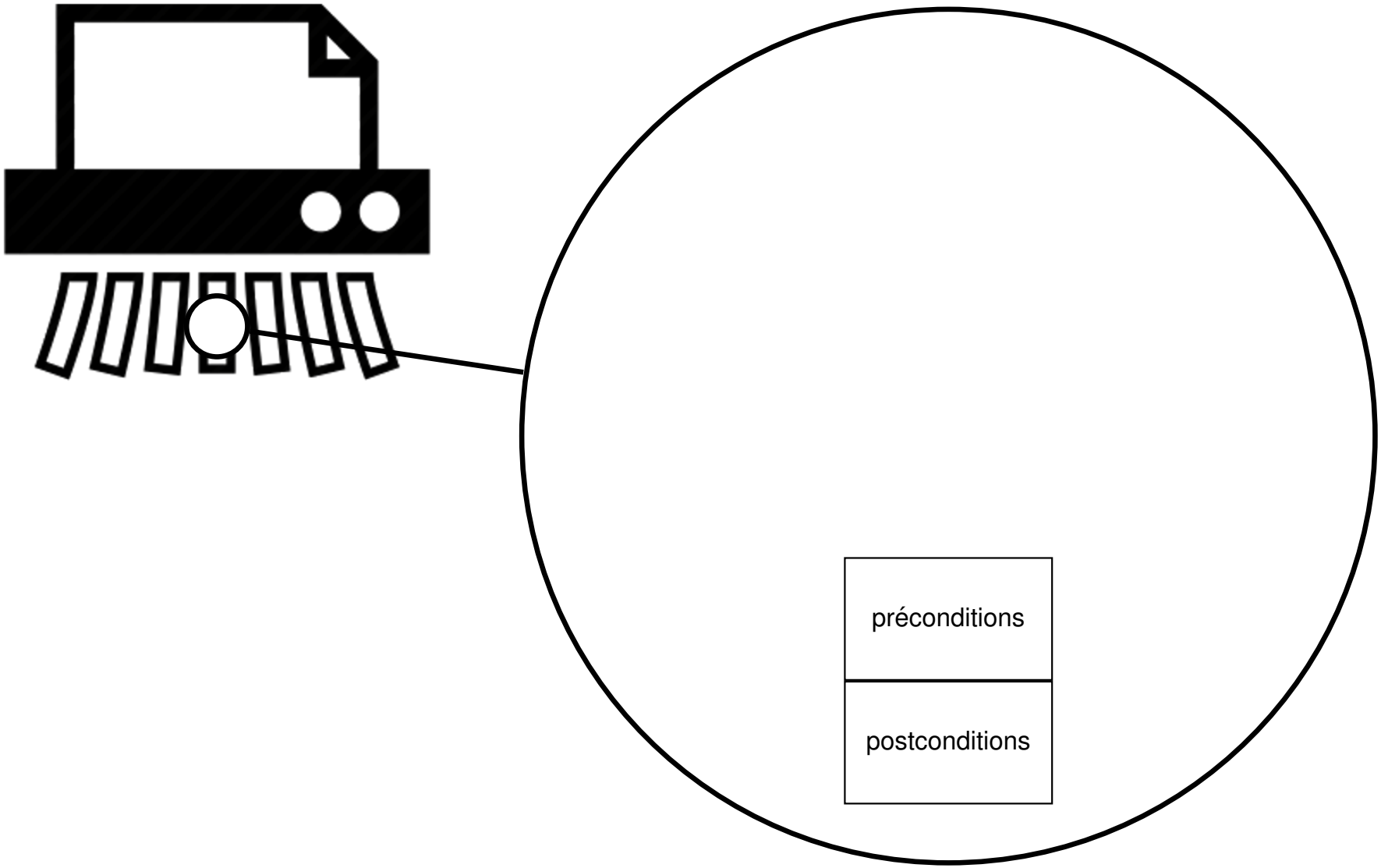
Analyse statique par interprétation abstraite



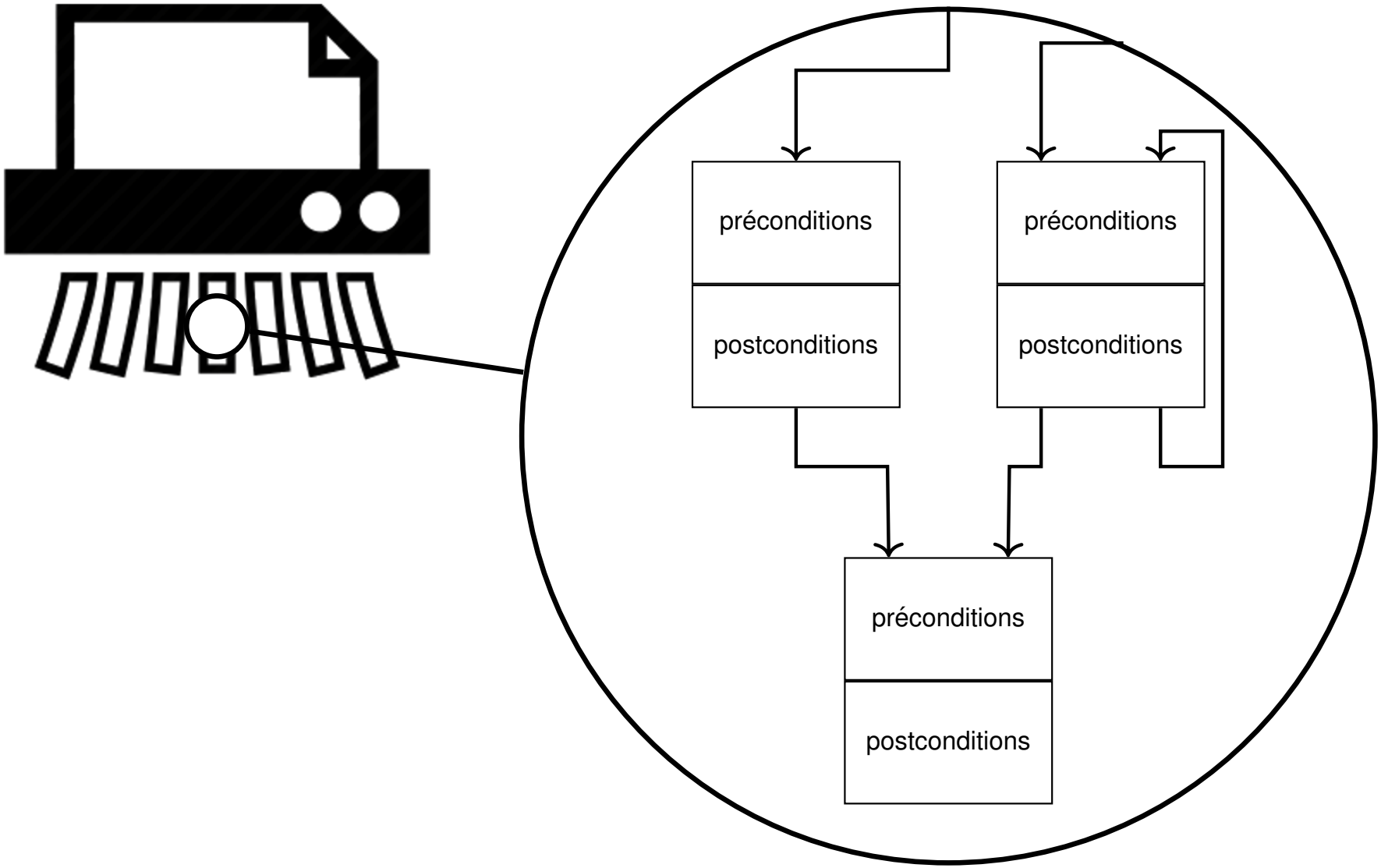
- Constat
  - trop d'informations
- Solution
  - utilisation d'abstractions
- Difficulté
  - garder suffisamment d'informations
  - mais pas trop

