« Control and Observation of Real-Time Open Systems »

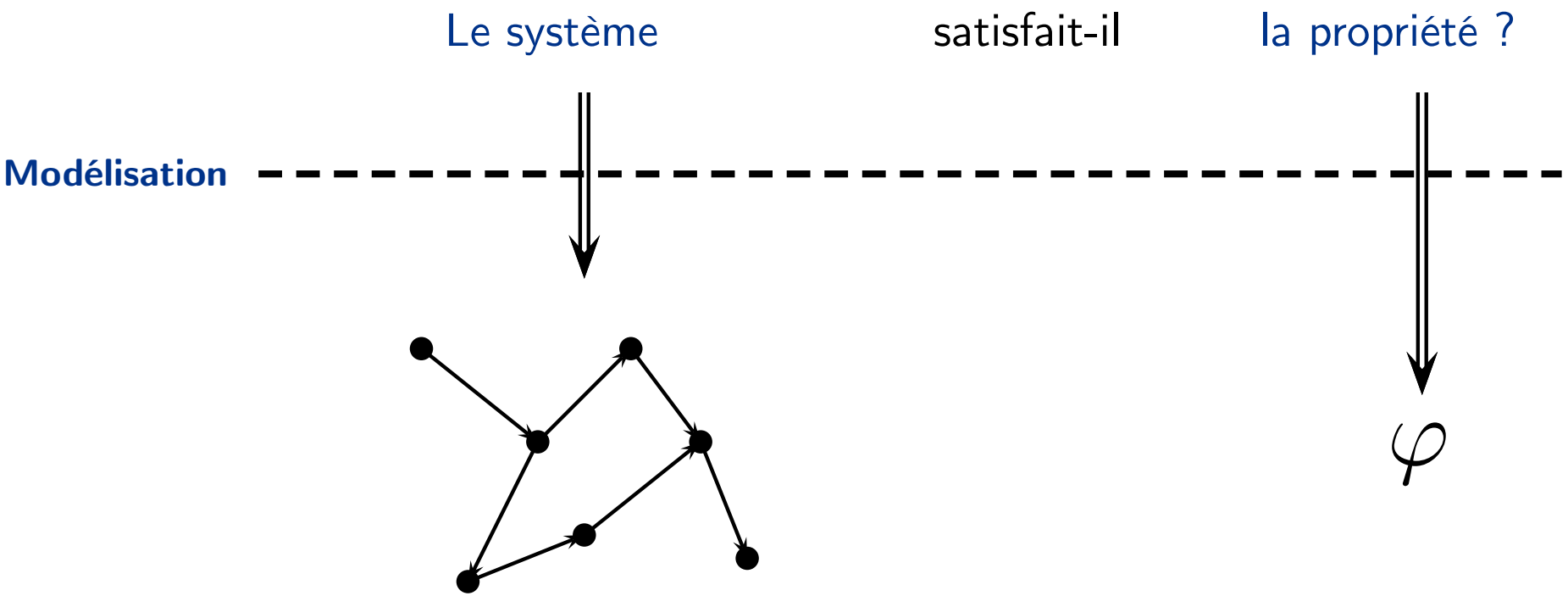
Projet de l'ACI Sécurité Informatique 2003

`http://www.lsv.ens-cachan.fr/aci-cortos/`

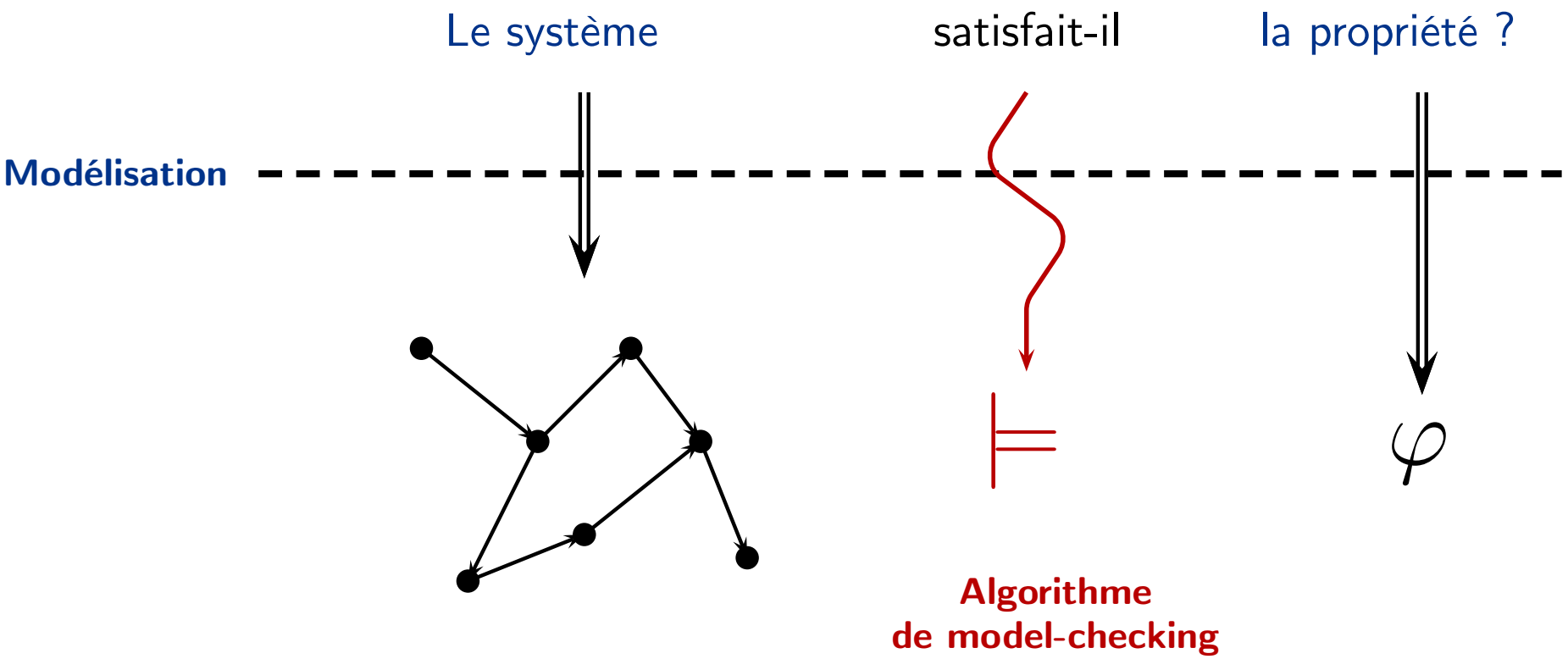
Personnes impliquées

IRCCyN (Nantes)	**LSV** (Cachan)	**VERIMAG** (Grenoble)
Franck Cassez	Béatrice Bérard	Karine Altisen
Julien D'Orso	Patricia Bouyer	Thao Dang
Guillaume Gardey	Laura Bozzelli	Moez Krichen
Didier Lime	Thierry Cachat	Stavros Tripakis
Olivier Roux	Fabrice Chevalier	
Olivier-Henri Roux	Stéphane Demri	
	François Laroussinie	
	Nicolas Markey	
	Pierre-Alain Reynier	

Le model-checking



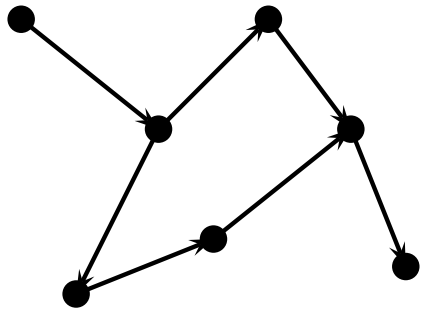
Le model-checking



La problématique du contrôle

Peut-on guider le système pour qu'il satisfasse la propriété ?

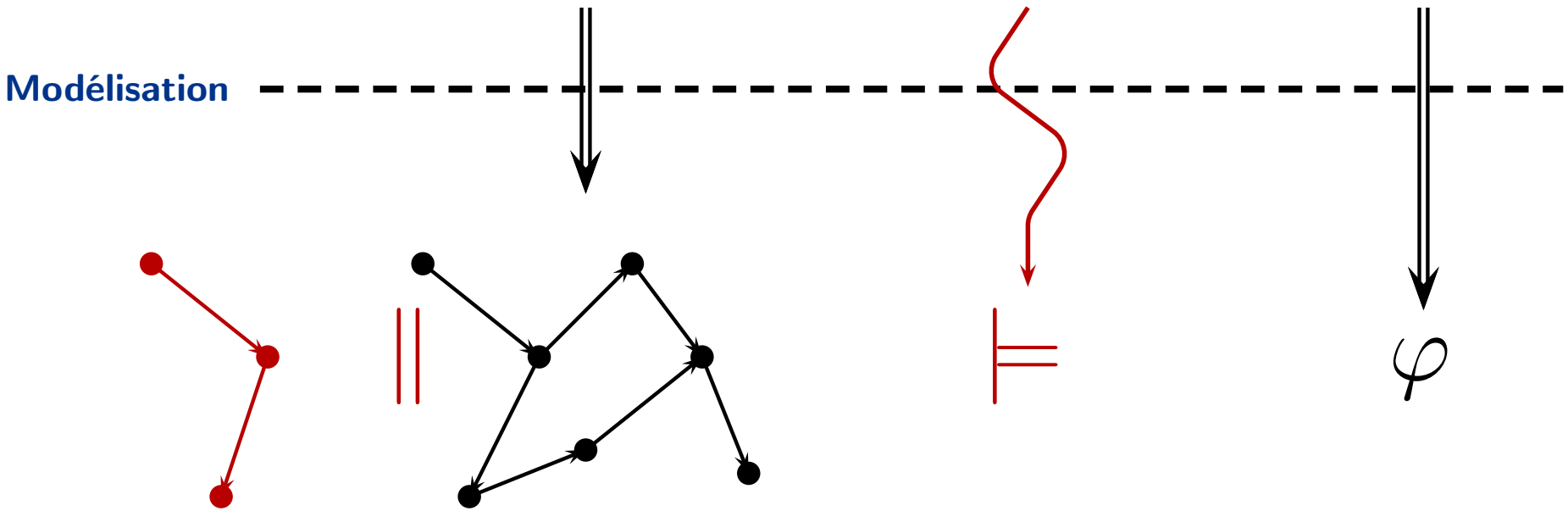
Modélisation



φ

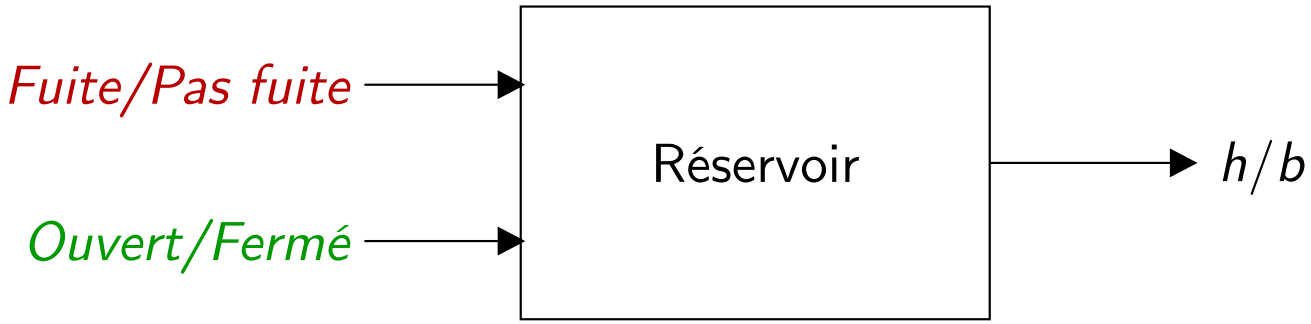
La problématique du contrôle

Peut-on guider le système pour qu'il satisfasse la propriété ?



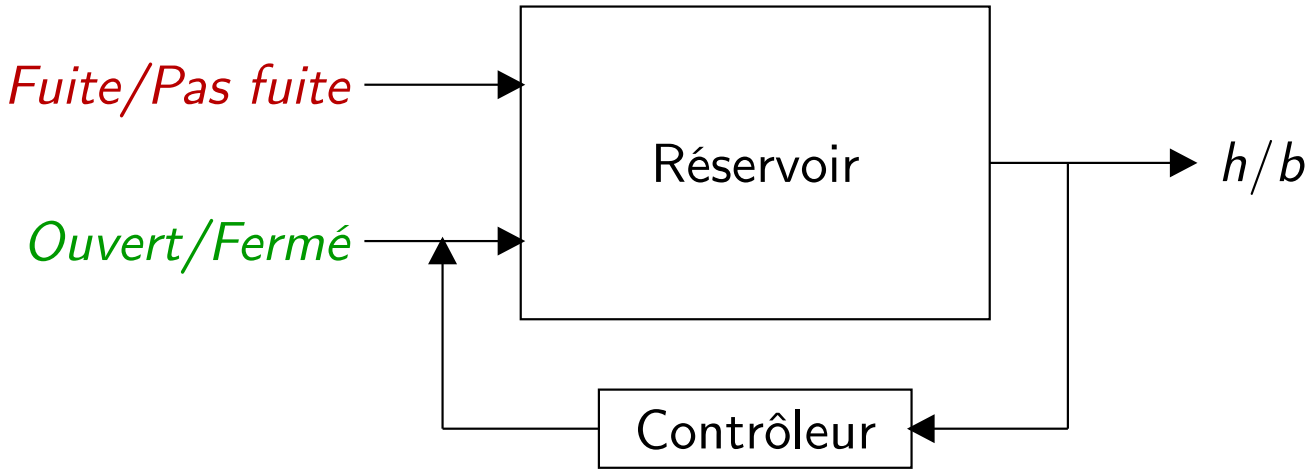
Synthèse de contrôleur

Le principe du contrôle illustré



- Système ouvert = système à contrôler
  Actions incontrôlables *vs* actions contrôlables
- **But :** guider le système pour que le niveau du réservoir soit toujours entre h et b
- Système fermé = système contrôlé

Le principe du contrôle illustré



- Système ouvert = système à contrôler
  Actions incontrôlables *vs* actions contrôlables
- **But :** guider le système pour que le niveau du réservoir soit toujours entre h et b
- Système fermé = système contrôlé

Les systèmes que nous considérons

- **systèmes temporisés**
  ex : modéliser des temps de réponse, des délais d'attente
  ➜ automates temporisés/hybrides, réseaux de Petri temporels

Les systèmes que nous considérons

- **systèmes temporisés**
  ex : modéliser des temps de réponse, des délais d'attente
  ➜ automates temporisés/hybrides, réseaux de Petri temporels

- **systèmes ouverts**
  ex : modéliser une interaction avec un environnement
  ➜ actions contrôlables/incontrôlables, jeux

Les systèmes que nous considérons

- **systèmes temporisés**
  ex : modéliser des temps de réponse, des délais d'attente
  ➜ automates temporisés/hybrides, réseaux de Petri temporels

- **systèmes ouverts**
  ex : modéliser une interaction avec un environnement
  ➜ actions contrôlables/incontrôlables, jeux

- **systèmes partiellement observables**
  ex : actions de l'environnement, actions internes...
  ➜ actions observables/inobservables

Les systèmes que nous considérons

- **systèmes temporisés**
  ex : modéliser des temps de réponse, des délais d'attente
  ➜ automates temporisés/hybrides, réseaux de Petri temporels

- **systèmes ouverts**
  ex : modéliser une interaction avec un environnement
  ➜ actions contrôlables/incontrôlables, jeux

- **systèmes partiellement observables**
  ex : actions de l'environnement, actions internes...
  ➜ actions observables/inobservables

- **systèmes avec contraintes de ressources**
  ex : énergie, coût...
  ➜ informations de coût, critères d'optimalité

Quelques-uns de nos résultats I

- Observation de systèmes
  - détection d'erreurs [Bouyer, Chevalier, D'Souza - FoSSaCS'05]
  - application au test de conformité [Krichen, Tripakis - SPIN'04, FORMATS'04, TESTCOM'05]
  - observation distribuée [Tripakis - IPL 2004, ACSD'05]
- Contrôle des réseaux de Petri temporels
  - ordonnancement de tâches [Lime, Roux - RTSS'04, ICATPN'04]
  - décidabilité du contrôle de sûreté [Gardey, Roux - En soumission]
- Contrôle temporisé optimal
  - traces infinies optimales [Bouyer, Brinksma, Larsen - HSCC'04]
  - jeux temporisés d'accessibilité optimaux [Bouyer, Cassez, Fleury, Larsen - FSTTCS'04]
  - indécidabilité du contrôle optimal [Bouyer, Brihaye, Markey - En soumission]
- Contrôle sur les ω-séquences [Demri, Nowak - ATVA'05]
- Contrôle des systèmes hybrides o-minimaux [Bouyer, Brihaye, Chevalier - En soumission]