Vérification déductive

Vérification déductive

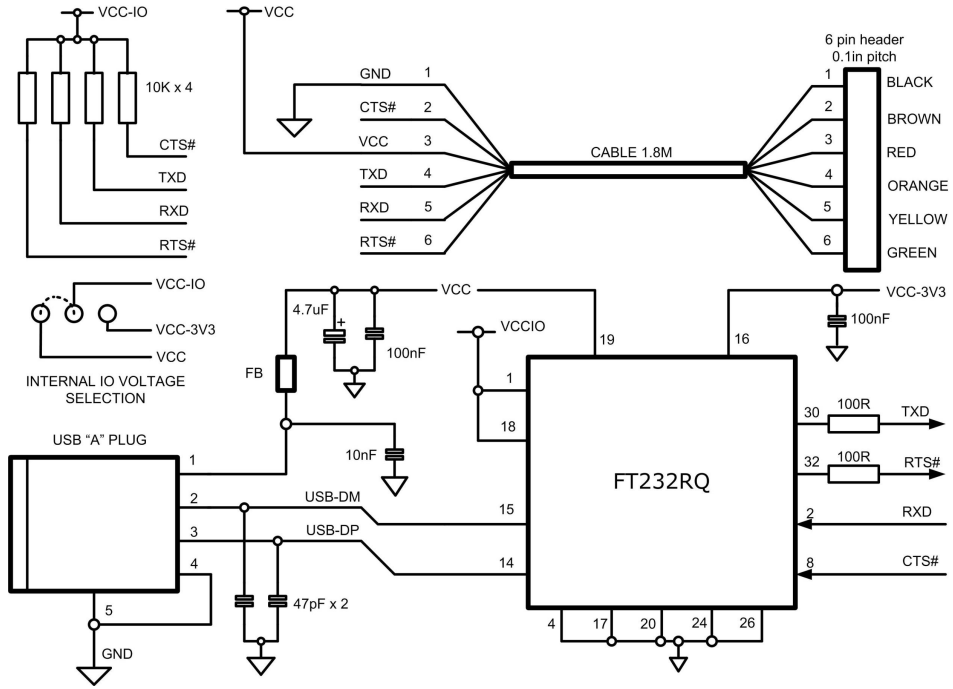


Vérification déductive



Vérification de modèles

- Analyse exhaustive
- Représentation astucieuse



Sommaire

1 Introduction

2 Analyse d'accessibilité

3 Sur-approximations d'ensemble de descendants

4 Méthode de complétion

Analyse d'accessibilité

Configurations

- Ensemble des configurations accessibles

Analyse d'accessibilité

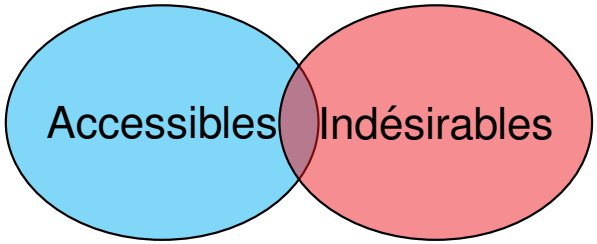
Configurations

- Ensemble des configurations accessibles
- Ensemble des configurations indésirables

Analyse d'accessibilité

Configurations

- Ensemble des configurations accessibles
- Ensemble des configurations indésirables

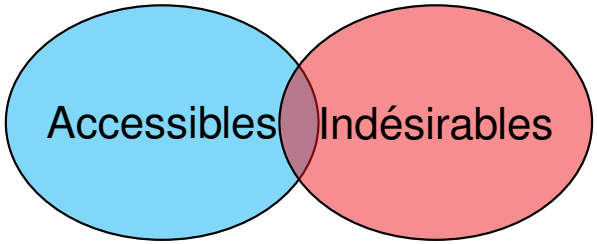


Il existe une configuration indésirable accessible

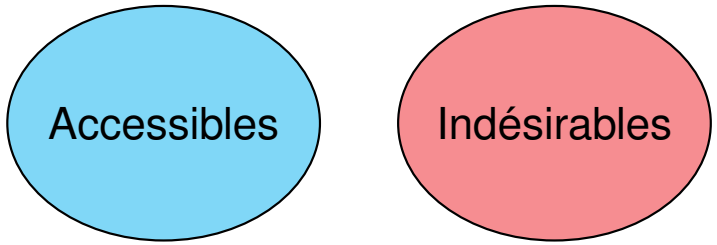
Analyse d'accessibilité

Configurations

- Ensemble des configurations accessibles
- Ensemble des configurations indésirables



Il existe une configuration indésirable accessible



Aucune configuration indésirable n'est accessible

Calcul de l'ensemble des configurations accessibles

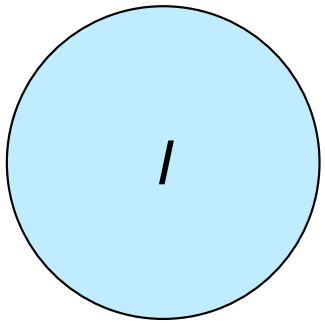
- Configurations initiales : *I*

Calcul de l'ensemble des configurations accessibles

- Configurations initiales : I
- Dynamique : R

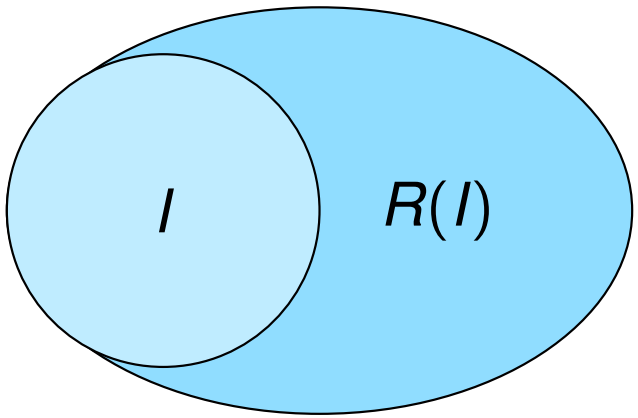
Calcul de l'ensemble des configurations accessibles

- Configurations initiales : I
- Dynamique : R



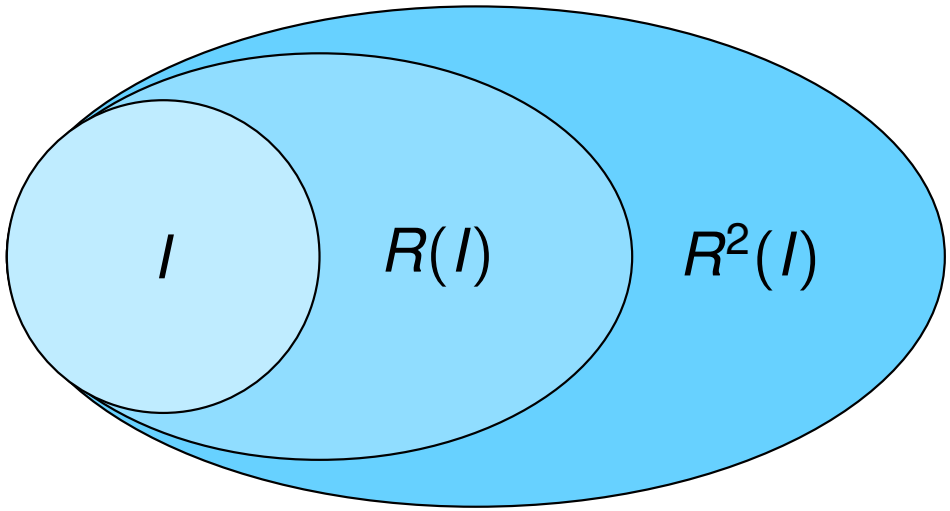
Calcul de l'ensemble des configurations accessibles

- Configurations initiales : I
- Dynamique : R



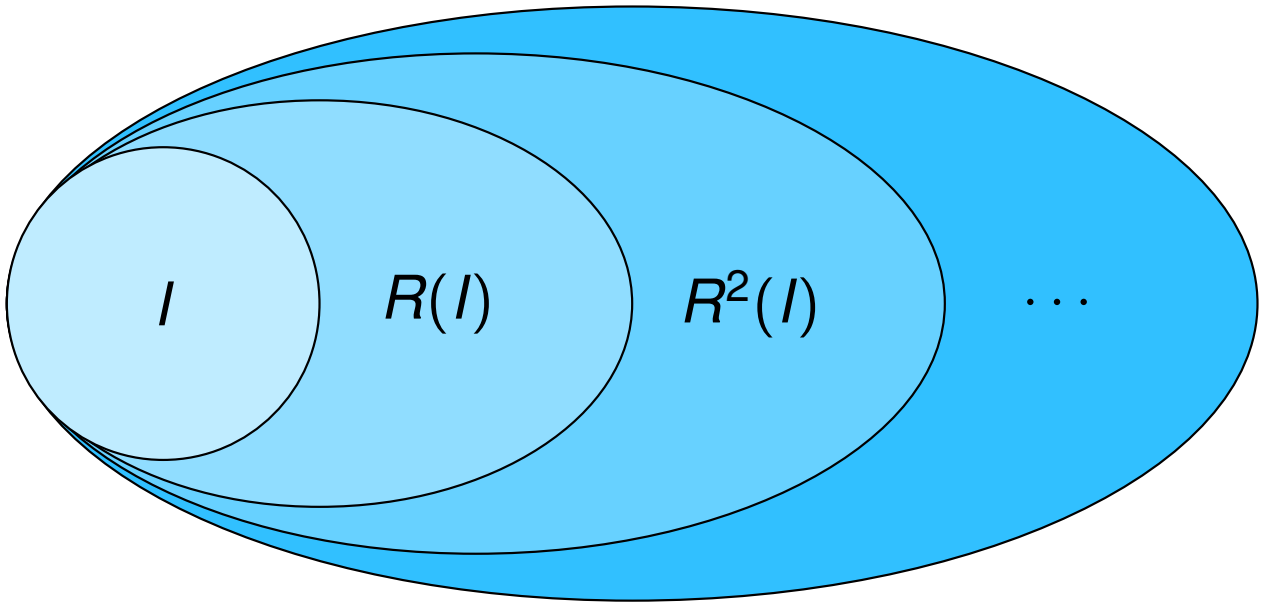
Calcul de l'ensemble des configurations accessibles