Quelques-uns de nos résultats II

- Implémentabilité des systèmes temporisés
  - un point de vue de modélisation [Altisen, Tripakis - FORMATS'05]
  - un point de vue sémantique
    - pure "safety" [De Wulf, Doyen, Markey, Raskin - FORMATS'04]
    - propriétés linéaires (LTL) [Bouyer, Markey, Reynier - LATIN'06]
- Algorithmes et outils pour le contrôle temporisé
  - algorithme en-avant $\longrightarrow$ TiGa (extension de Uppaal) [Cassez, David, Fleury, Lime, Larsen - CONCUR'05]
  - logique modale pour le contrôle $\longrightarrow$ CMC [Bouyer, Cassez, Laroussinie - CONCUR'05]
  - contrôle des RdP temporels $\longrightarrow$ Roméo + HyTech [Gardey, Roux]
  - contrôle optimal $\longrightarrow$ HyTech [Bouyer, Cassez, Fleury, Larsen - GDV'04]
- Applications du contrôle temporisé
  - ordonnancement de programmes temps-réels multithreads avec de la géométrie [Dang, Gerner - FORMATS'04]
  - "aspect oriented programming" [Altisen, Maraninchi, Stauch - FOAL'04]

Contrôle des réseaux de Petri temporels

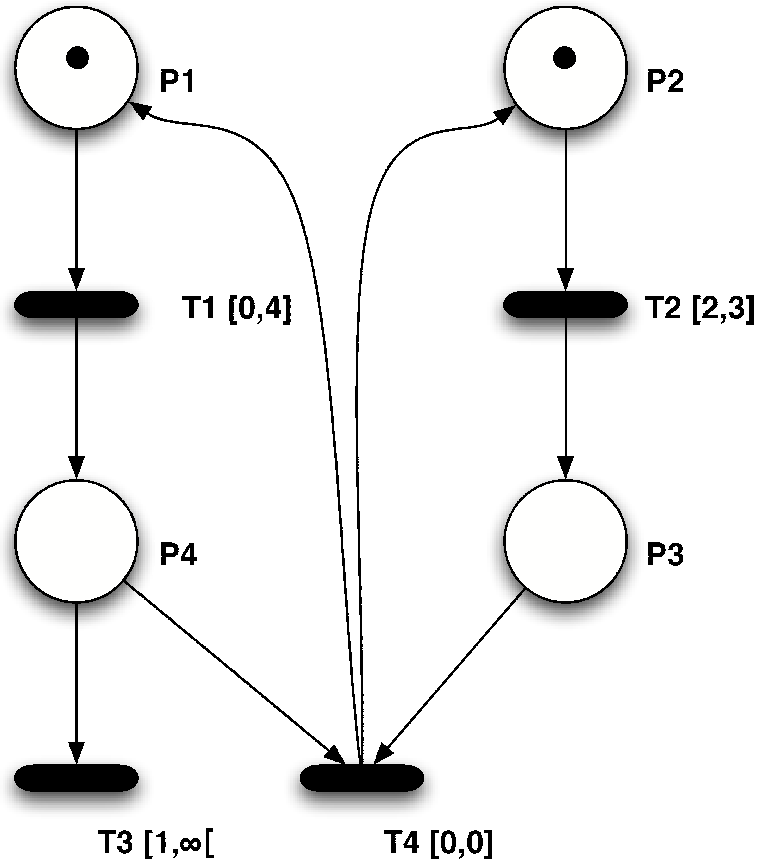
[Gardey, Roux - En soumission]

- Le contrôle des réseaux de Petri temporels pour des propriétés de sûreté bornées est décidable.

Exemple :

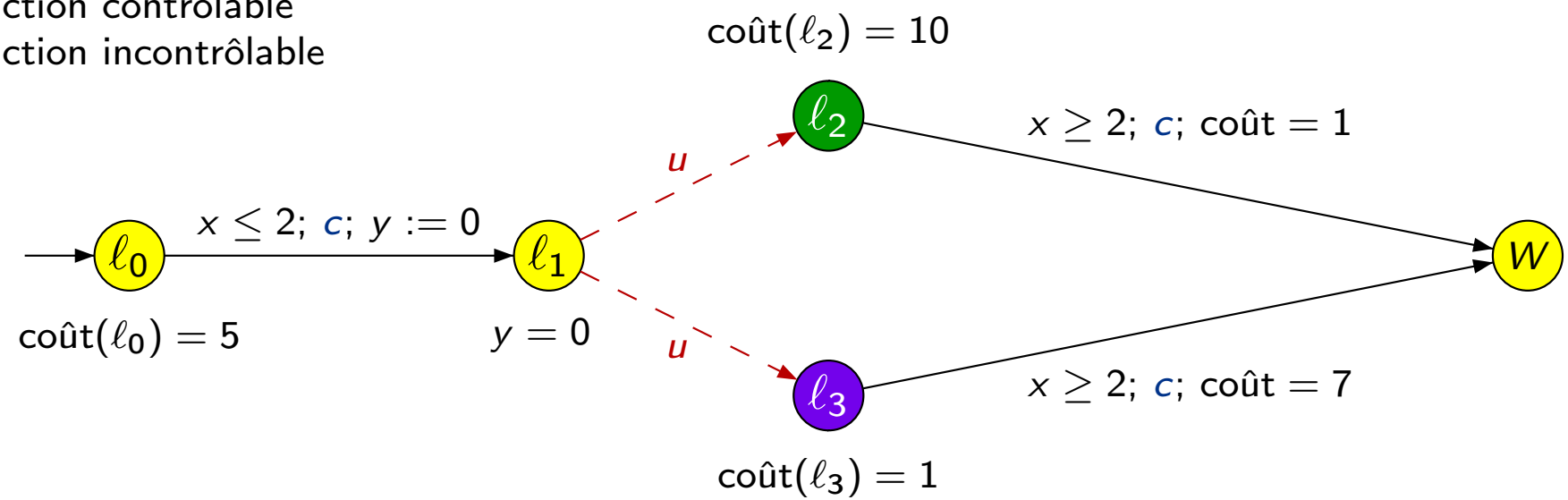
- $T_c = \{T_1\}$
- empêcher le tirage de T_3 :

$$M(P_1)+M(P_2)+M(P_3)+M(P_4) = 2$$



Contrôle optimal, un exemple

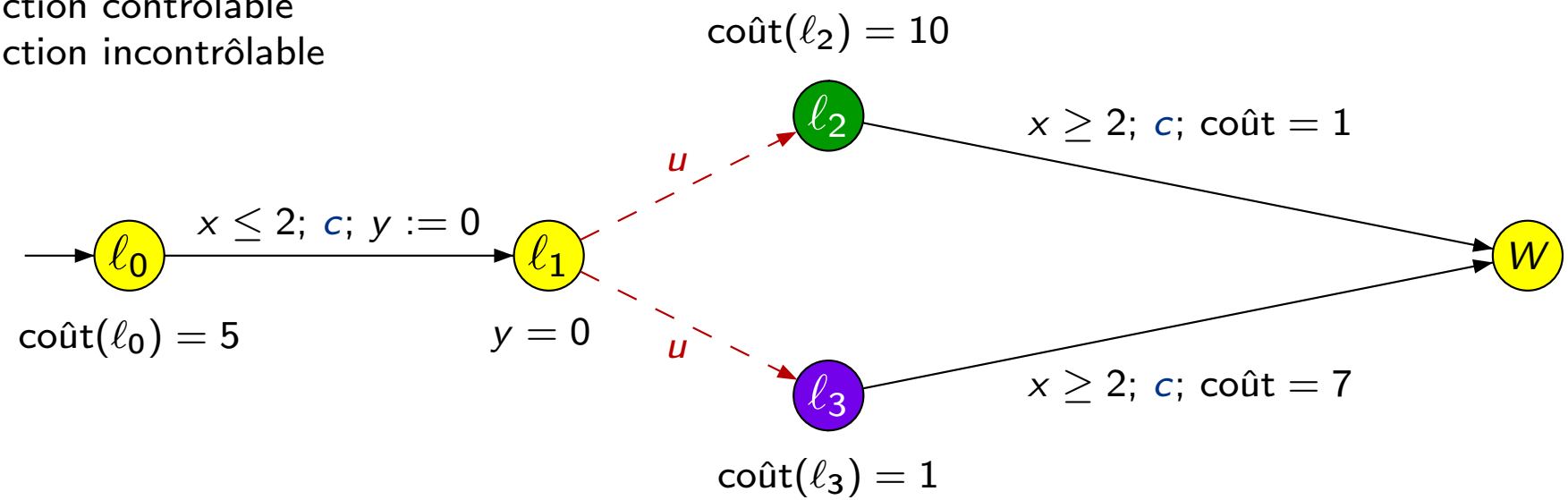
c: action contrôlable
u: action incontrôlable



Question: quel est le coût optimal que l'on peut assurer dans l'état ℓ_0 ?

Contrôle optimal, un exemple

c: action contrôlable
u: action incontrôlable

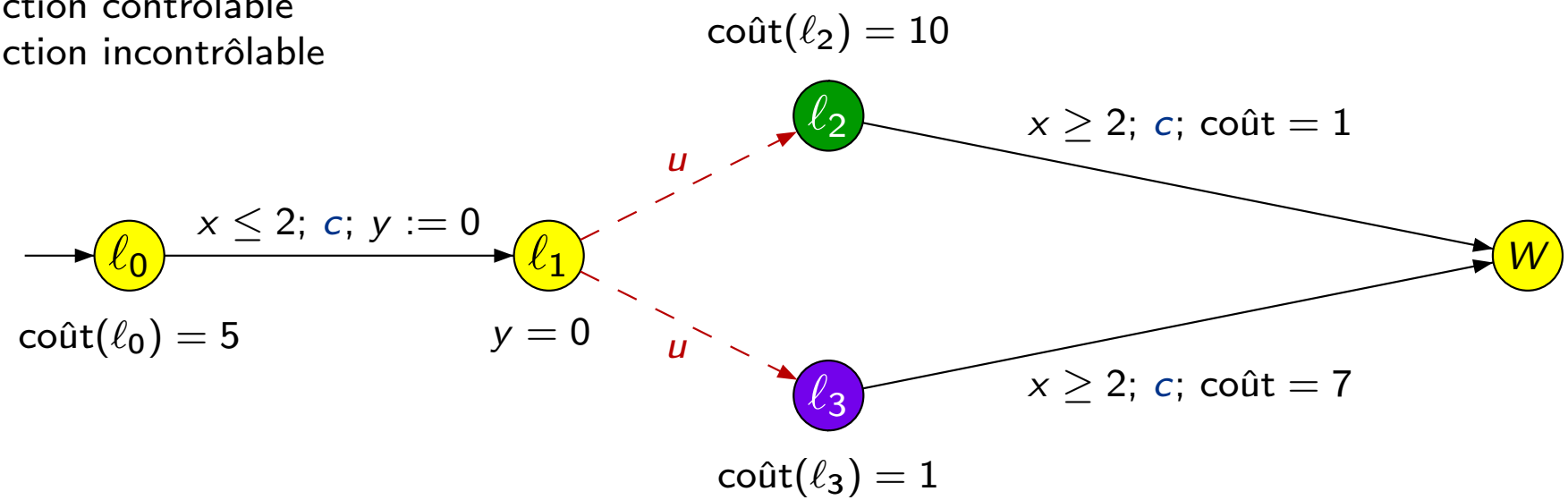


Question: quel est le coût optimal que l'on peut assurer dans l'état ℓ_0 ?

$$5t + 10(2 - t) + 1$$

Contrôle optimal, un exemple

c: action contrôlable
u: action incontrôlable

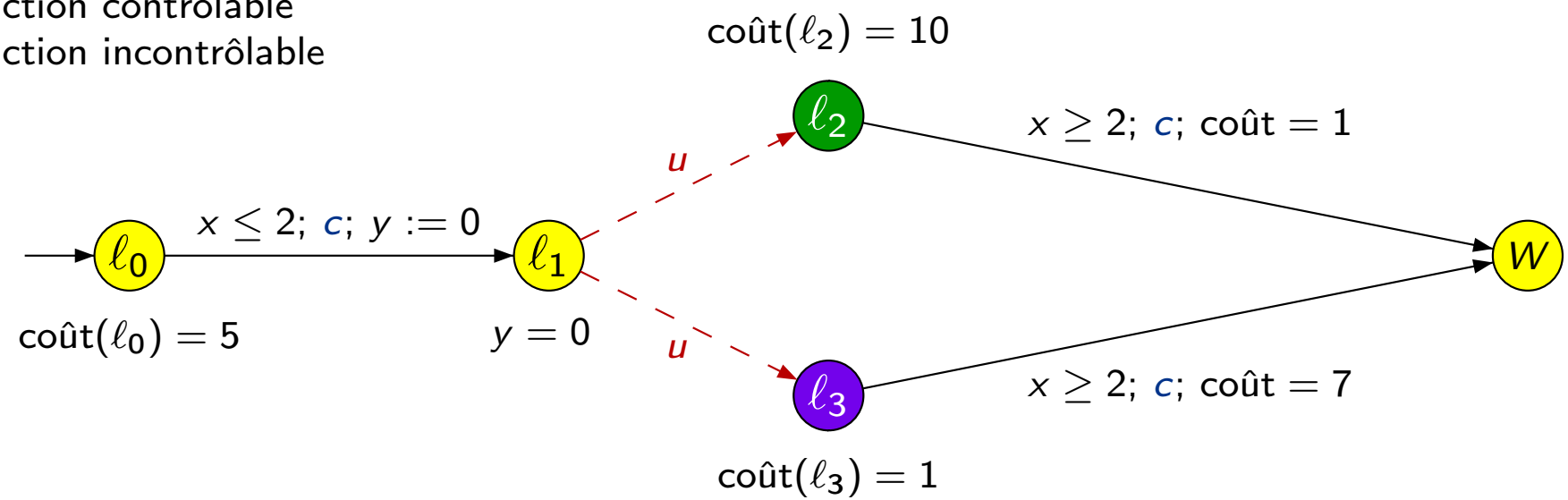


Question: quel est le coût optimal que l'on peut assurer dans l'état ℓ_0 ?

$$5t + 10(2 - t) + 1 \ , \ 5t + (2 - t) + 7$$

Contrôle optimal, un exemple

c: action contrôlable
u: action incontrôlable

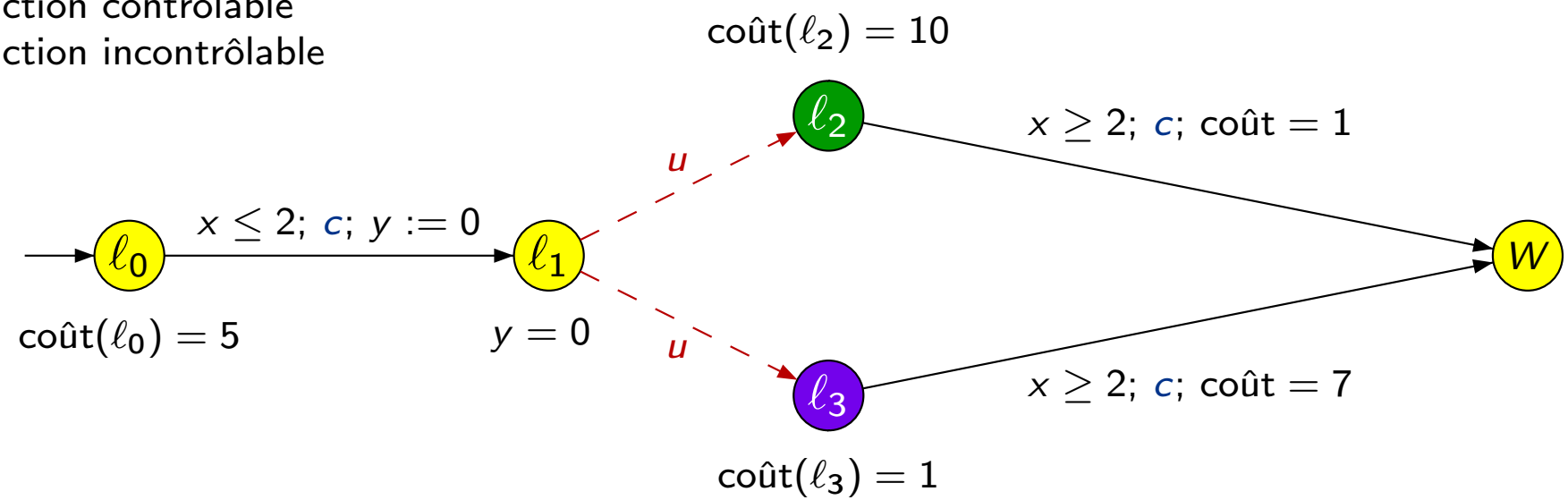


Question: quel est le coût optimal que l'on peut assurer dans l'état ℓ_0 ?