- Configurations initiales : I
- Dynamique : R



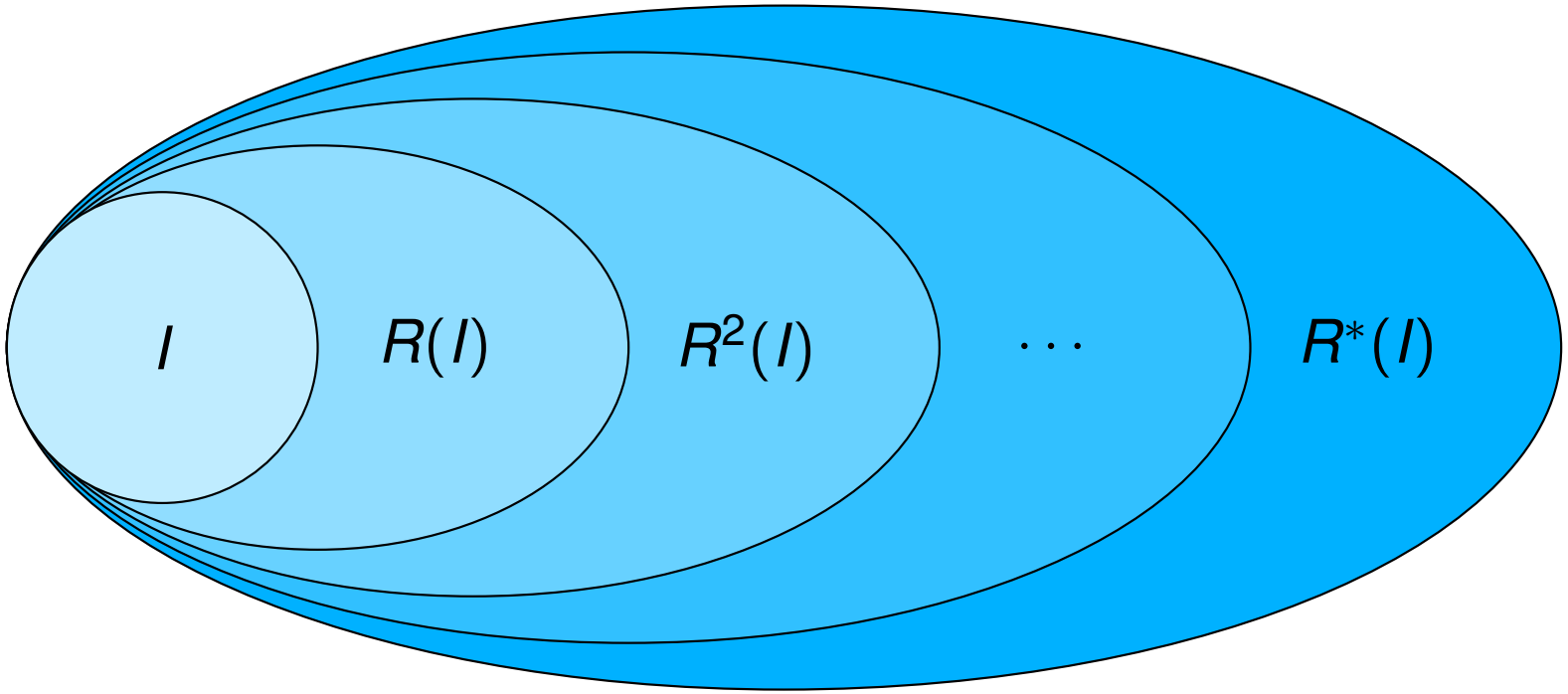
Calcul de l'ensemble des configurations accessibles