$$\max\ (\ 5t + 10(2-t) + 1\ ,\ 5t + (2-t) + 7\ )$$

Contrôle optimal, un exemple

c: action contrôlable
u: action incontrôlable

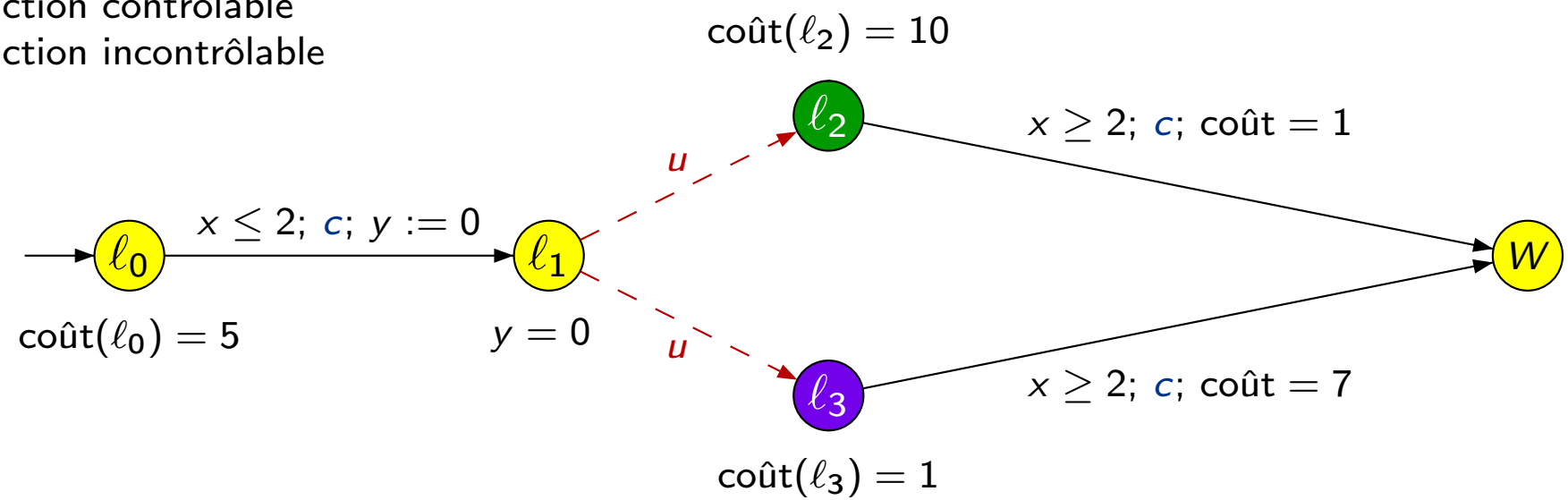


Question: quel est le coût optimal que l'on peut assurer dans l'état ℓ_0 ?

$$\inf_{0 \leq t \leq 2} \max\left(5t + 10(2-t) + 1 \ , \ 5t + (2-t) + 7 \right) = 14 + \frac{1}{3}$$

Contrôle optimal, un exemple

c: action contrôlable
u: action incontrôlable



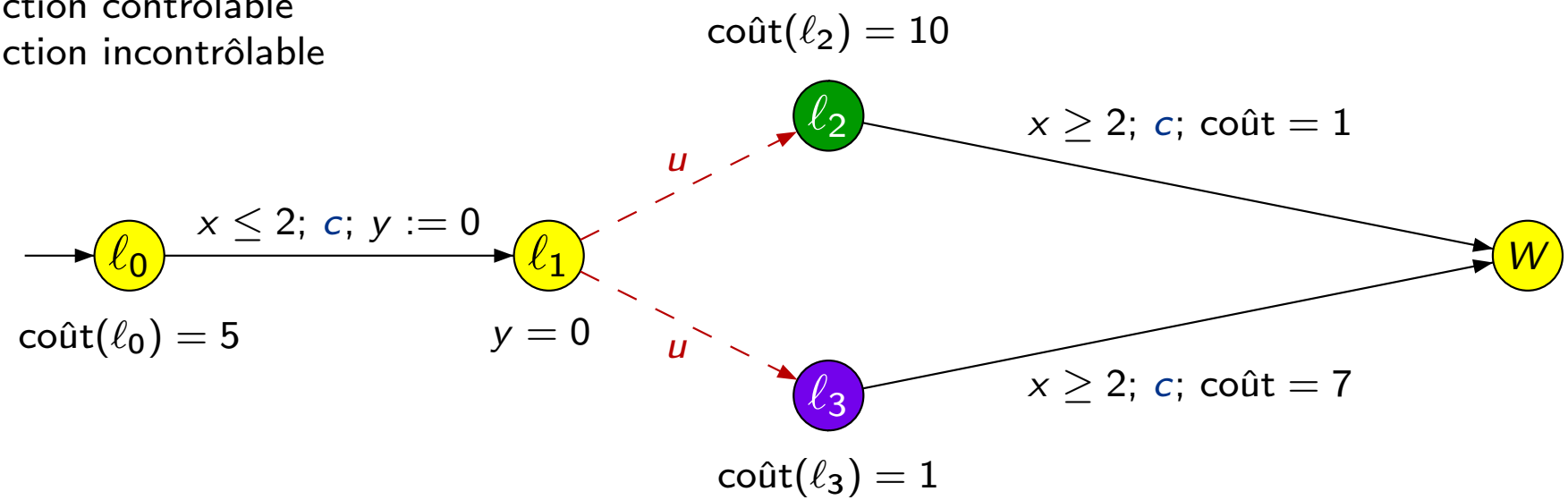
Question: quel est le coût optimal que l'on peut assurer dans l'état ℓ_0 ?

$$\inf_{0 \leq t \leq 2} \max\left(5t + 10(2-t) + 1 \ , \ 5t + (2-t) + 7 \right) = 14 + \frac{1}{3}$$

➜ **stratégie :** attendre en ℓ_0 et lorsque $t = \frac{4}{3}$, aller en ℓ_1

Contrôle optimal, un exemple

c: action contrôlable
u: action incontrôlable



Question: quel est le coût optimal que l'on peut assurer dans l'état ℓ_0 ?

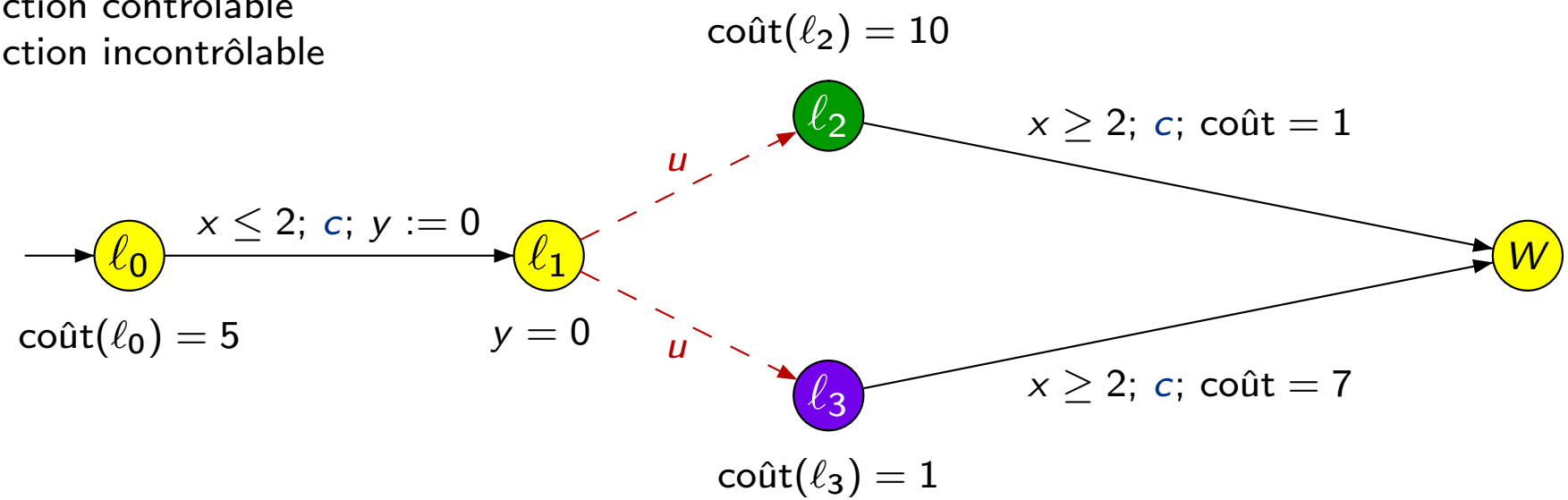
$$\inf_{0 \leq t \leq 2} \max\left(5t + 10(2-t) + 1 \ , \ 5t + (2-t) + 7 \right) = 14 + \frac{1}{3}$$

➜ **stratégie :** attendre en ℓ_0 et lorsque $t = \frac{4}{3}$, aller en ℓ_1

- Comment calculer automatiquement les coûts optimaux ?

Contrôle optimal, un exemple

c: action contrôlable
u: action incontrôlable



Question: quel est le coût optimal que l'on peut assurer dans l'état ℓ_0 ?

$$\inf_{0 \leq t \leq 2} \max\left(5t + 10(2-t) + 1 \ , \ 5t + (2-t) + 7 \right) = 14 + \frac{1}{3}$$

➜ **stratégie :** attendre en ℓ_0 et lorsque $t = \frac{4}{3}$, aller en ℓ_1

- Comment calculer automatiquement les coûts optimaux ?
- Comment synthétiser des stratégies optimales (lorsqu'il en existe) ?

Un domaine actif...

- [Asarin, Maler - HSCC'99]:
  - optimal time is computable in timed games

Un domaine actif...

- [Asarin, Maler - HSCC'99]:
  - optimal time is computable in timed games
- [La Torre, Mukhopadhyay, Murano - TCS'02]:
  - case of acyclic games

Un domaine actif...

- [Asarin, Maler - HSCC'99]:
  - optimal time is computable in timed games
- [La Torre, Mukhopadhyay, Murano - TCS'02]:
  - case of acyclic games
- [Alur, Bernadsky, Madhusudan - ICALP'04]:
  - k-step games can be solved in exponential time and may need an exponential number of splittings
  - under a strongly non-*zeno* assumption, optimal cost is computable

Un domaine actif...

- [Asarin, Maler - HSCC'99]:
  - optimal time is computable in timed games
- [La Torre, Mukhopadhyay, Murano - TCS'02]:
  - case of acyclic games
- [Alur, Bernadsky, Madhusudan - ICALP'04]:
  - k-step games can be solved in exponential time and may need an exponential number of splittings
  - under a strongly non-*zeno* assumption, optimal cost is computable
- [Bouyer, Cassez, Fleury, Larsen - FSTTCS'04] :
  - structural properties of strategies: may need memory, state-based strategies for a subclass of games
  - under a strongly non-*zeno* assumption, optimal cost is computable

Un domaine actif...

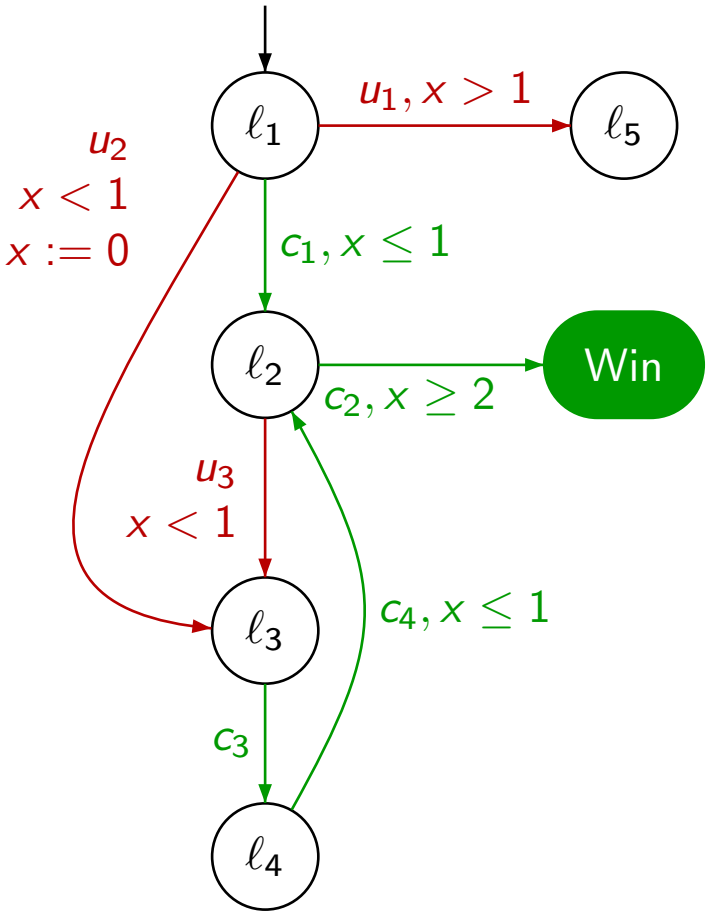
- [Asarin, Maler - HSCC'99]:
  - optimal time is computable in timed games
- [La Torre, Mukhopadhyay, Murano - TCS'02]:
  - case of acyclic games
- [Alur, Bernadsky, Madhusudan - ICALP'04]:
  - k-step games can be solved in exponential time and may need an exponential number of splittings
  - under a strongly non-*zeno* assumption, optimal cost is computable
- [Bouyer, Cassez, Fleury, Larsen - FSTTCS'04] :
  - structural properties of strategies: may need memory, state-based strategies for a subclass of games
  - under a strongly non-*zeno* assumption, optimal cost is computable
- [Brihaye, Bruyère, Raskin - FORMATS'05]:
  - with five clocks, optimal cost is not computable!
  - with one clock and one stopwatch cost, optimal cost is computable

Un domaine actif...

- [Asarin, Maler - HSCC'99]:
  - optimal time is computable in timed games
- [La Torre, Mukhopadhyay, Murano - TCS'02]:
  - case of acyclic games
- [Alur, Bernadsky, Madhusudan - ICALP'04]:
  - k-step games can be solved in exponential time and may need an exponential number of splittings
  - under a strongly non-*zeno* assumption, optimal cost is computable
- [Bouyer, Cassez, Fleury, Larsen - FSTTCS'04] :
  - structural properties of strategies: may need memory, state-based strategies for a subclass of games
  - under a strongly non-*zeno* assumption, optimal cost is computable
- [Brihaye, Bruyère, Raskin - FORMATS'05]:
  - with five clocks, optimal cost is not computable!
  - with one clock and one stopwatch cost, optimal cost is computable
- [Bouyer, Brihaye, Markey - Soumis à IPL, 2005] :
  - with three clocks, optimal cost is not computable

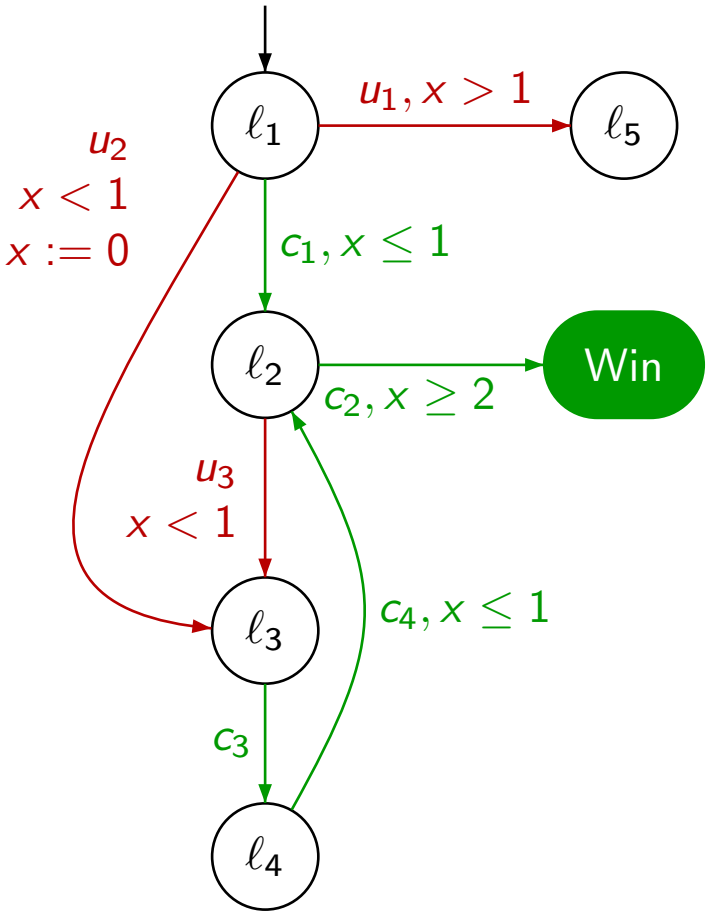
Algorithme en avant pour les états gagnants

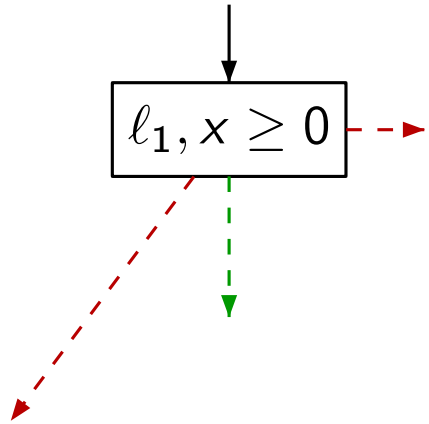
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]



Algorithme en avant pour les états gagnants

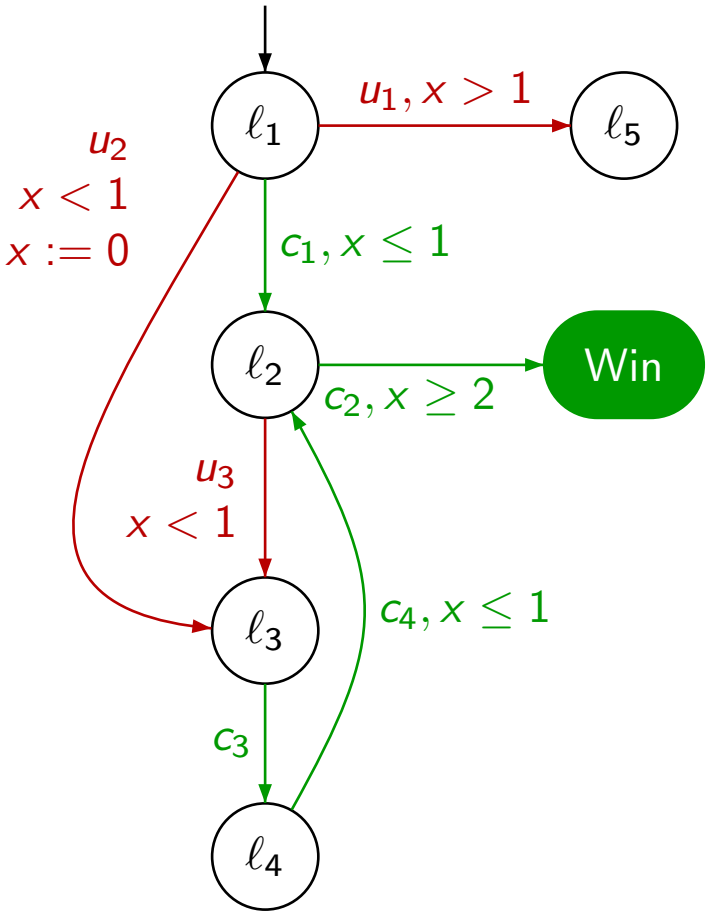
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

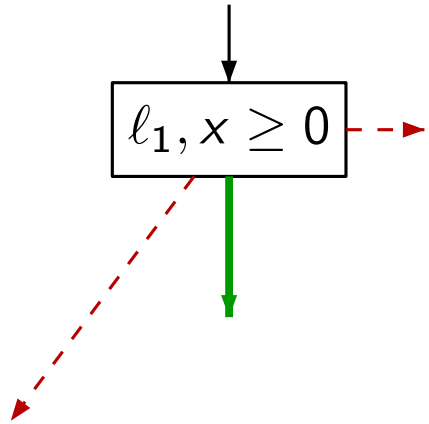




Algorithme en avant pour les états gagnants

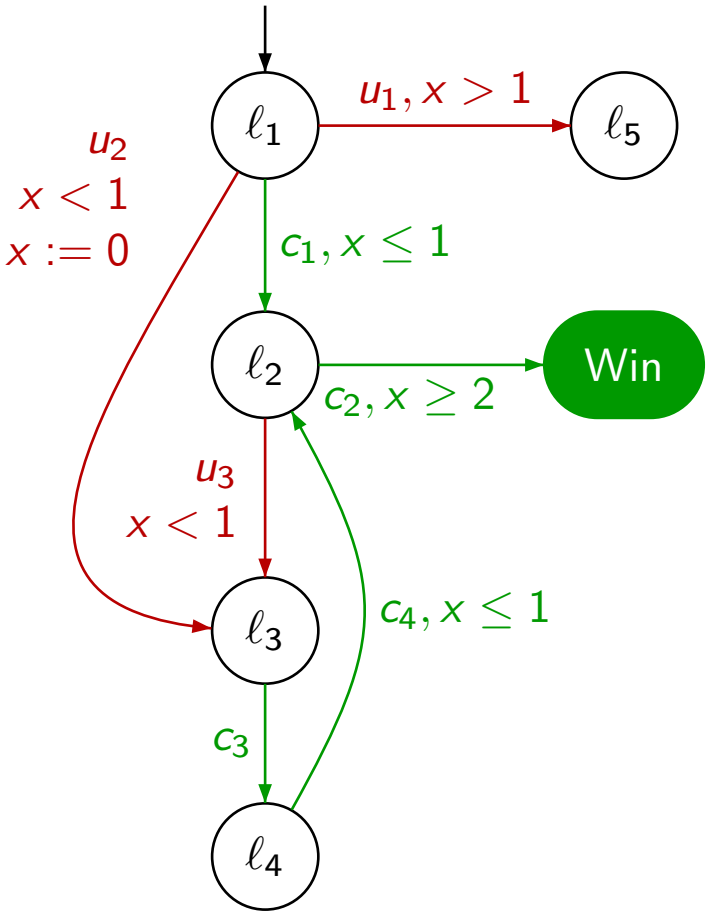
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

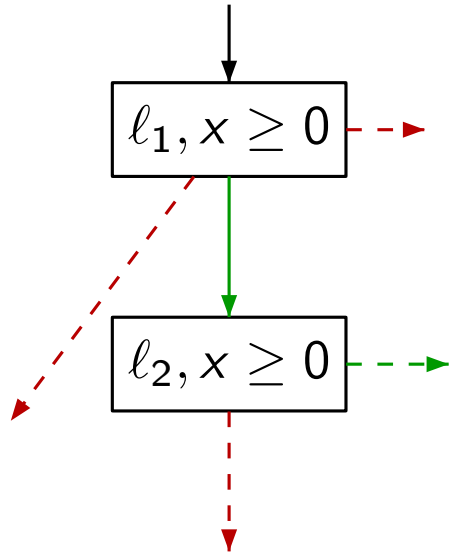




Algorithme en avant pour les états gagnants

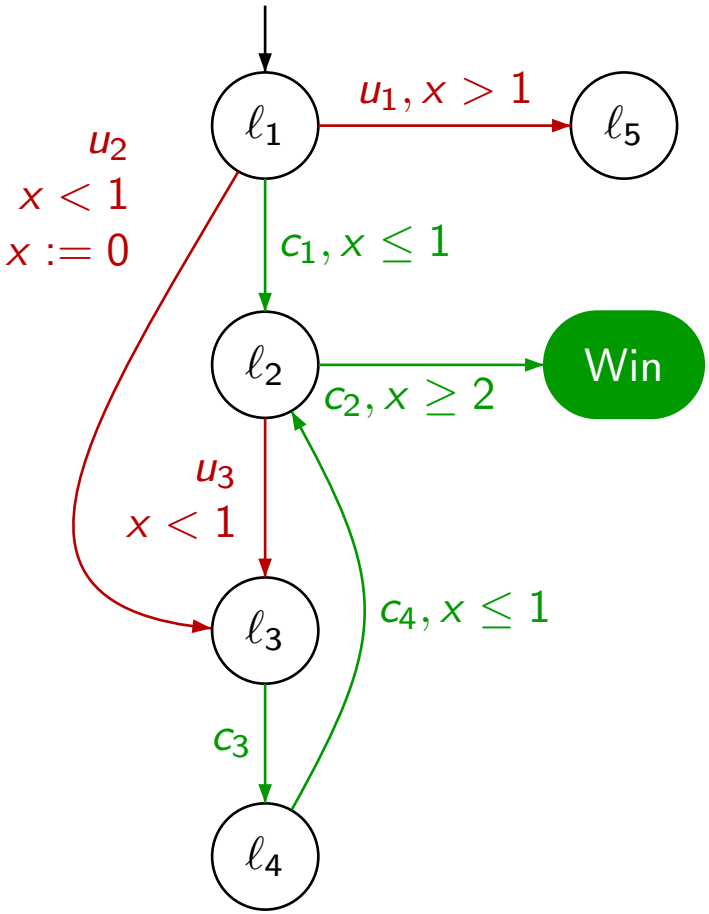
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

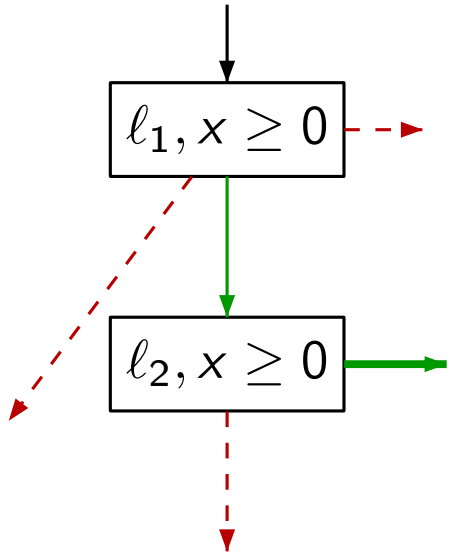




Algorithme en avant pour les états gagnants

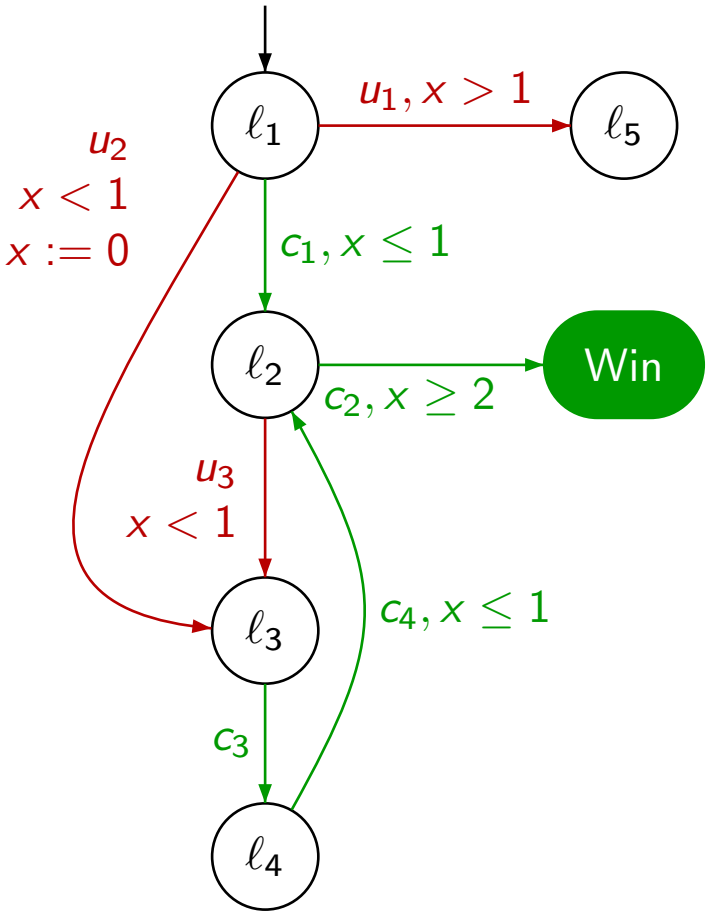
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

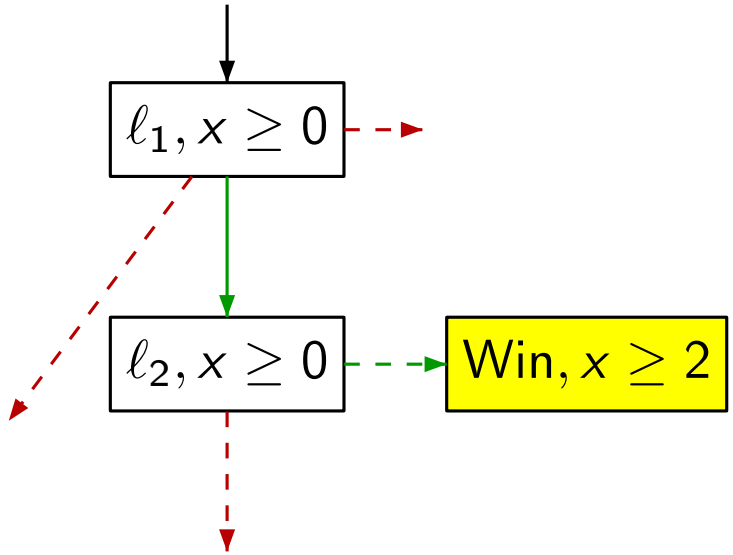




Algorithme en avant pour les états gagnants

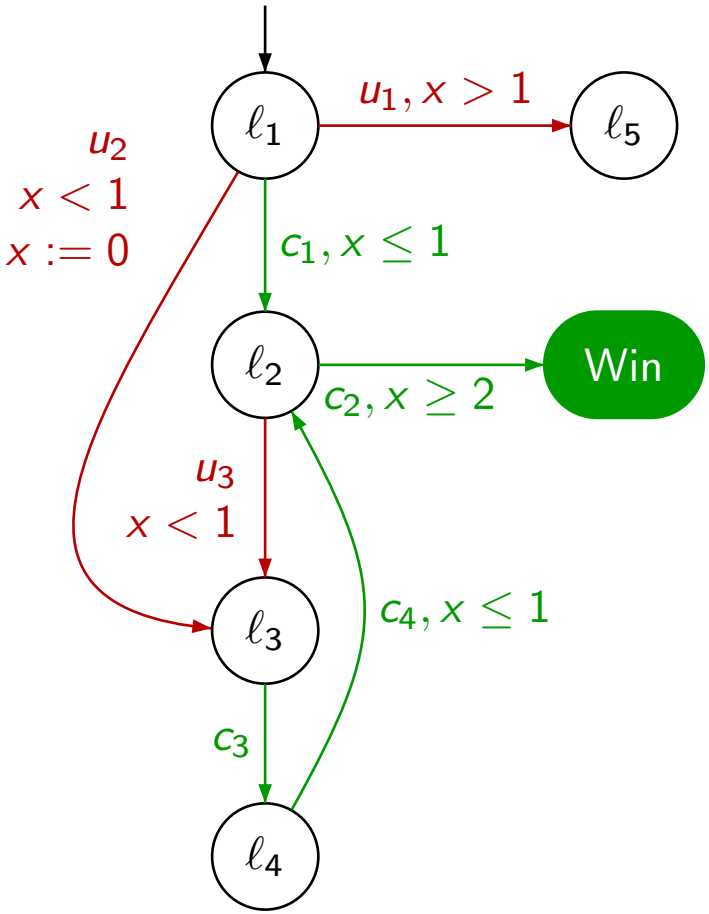
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