- Configurations initiales : I
- Dynamique : R

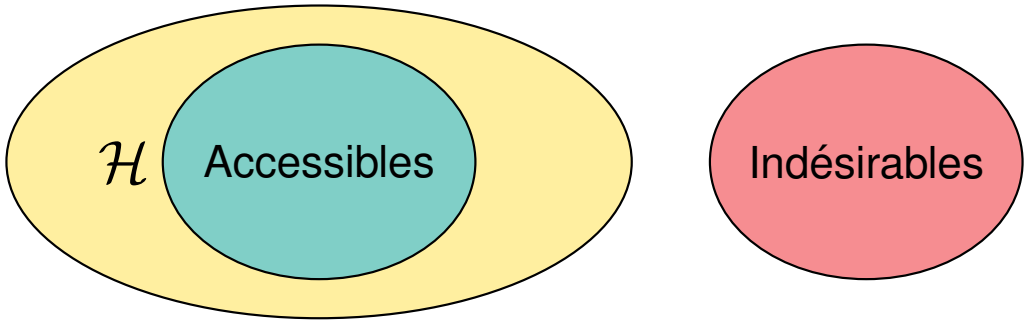


Calcul de l'ensemble des configurations accessibles

- Configurations initiales : I
- Dynamique : R

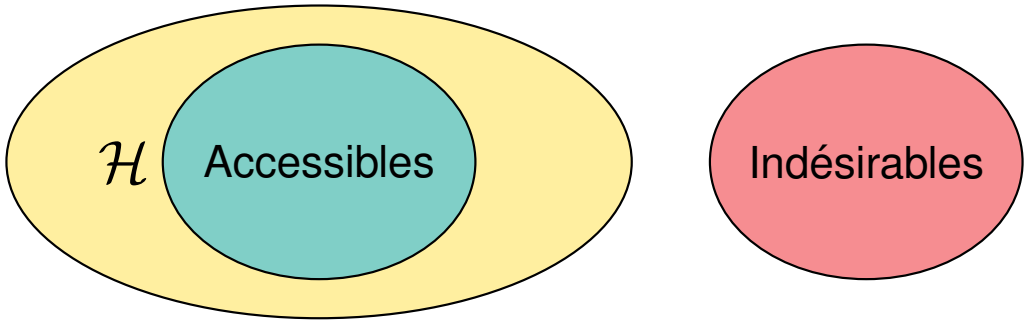


Sur-approximations

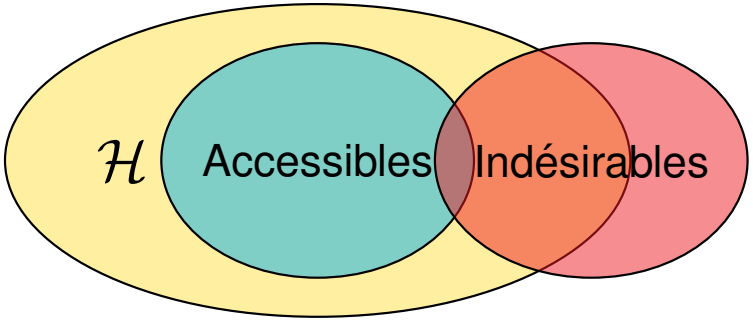


Aucune configuration indésirable accessible

Sur-approximations

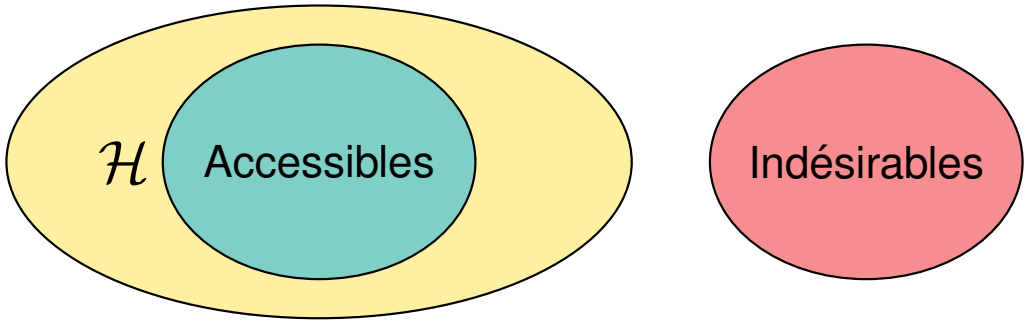


Aucune configuration indésirable accessible

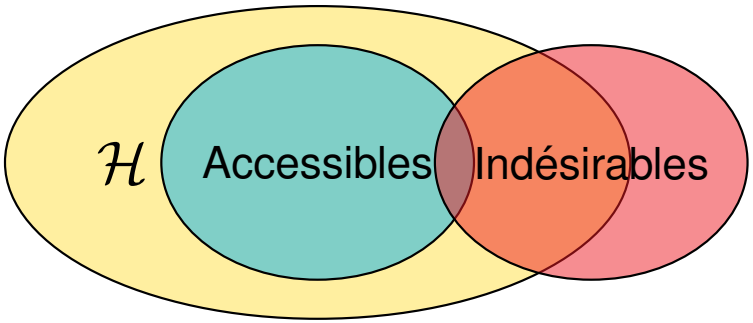


Il existe une configuration indésirable accessible

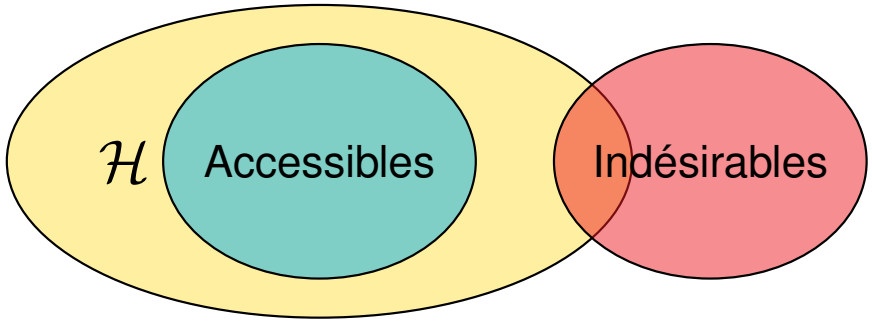
Sur-approximations



Aucune configuration indésirable accessible



Il existe une configuration indésirable accessible



Aucune configuration indésirable accessible (faux-positif)

Notre modélisation

- Configuration : un terme

Notre modélisation

- Configuration : un terme
- Configurations initiales : un langage de termes

Notre modélisation

- Configuration : un terme
- Configurations initiales : un langage de termes
- Dynamique du système : un système de réécriture

Notre modélisation

- Configuration : un terme
- Configurations initiales : un langage de termes
- Dynamique du système : un système de réécriture
- Configurations indésirables : un langage de termes

Sommaire

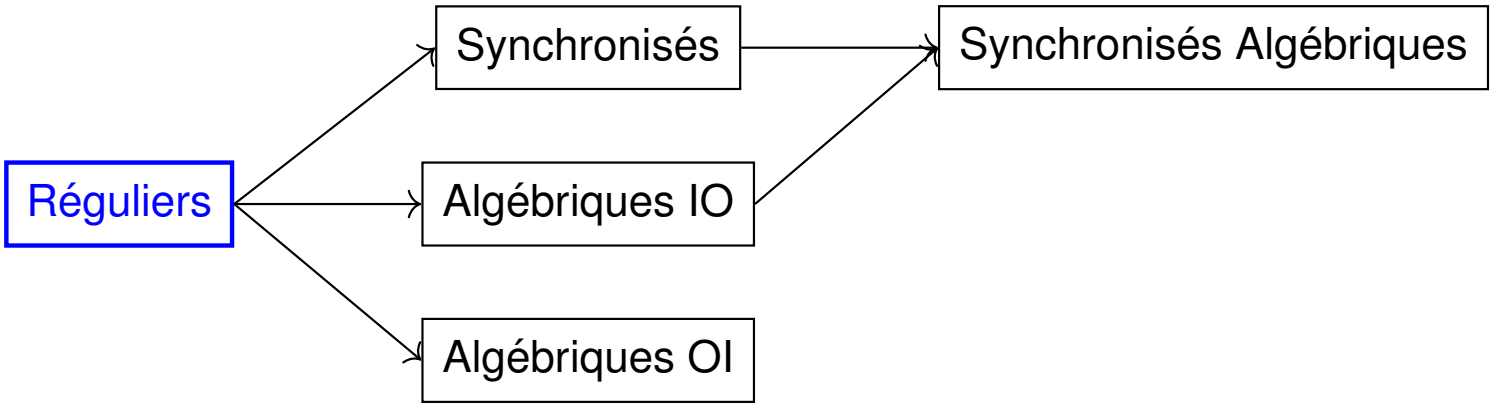
1 Introduction

2 Analyse d'accessibilité

3 Sur-approximations d'ensemble de descendants

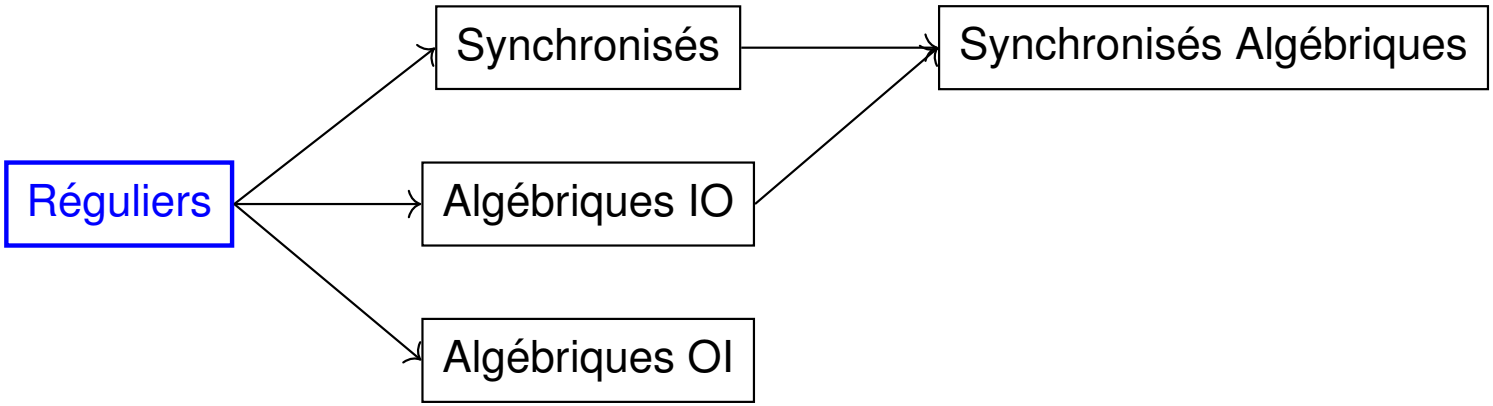
4 Méthode de complétion

Les différentes techniques



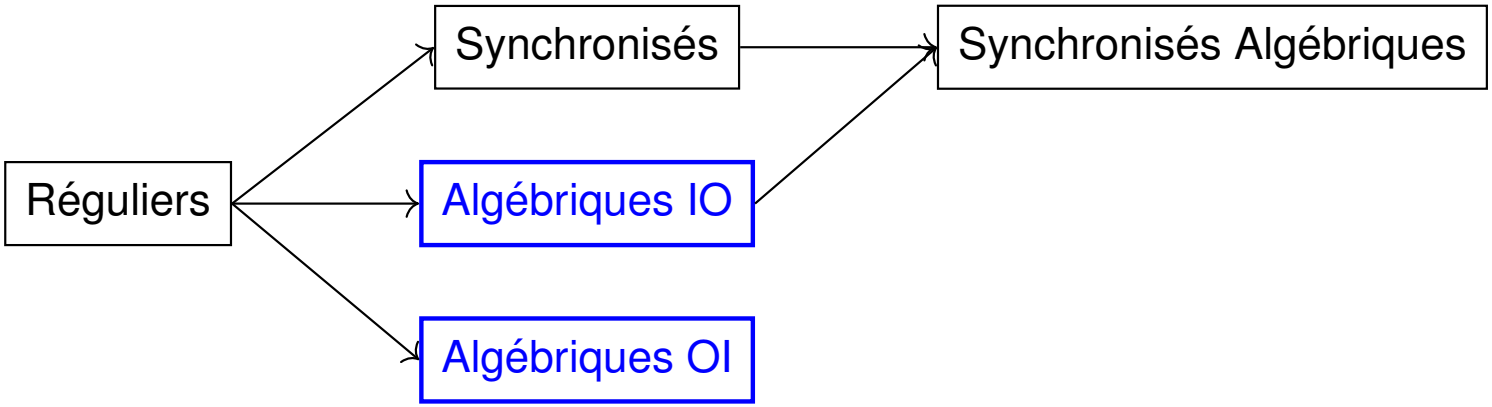
- T. Genet, Decidable approximations of sets of descendants and sets of normal forms, RTA, 1998
- T. Genet et F. Klay, Rewriting for cryptographic protocol verification, CADE, 2000
- T. Genet et V. Rusu, Equational approximations for tree automata completion, JSC, 2010

Les différentes techniques



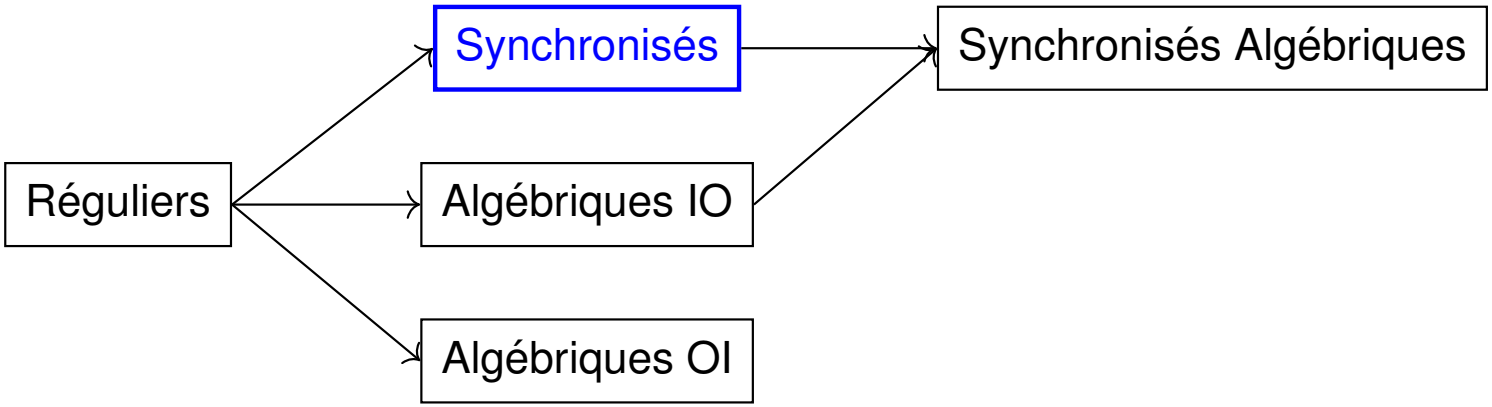
- Y. Boichut et P.-C. Héam, A theoretical limit for safety verification techniques with regular fix-point computations, IPL, 2008

Les différentes techniques



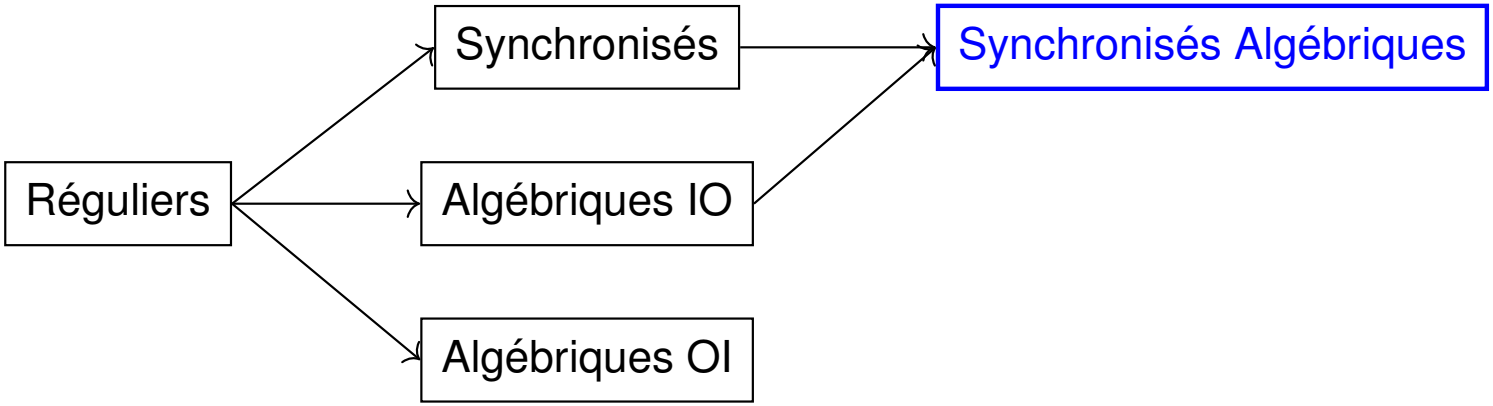
- J. Kochems et L. Ong, Improved functional flow and reachability analyses using indexed linear tree grammars, RTA, 2011

Les différentes techniques



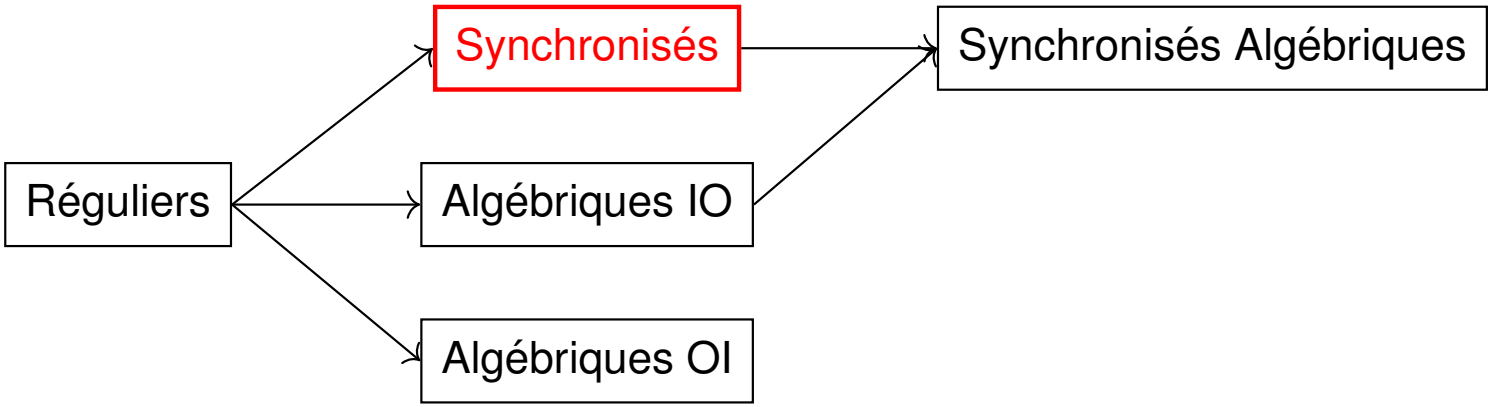
- Y. Boichut, J. Chabin, et P. Réty, Over-approximating descendants by synchronized tree languages, RTA, 2013

Les différentes techniques



- Y. Boichut, J. Chabin, et P. Réty, Towards more precise rewriting approximations, LATA, 2015

Les différentes techniques

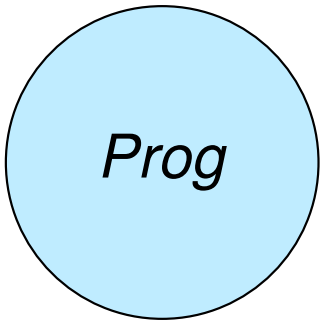


- Y. Boichut, V. Pelletier, et P. Réty, Synchronized tree languages for reachability in non-right-linear term rewrite systems, WRLA, 2016