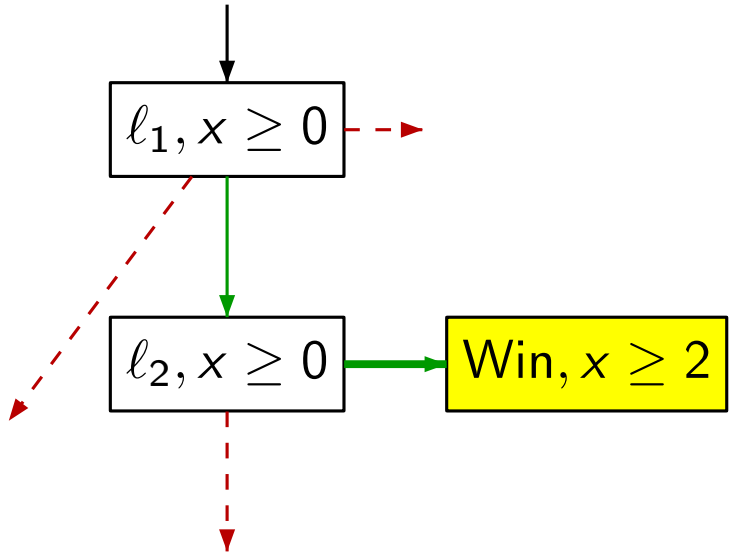




Algorithme en avant pour les états gagnants

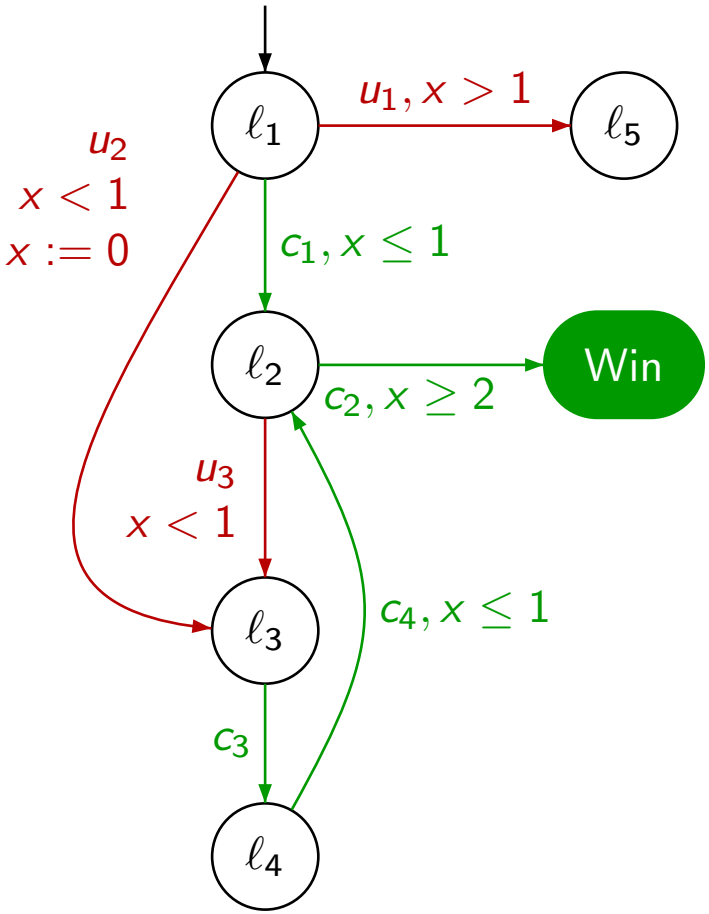
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

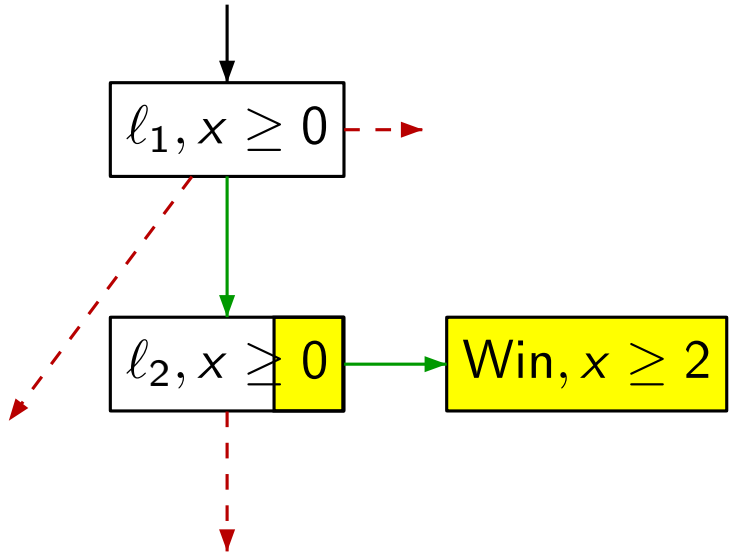




Algorithme en avant pour les états gagnants

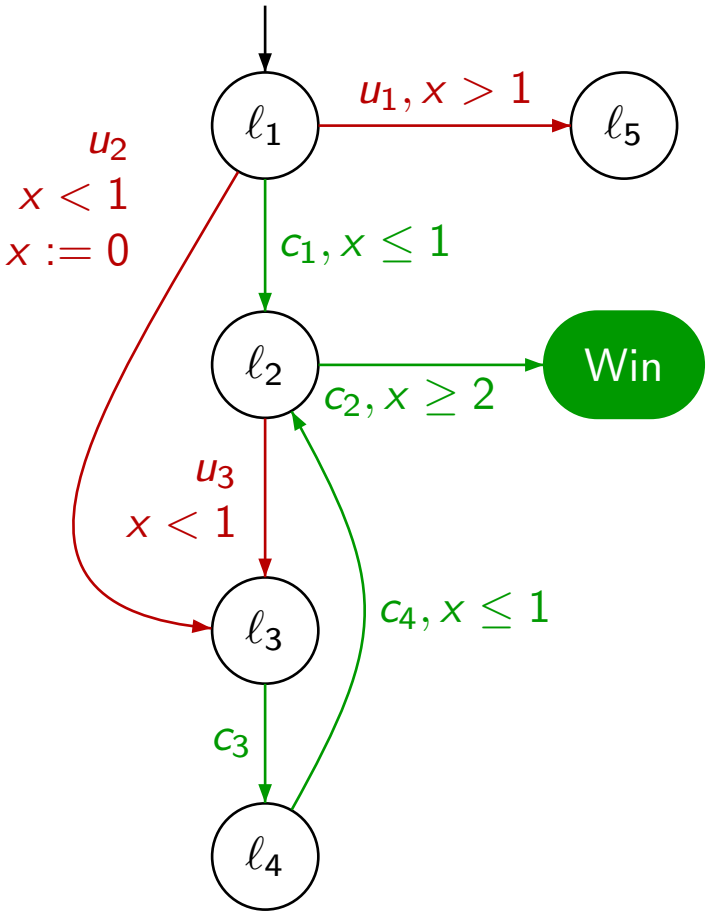
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

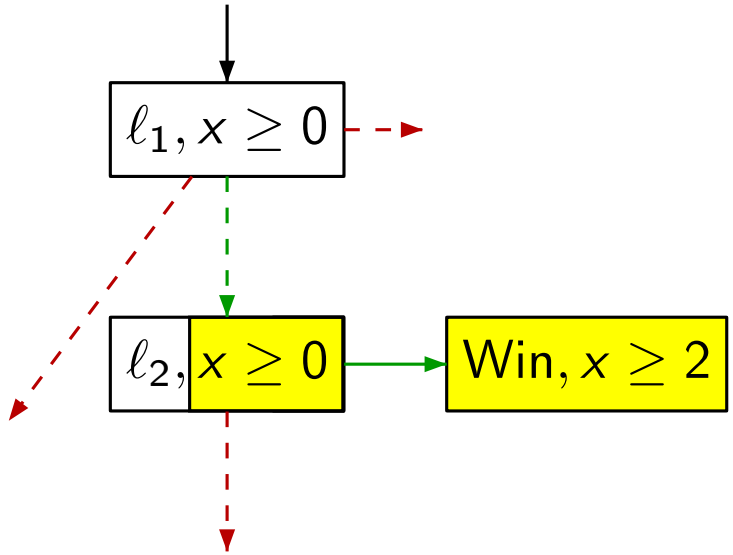




Algorithme en avant pour les états gagnants

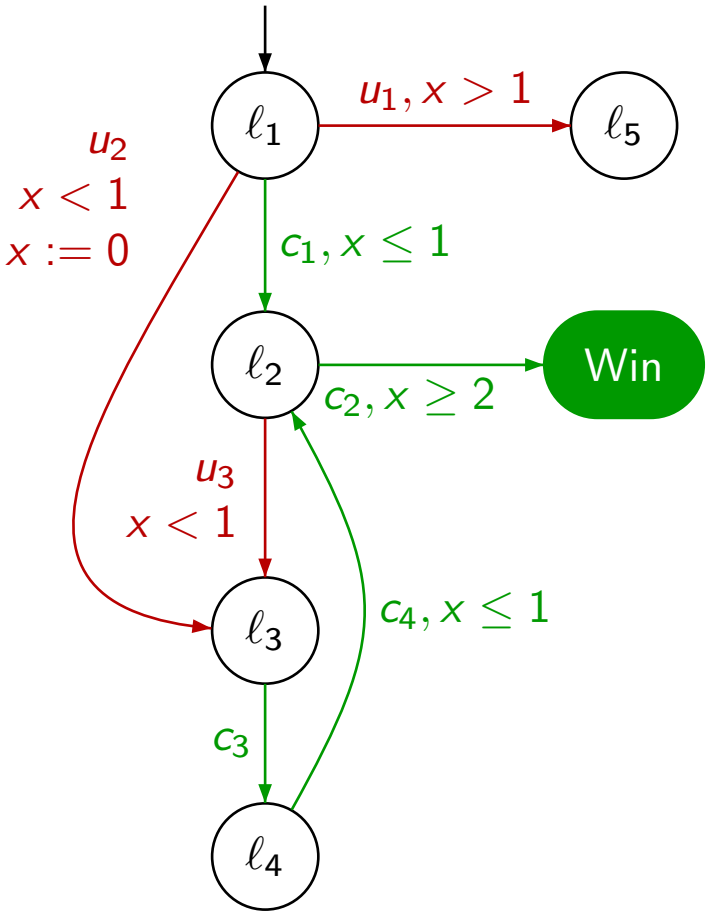
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

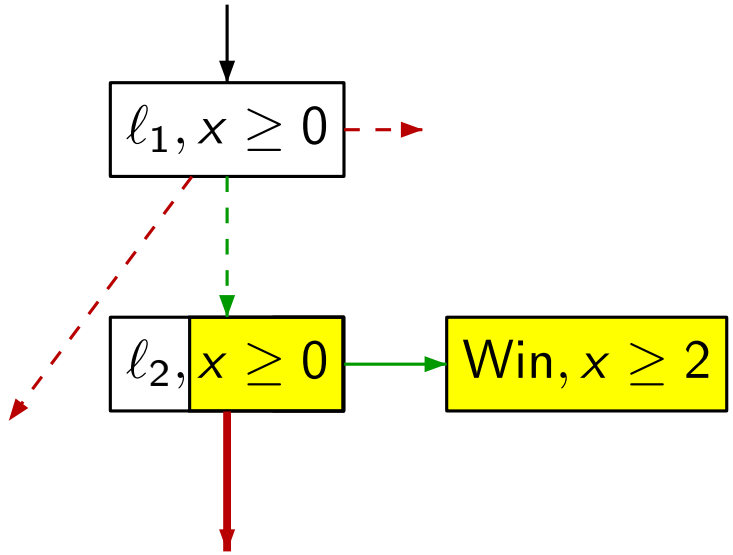




Algorithme en avant pour les états gagnants

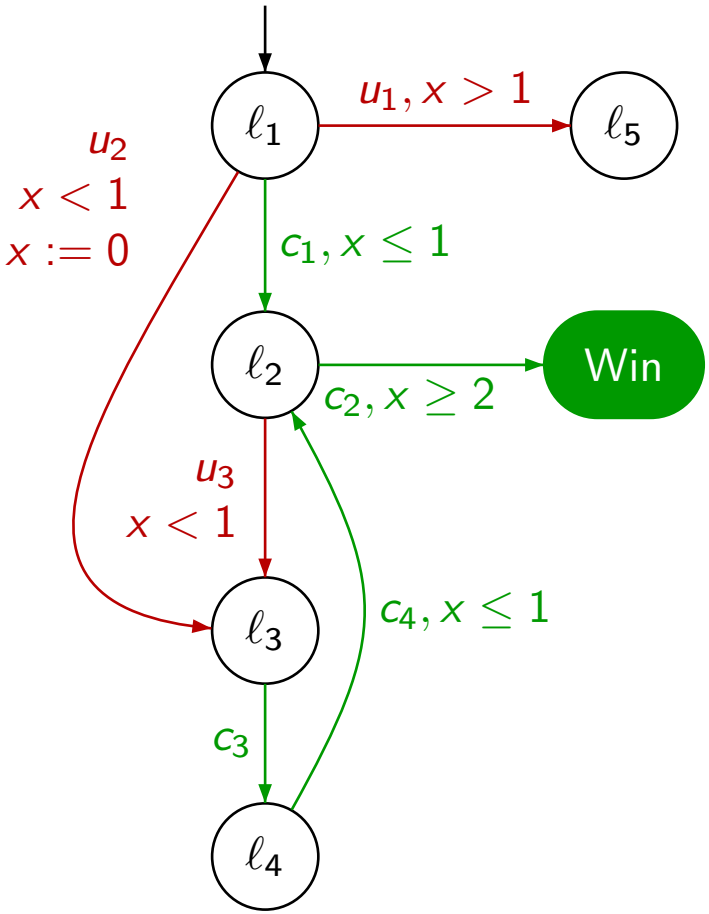
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

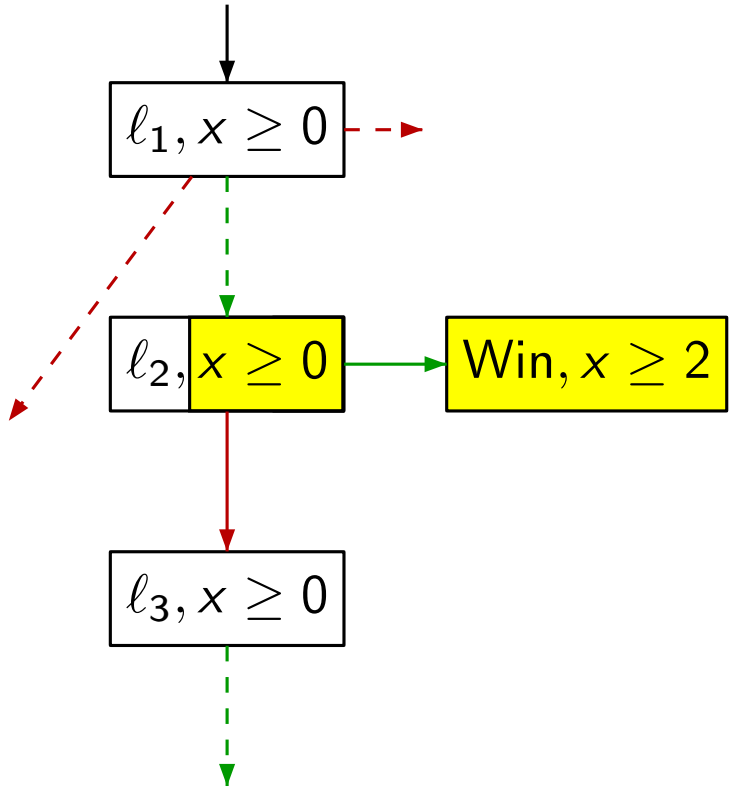




Algorithme en avant pour les états gagnants

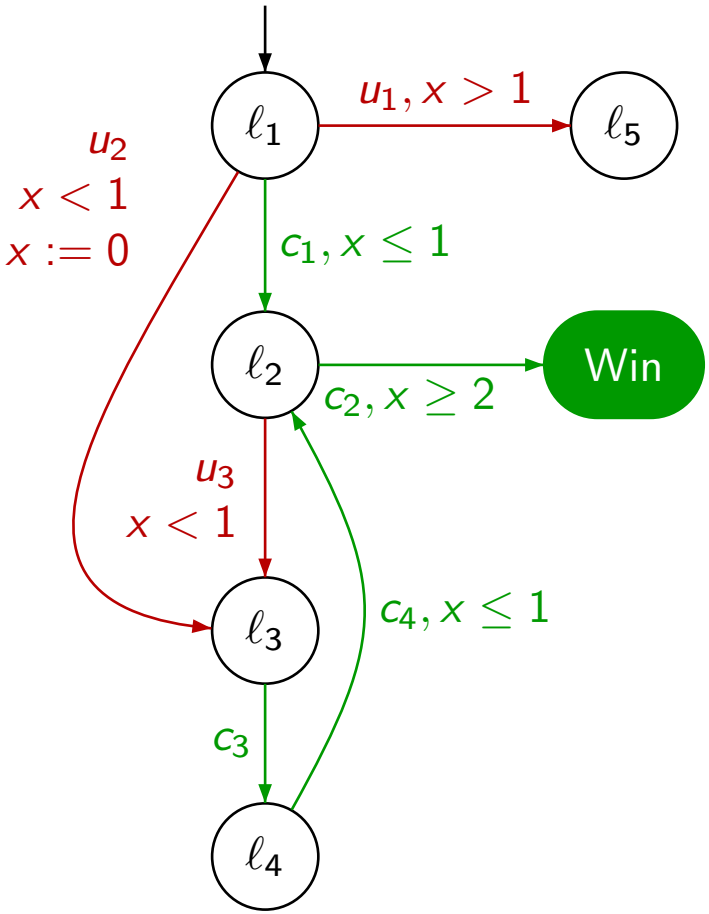
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

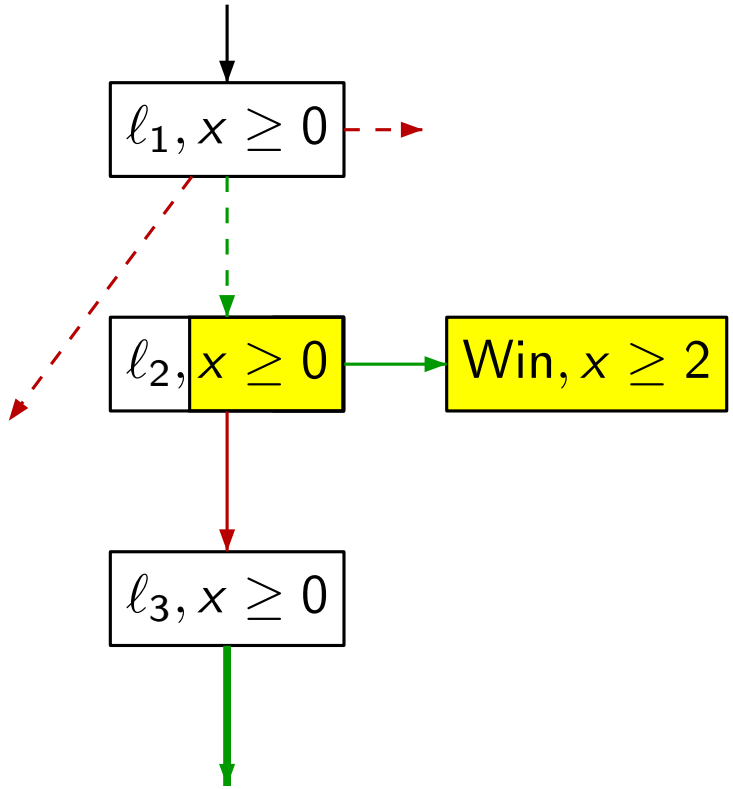




Algorithme en avant pour les états gagnants

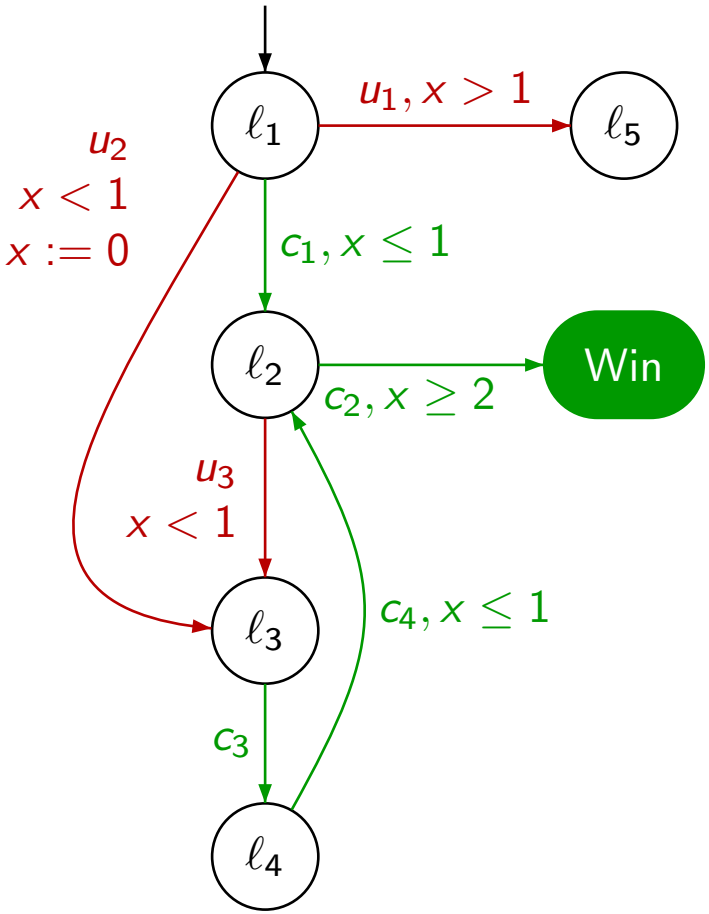
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

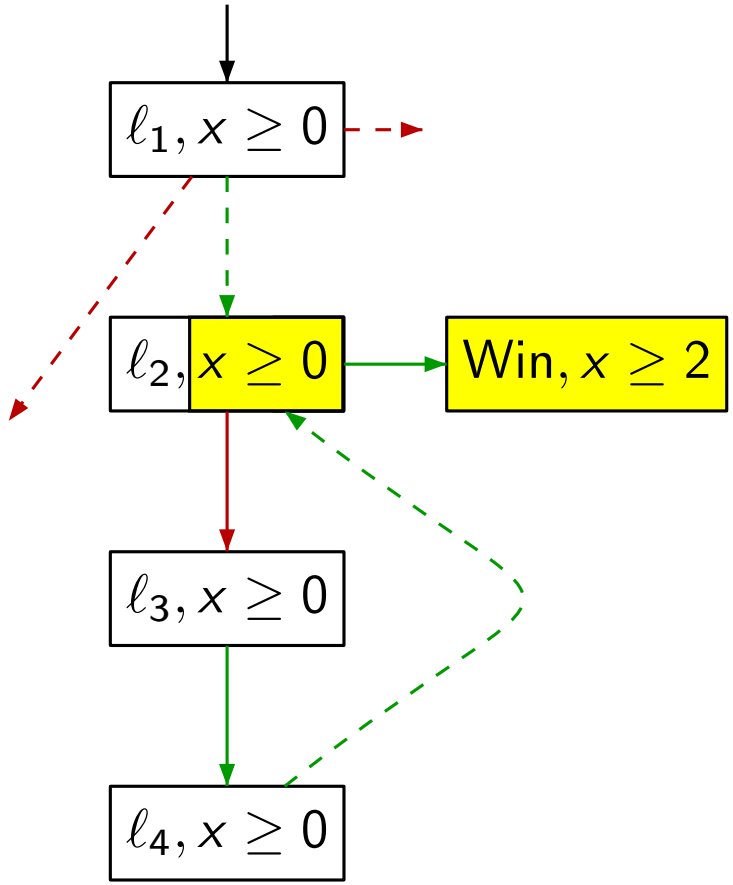




Algorithme en avant pour les états gagnants

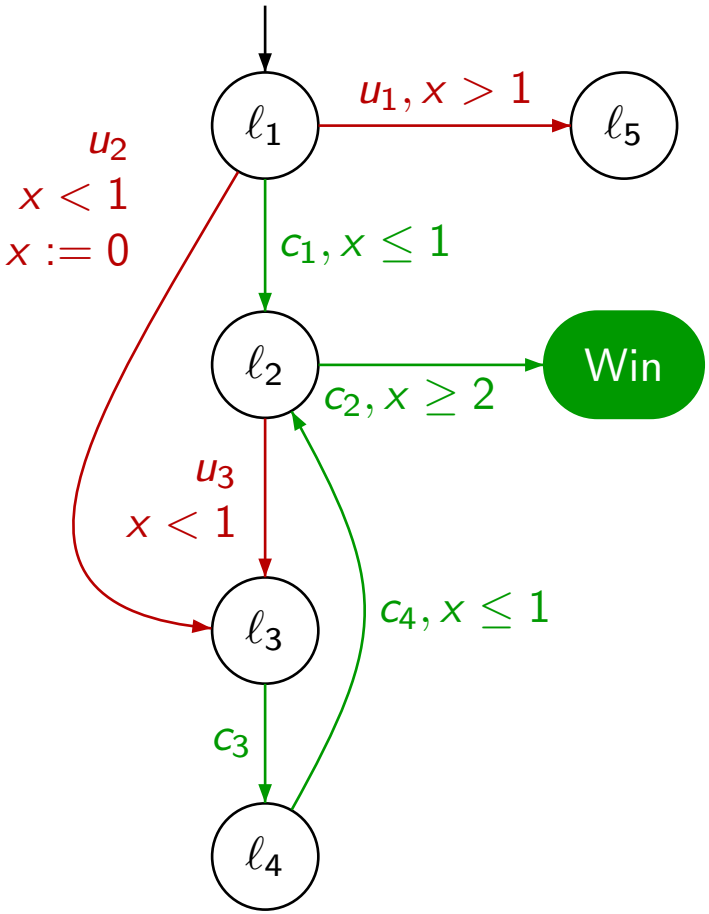
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

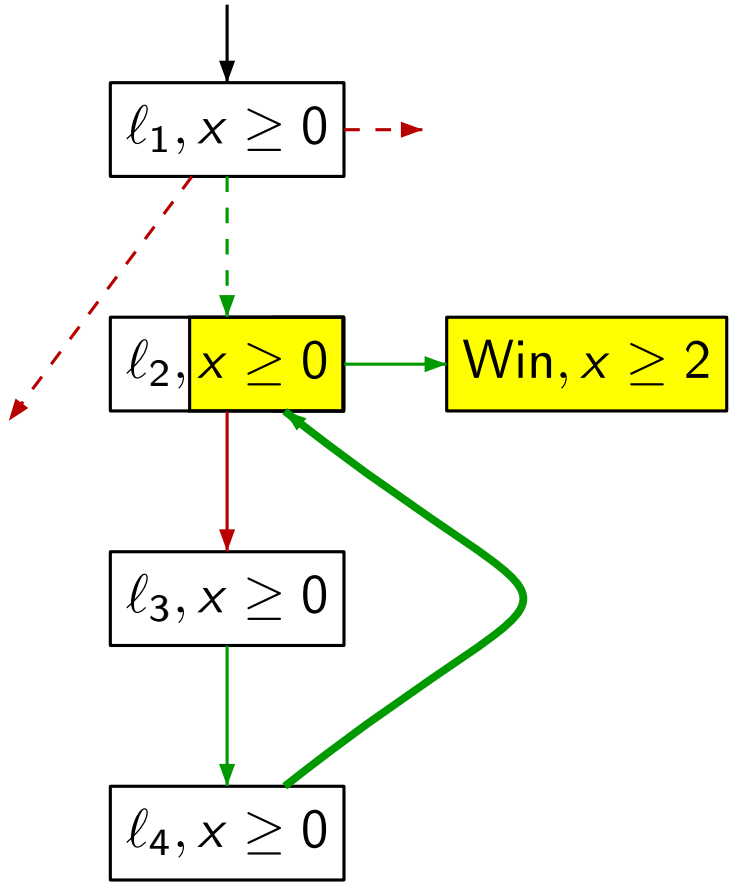




Algorithme en avant pour les états gagnants

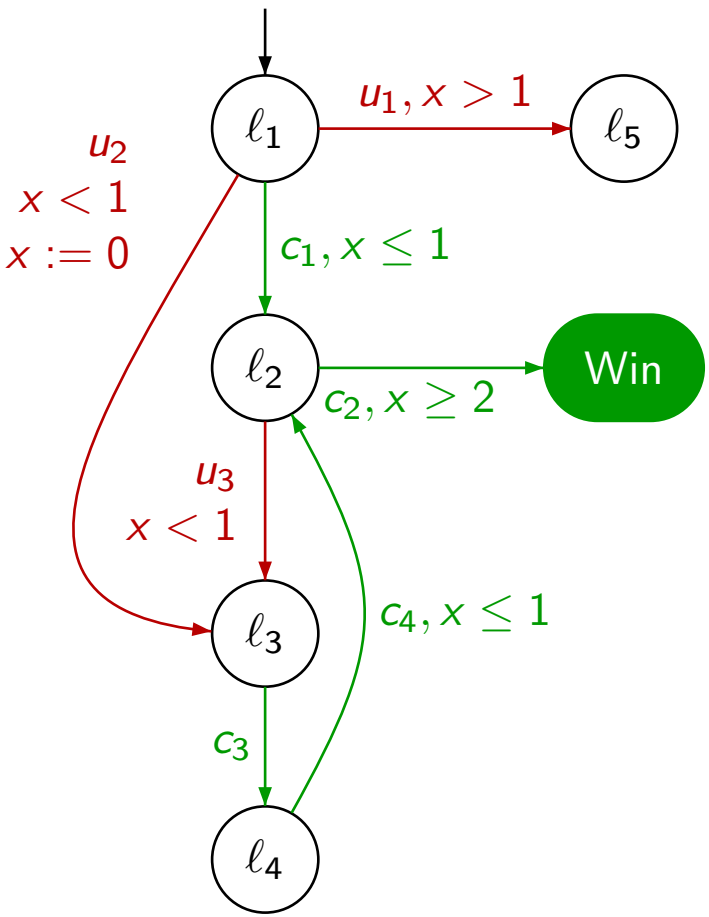
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

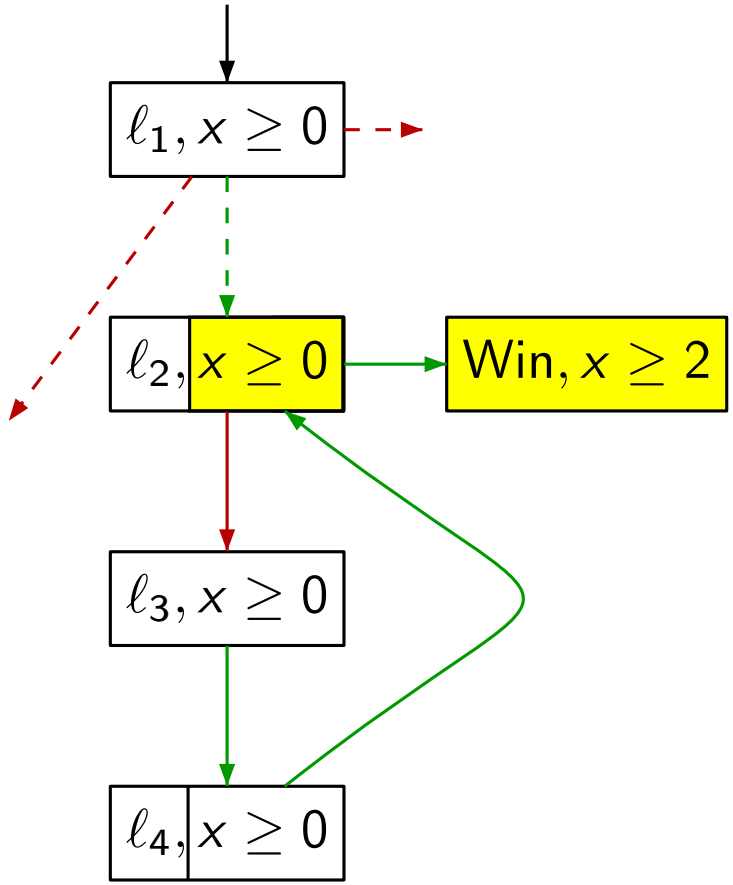




Algorithme en avant pour les états gagnants

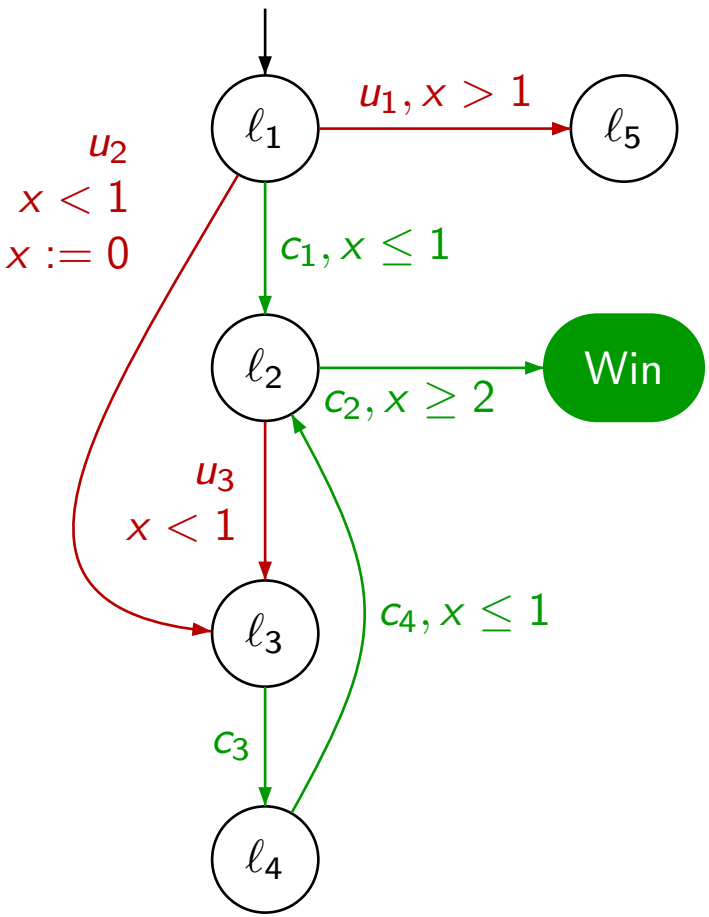
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