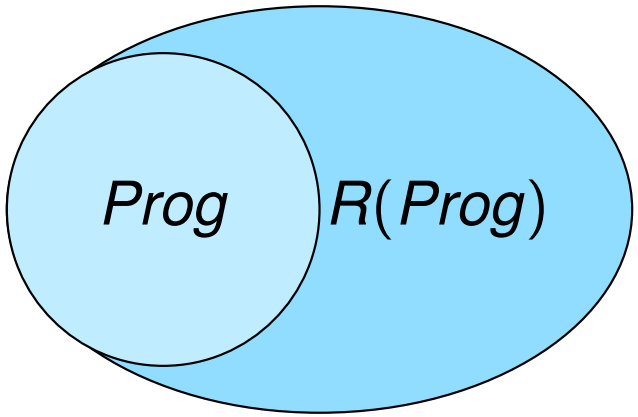
Sommaire

1. Introduction
2. Analyse d'accessibilité
3. Sur-approximations d'ensemble de descendants
4. Méthode de complétion

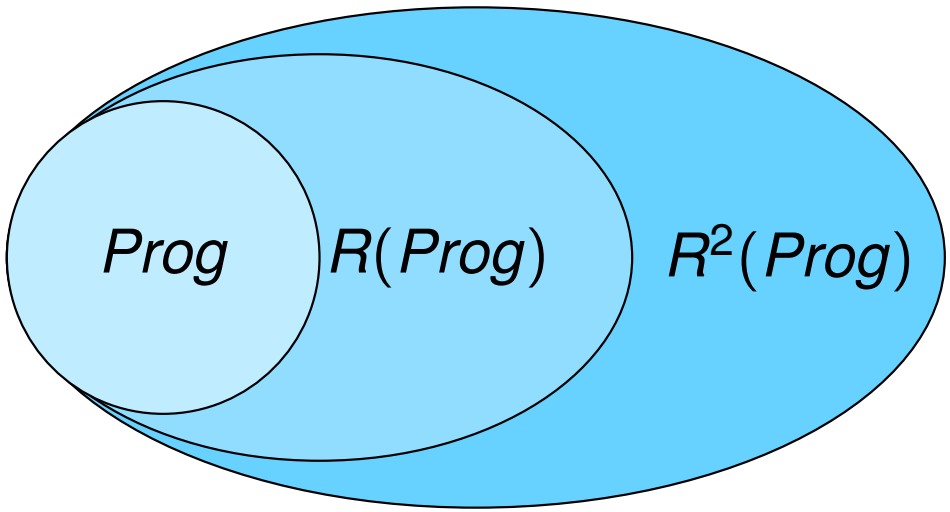
Méthode de complétion



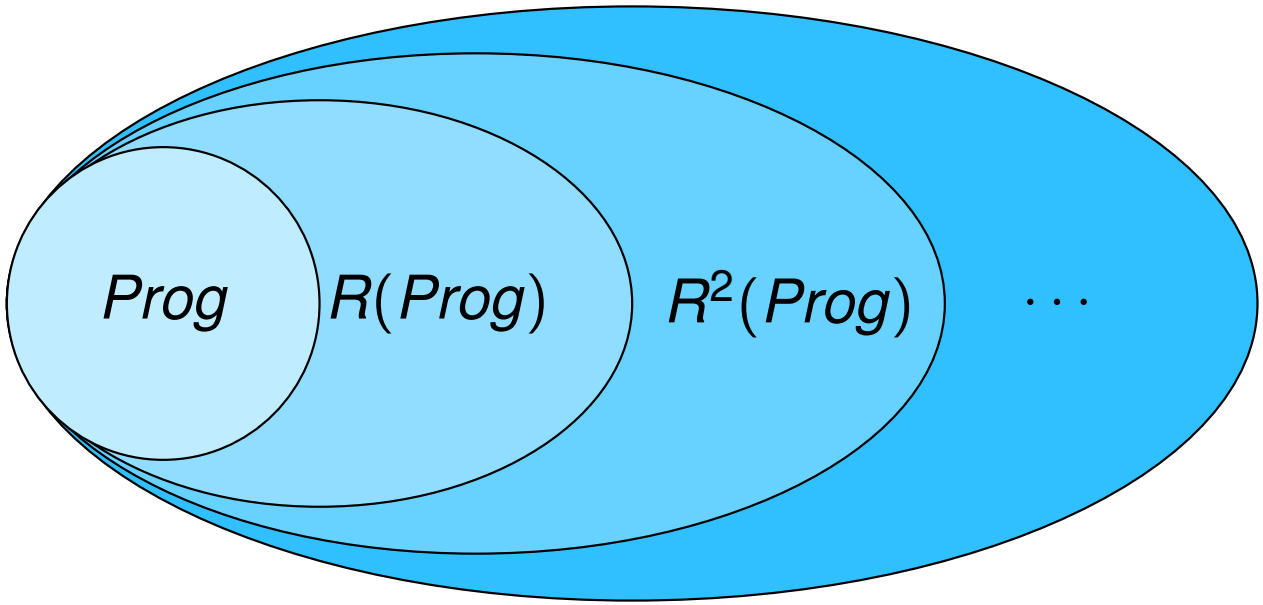
Méthode de complétion



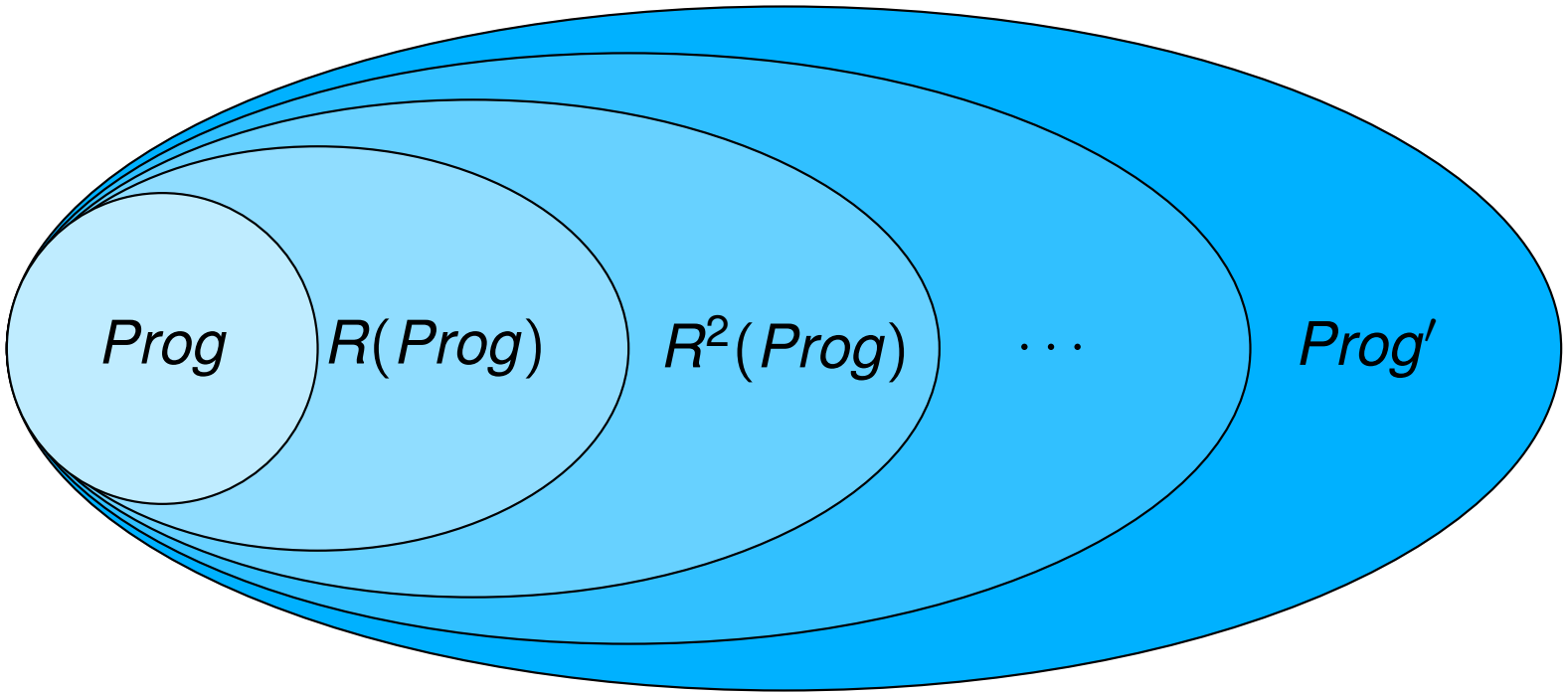
Méthode de complétion