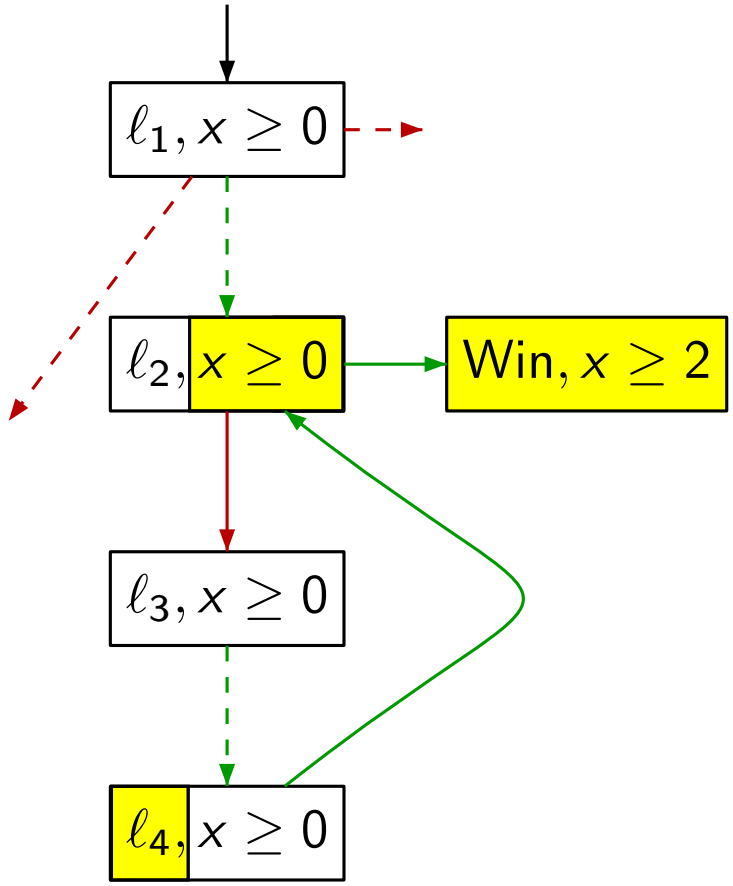




Algorithme en avant pour les états gagnants

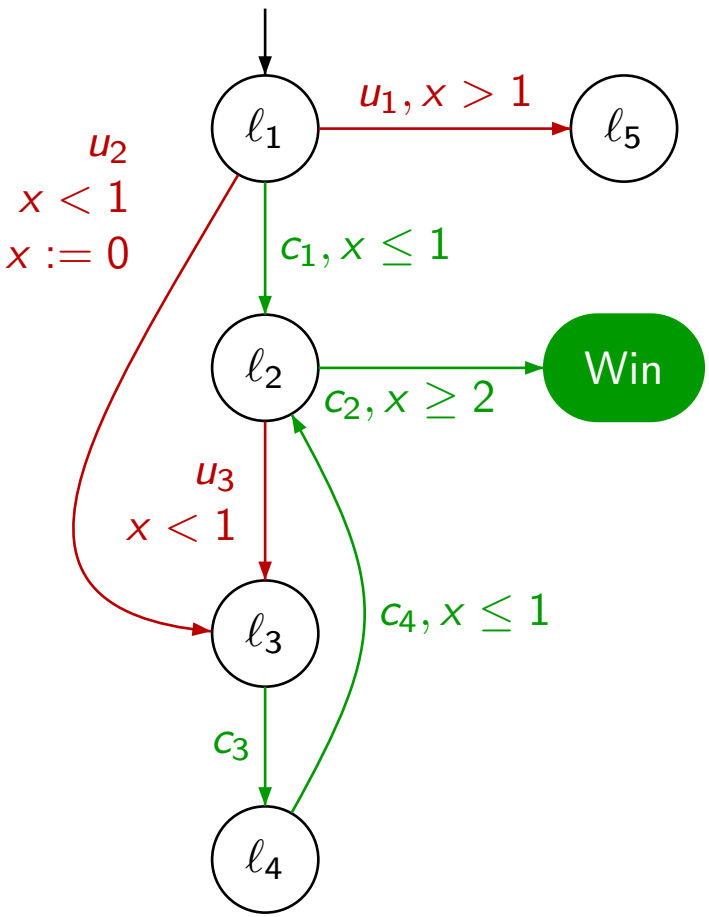
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

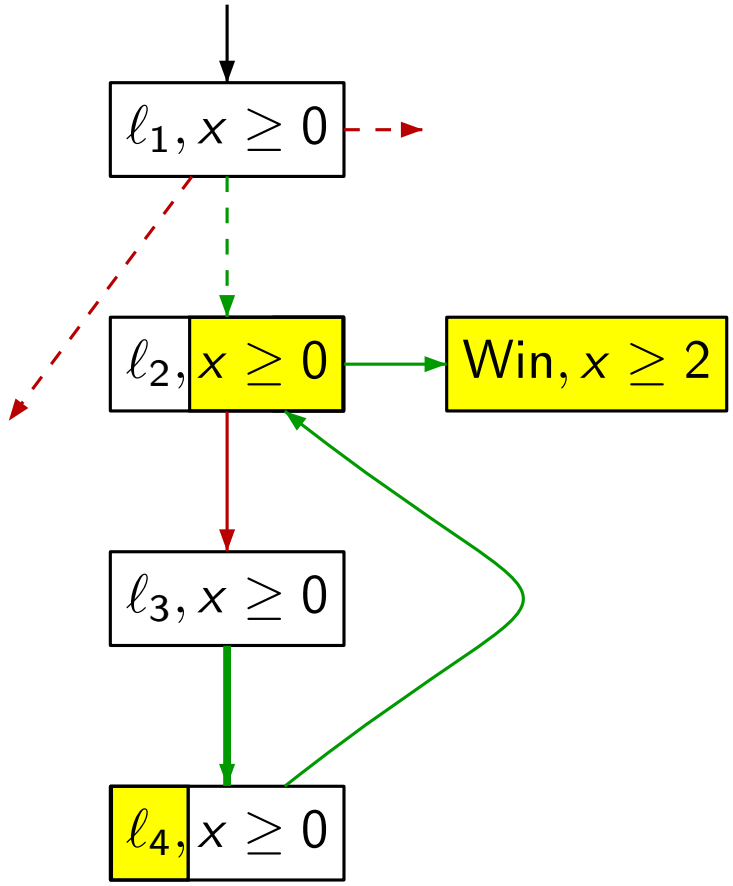




Algorithme en avant pour les états gagnants

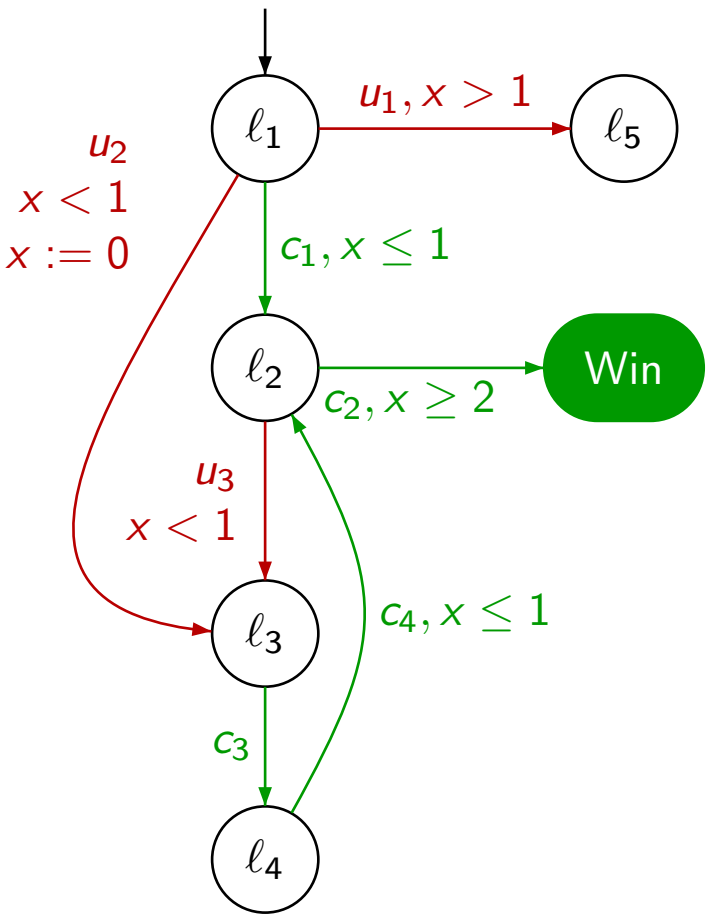
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

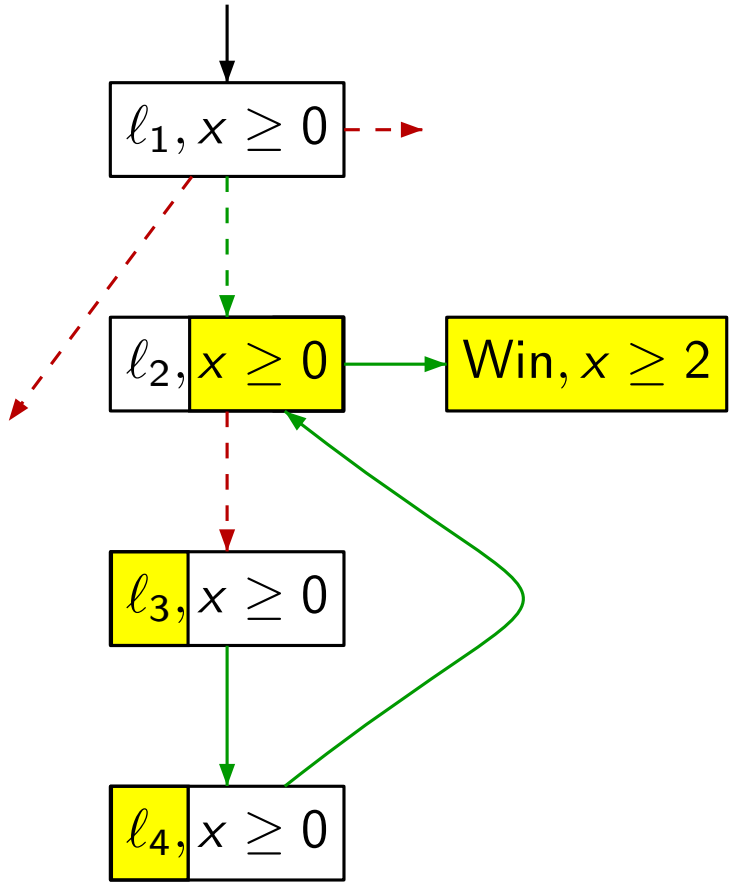




Algorithme en avant pour les états gagnants

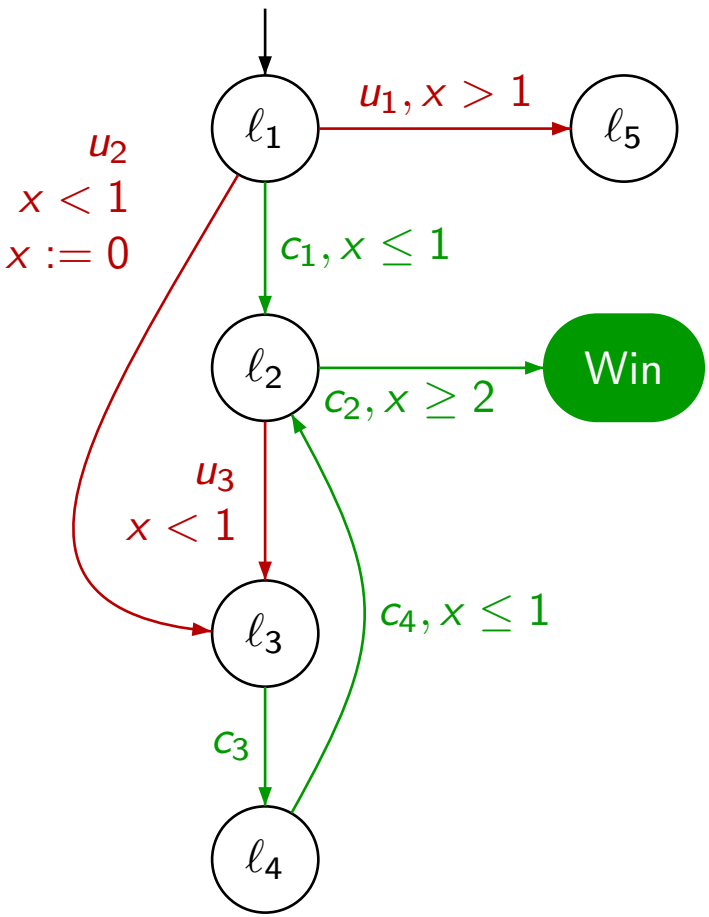
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

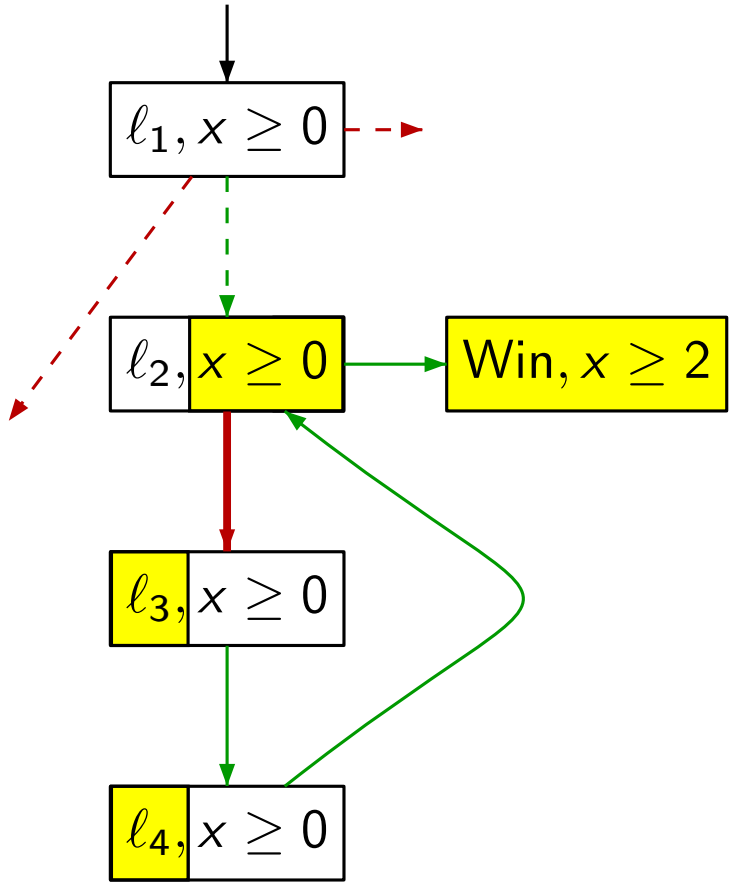




Algorithme en avant pour les états gagnants

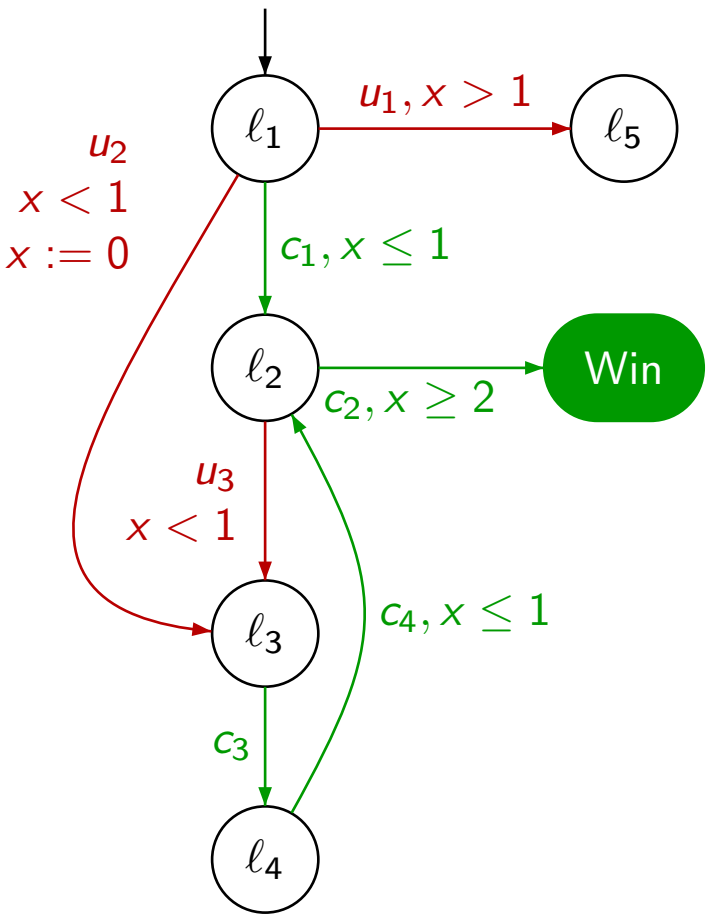
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