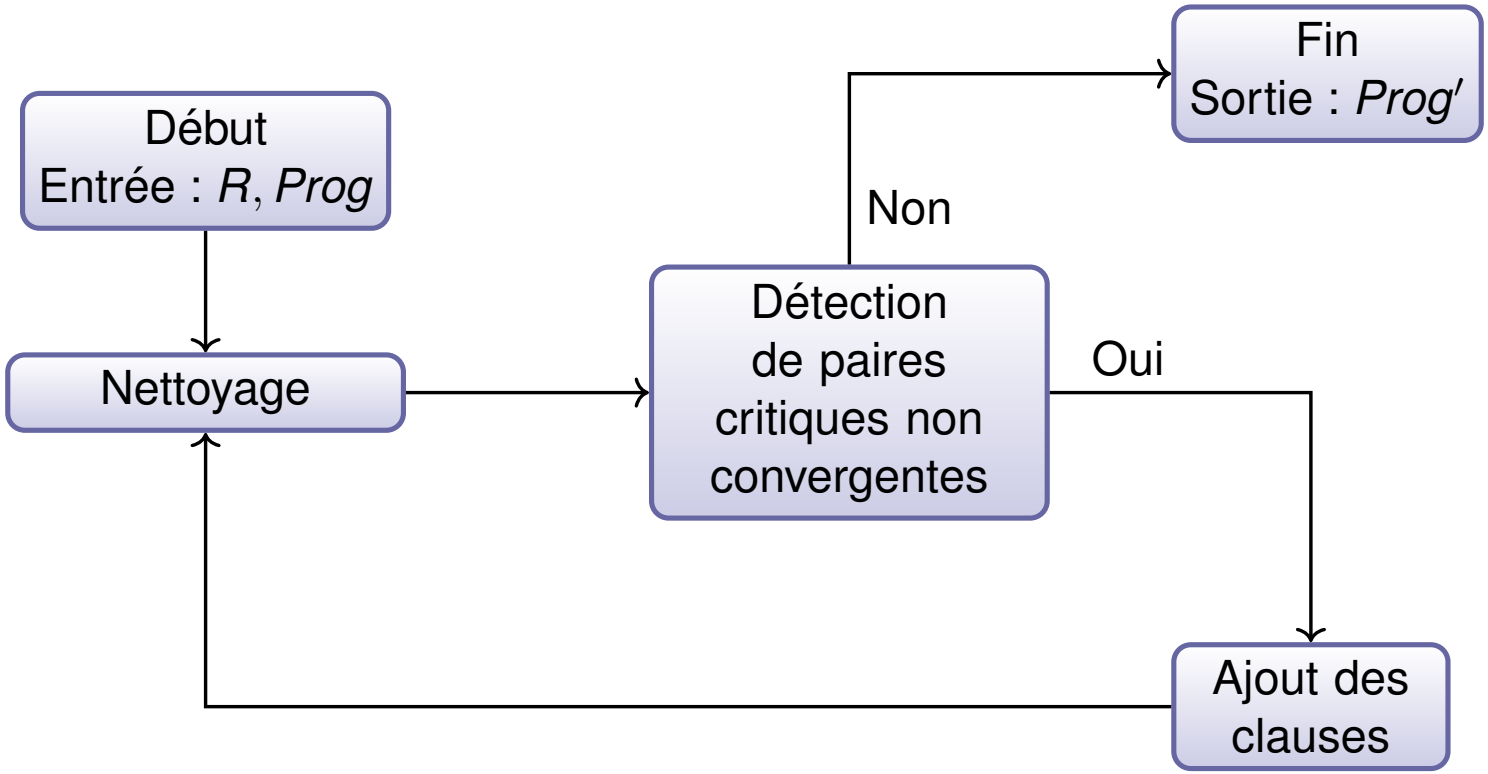
Méthode de complétion



Méthode de complétion

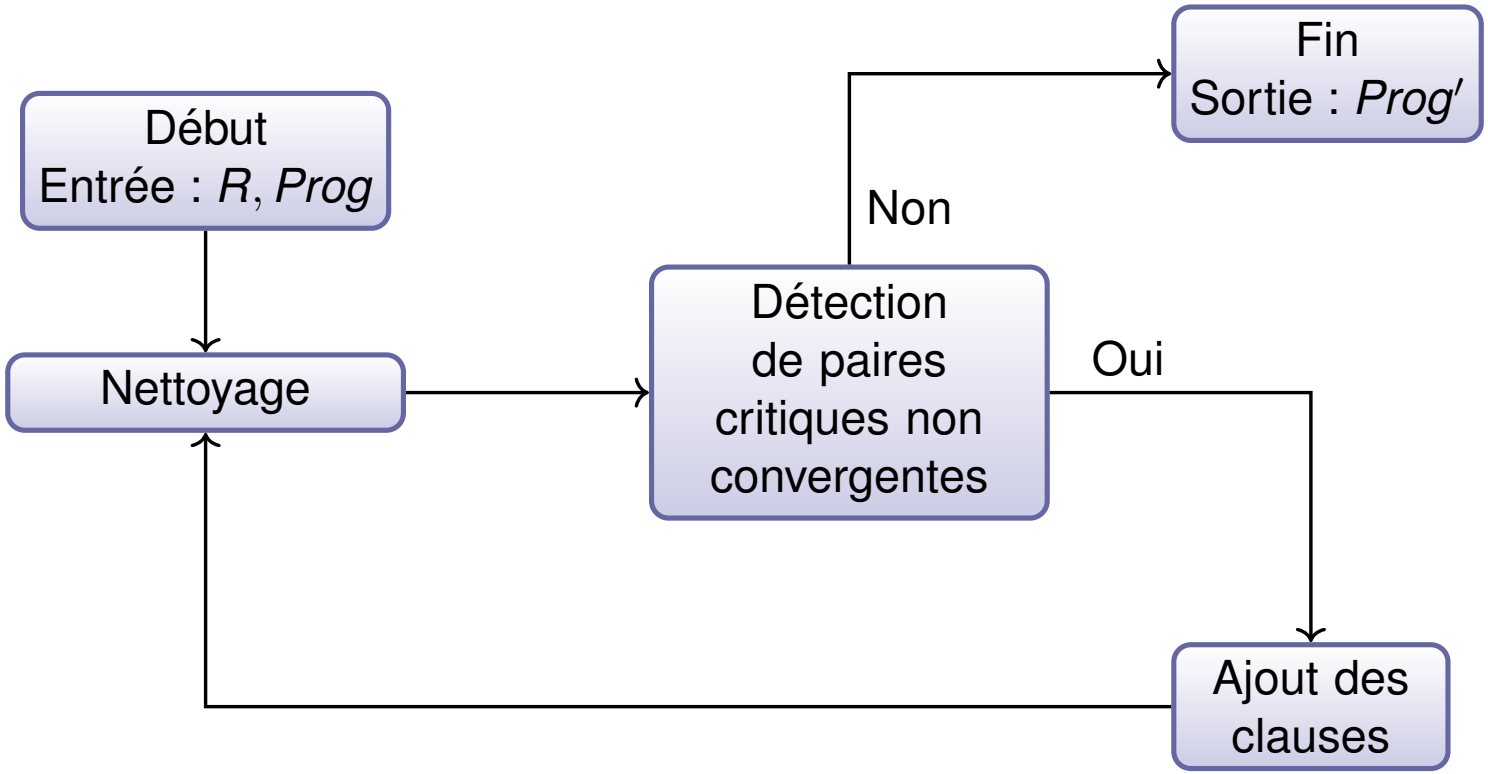


L'algorithme de complétion



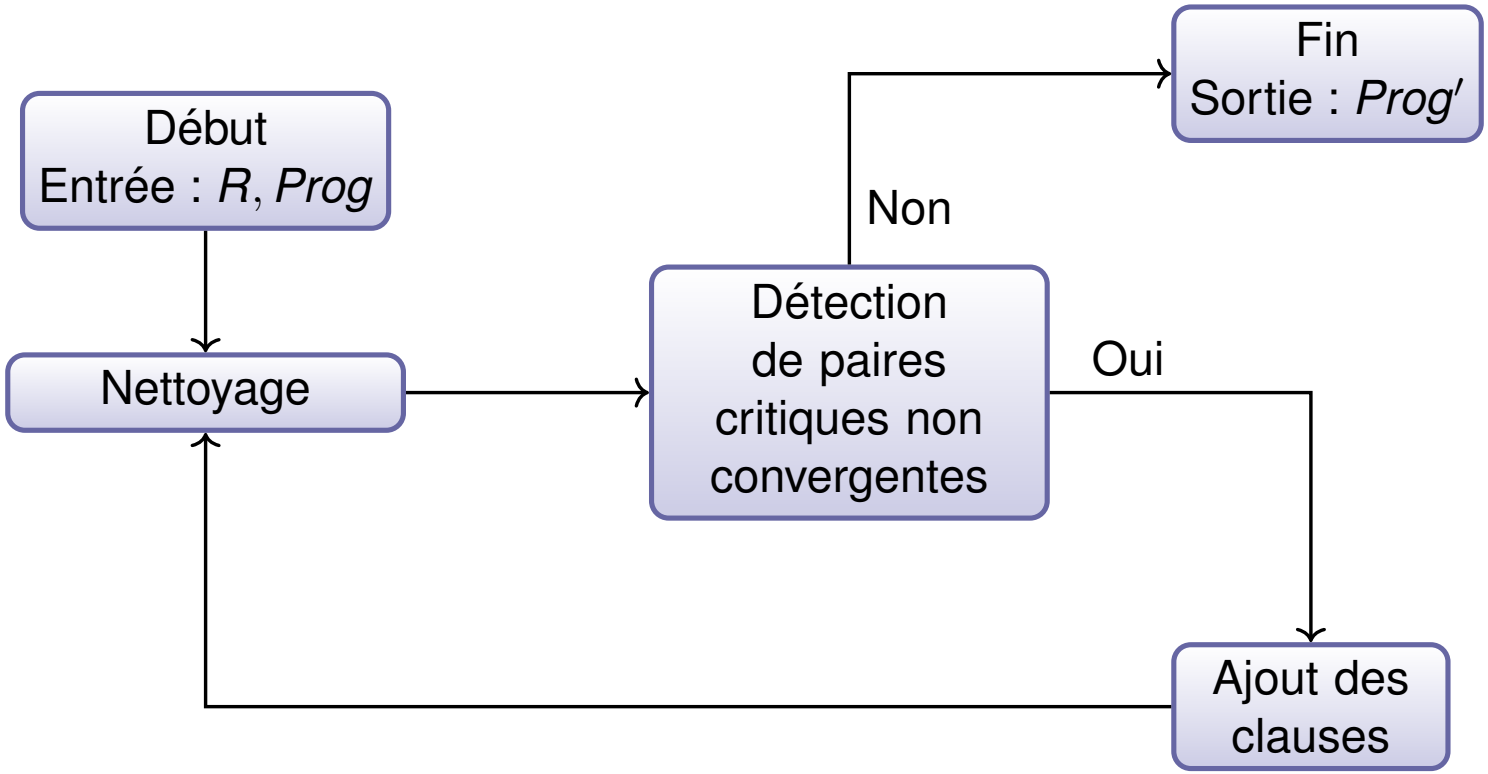
- Un CS-programme initial

L'algorithme de complétion



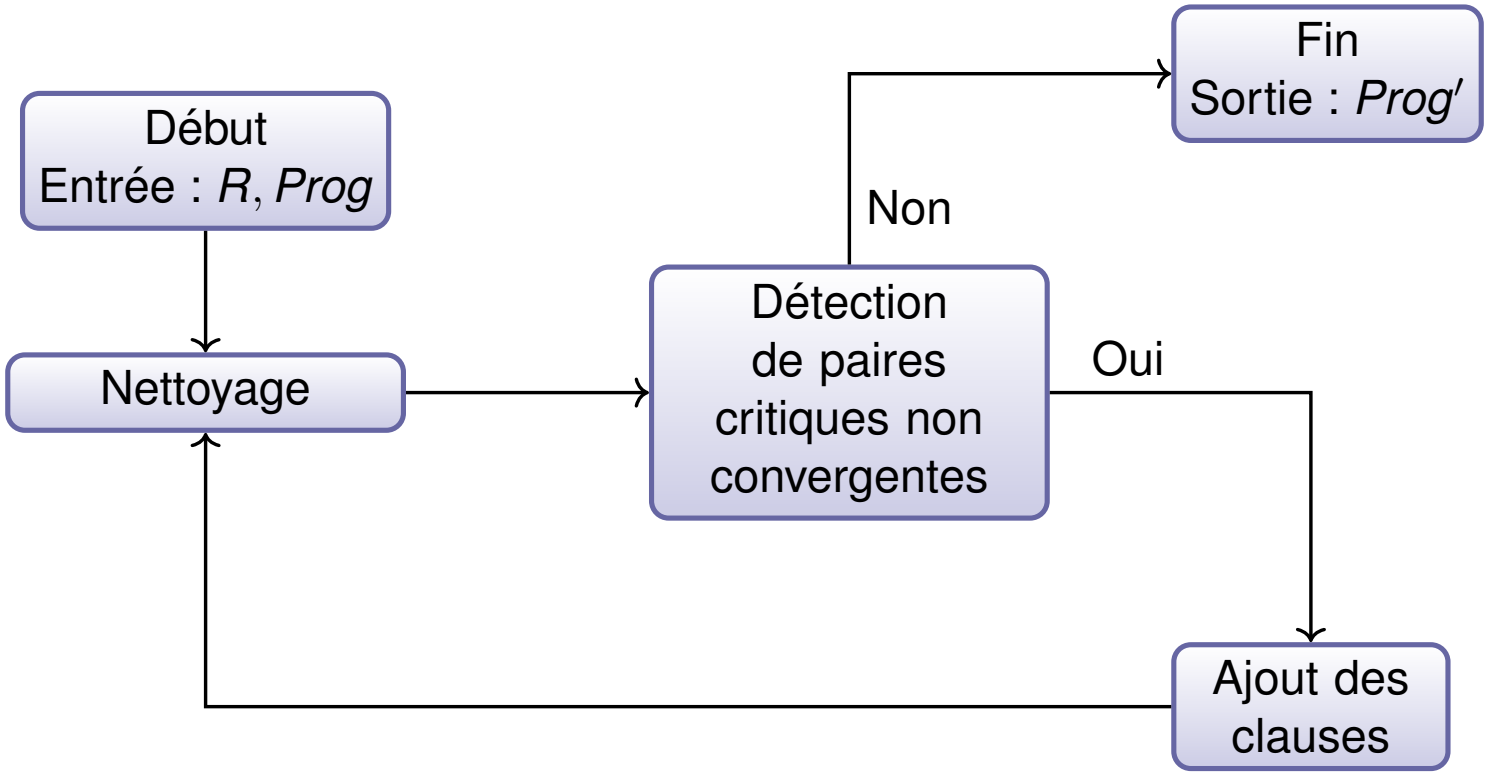
- Un CS-programme initial
  - non copiant

L'algorithme de complétion



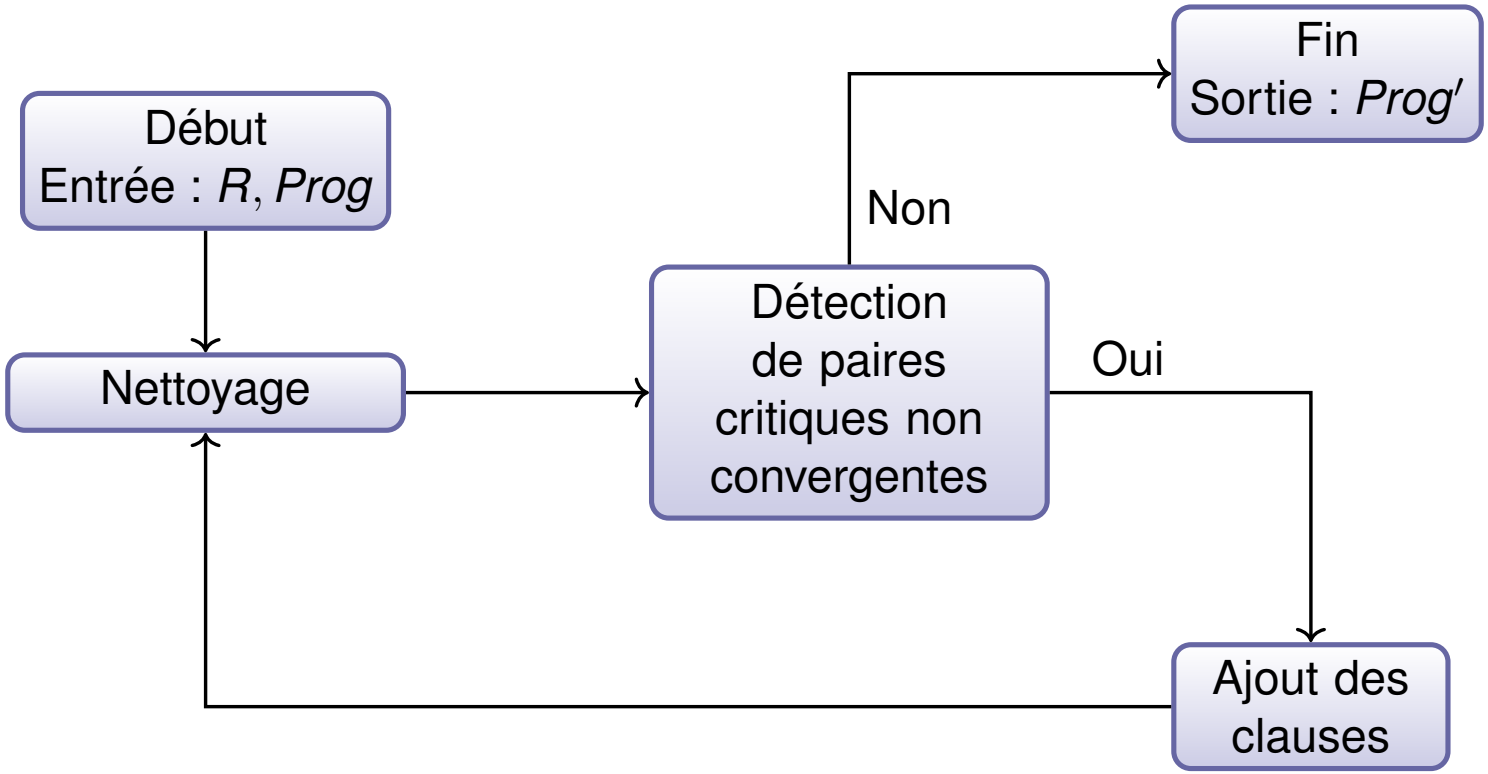
- Un CS-programme initial
  - non copiant
  - normalisé

L'algorithme de complétion



- Un CS-programme initial
  - non copiant
  - normalisé
- Un système de réécriture

L'algorithme de complétion



- Un CS-programme initial
  - non copiant
  - normalisé
- Un système de réécriture
  - linéaire gauche

Remarques et questions

Merci de votre attention