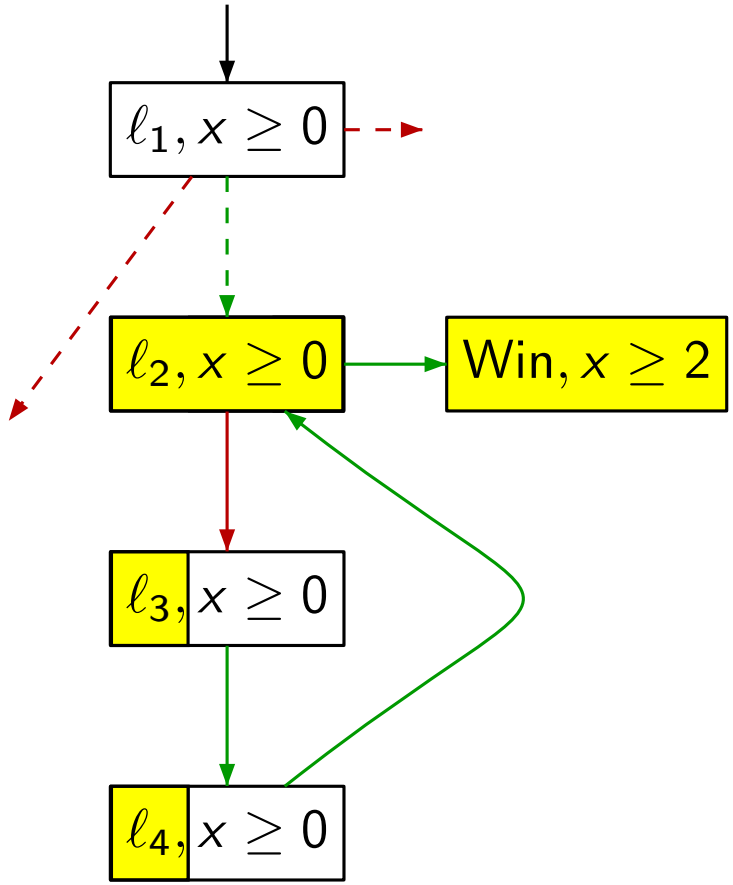




Algorithme en avant pour les états gagnants

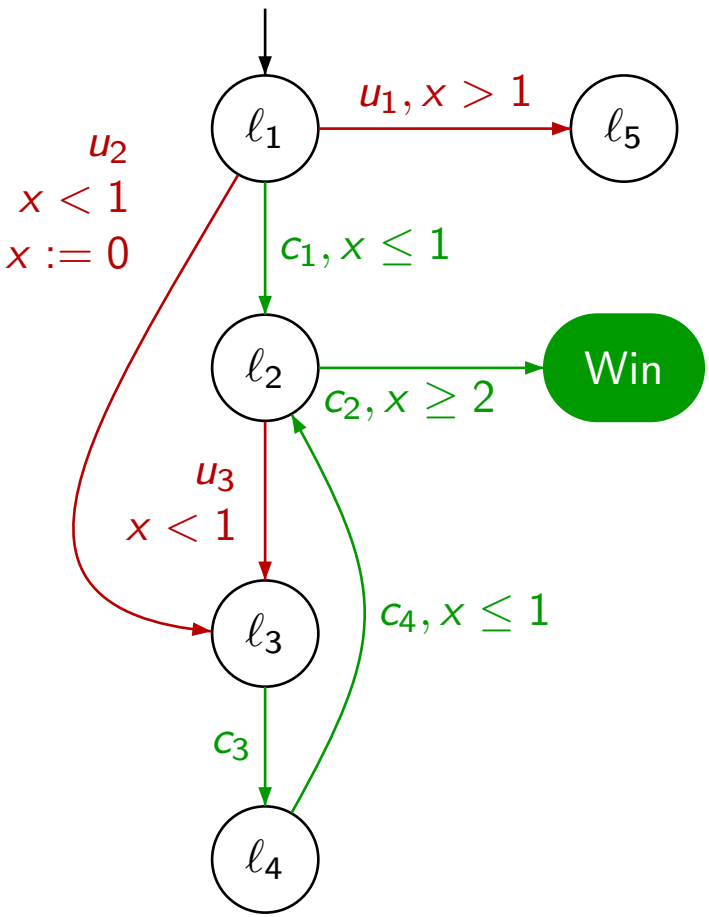
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

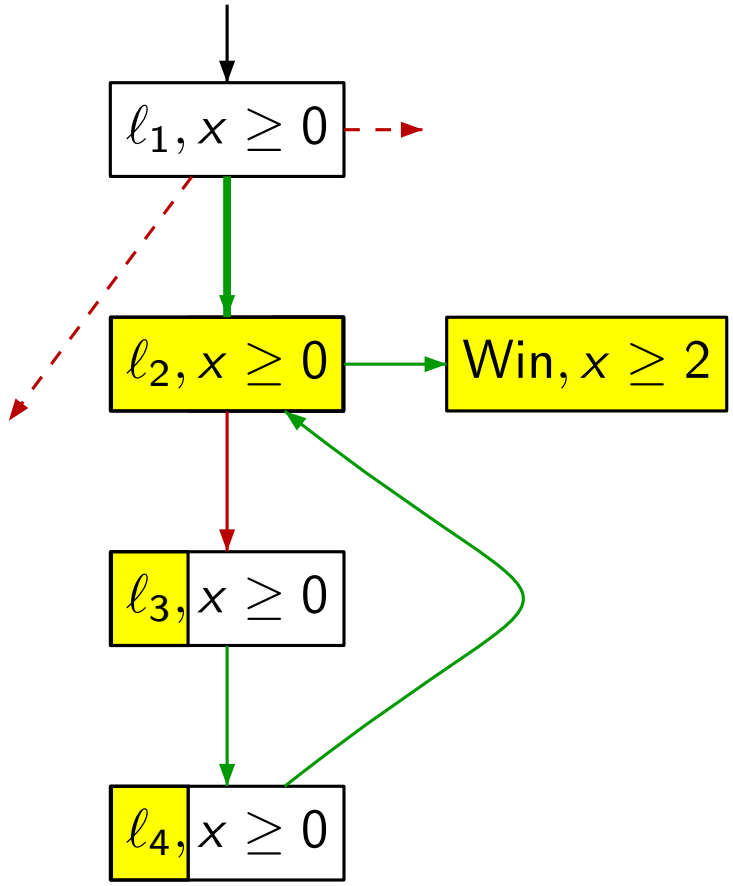




Algorithme en avant pour les états gagnants

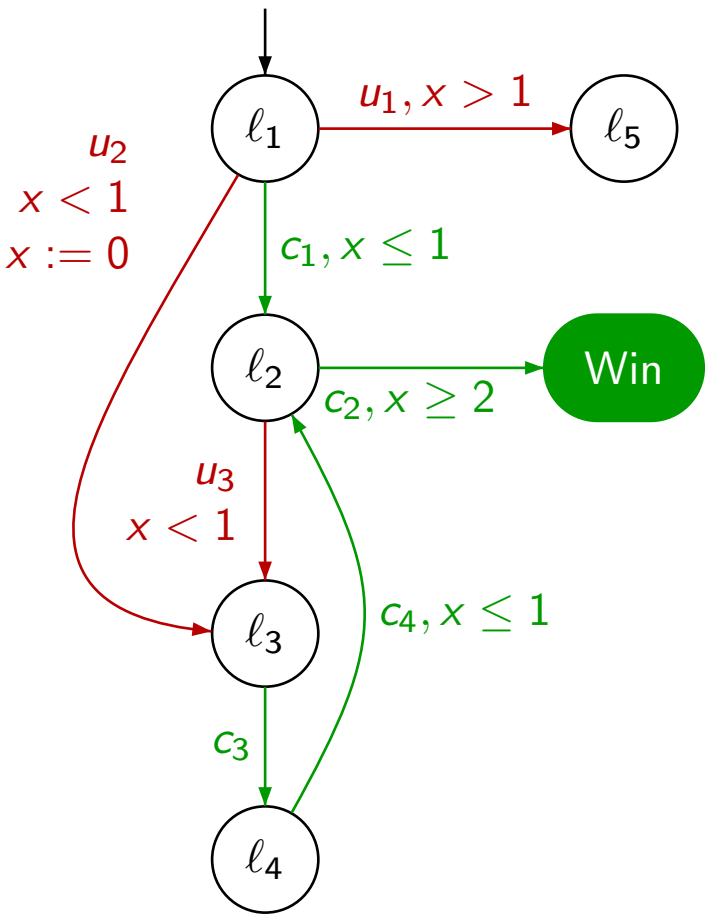
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

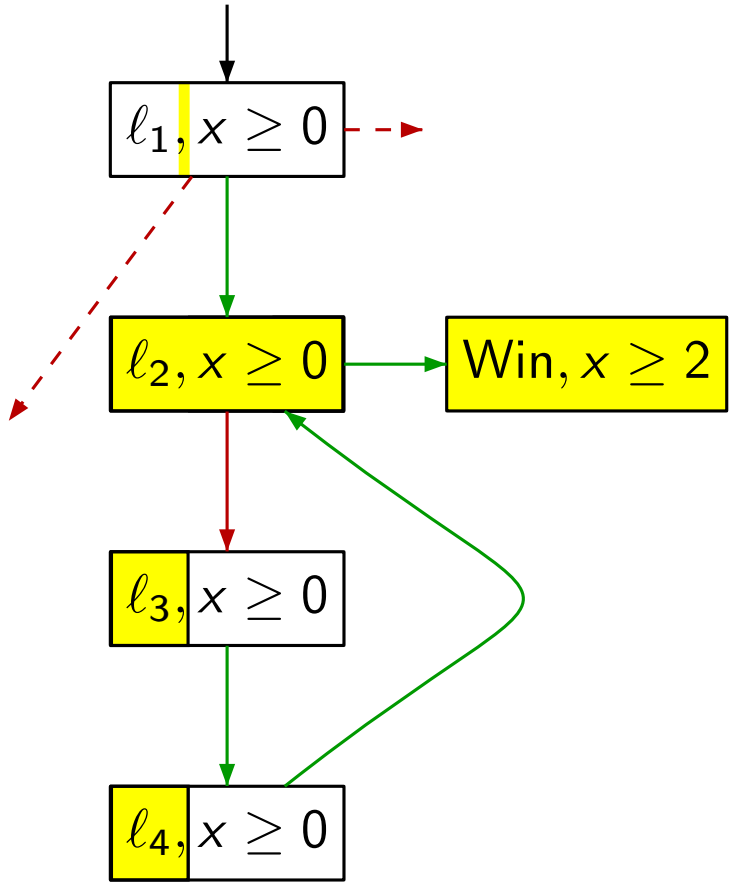




Algorithme en avant pour les états gagnants

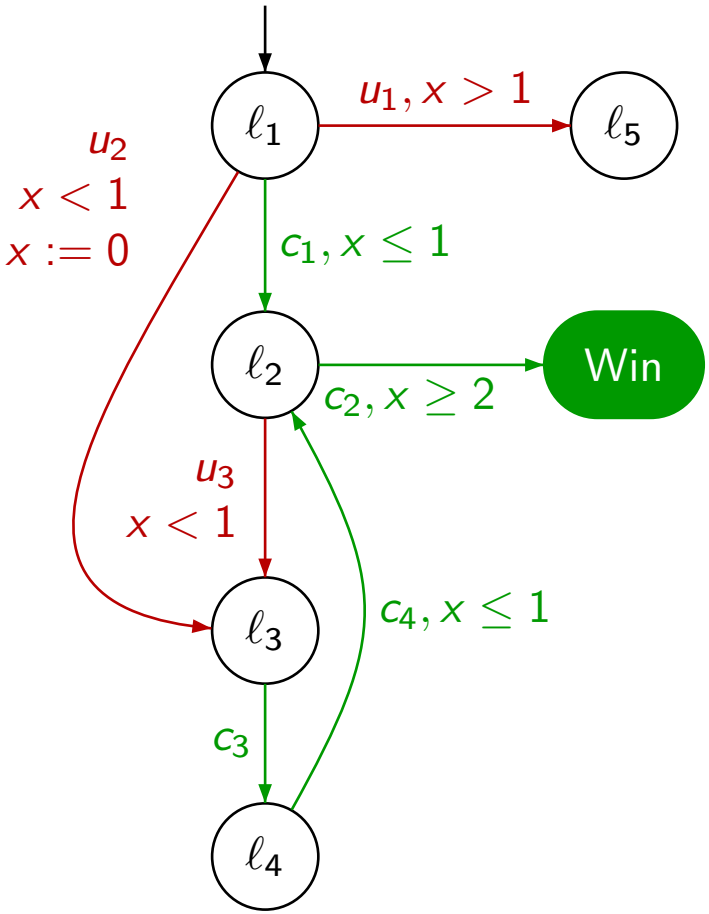
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

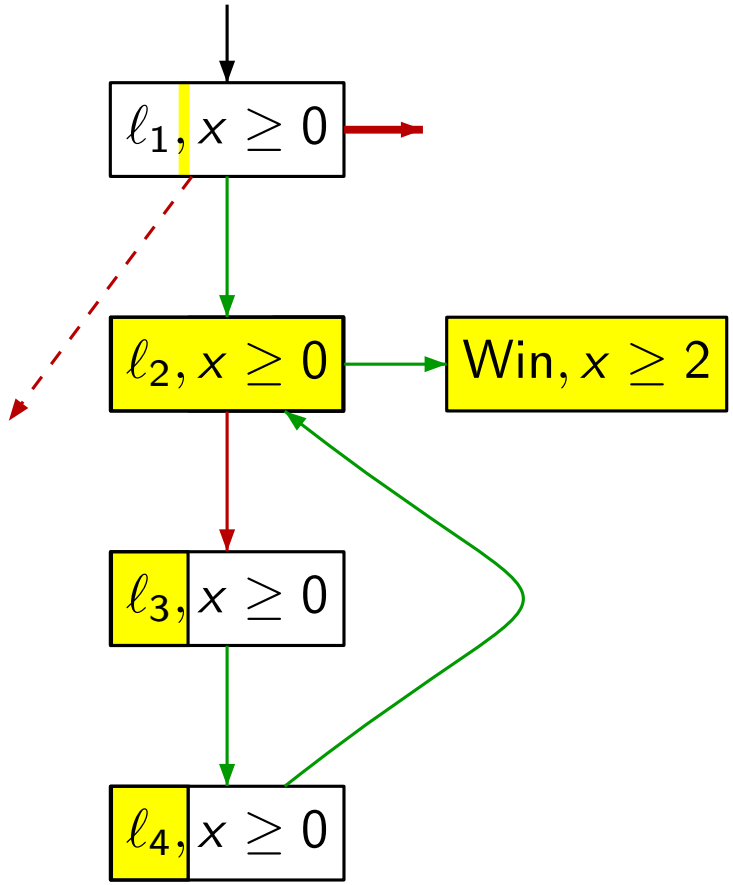




Algorithme en avant pour les états gagnants

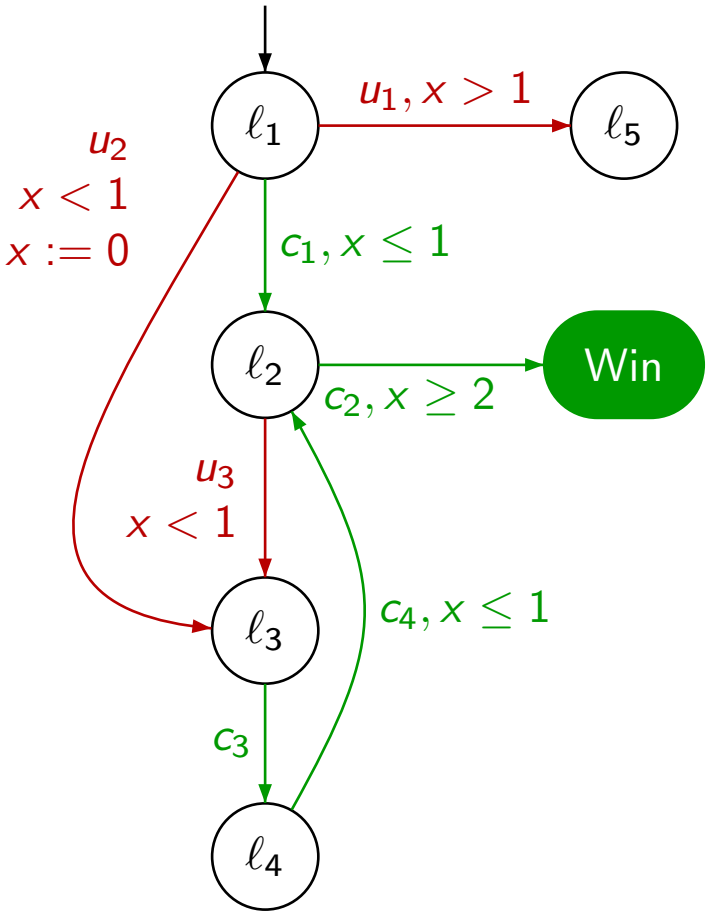
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

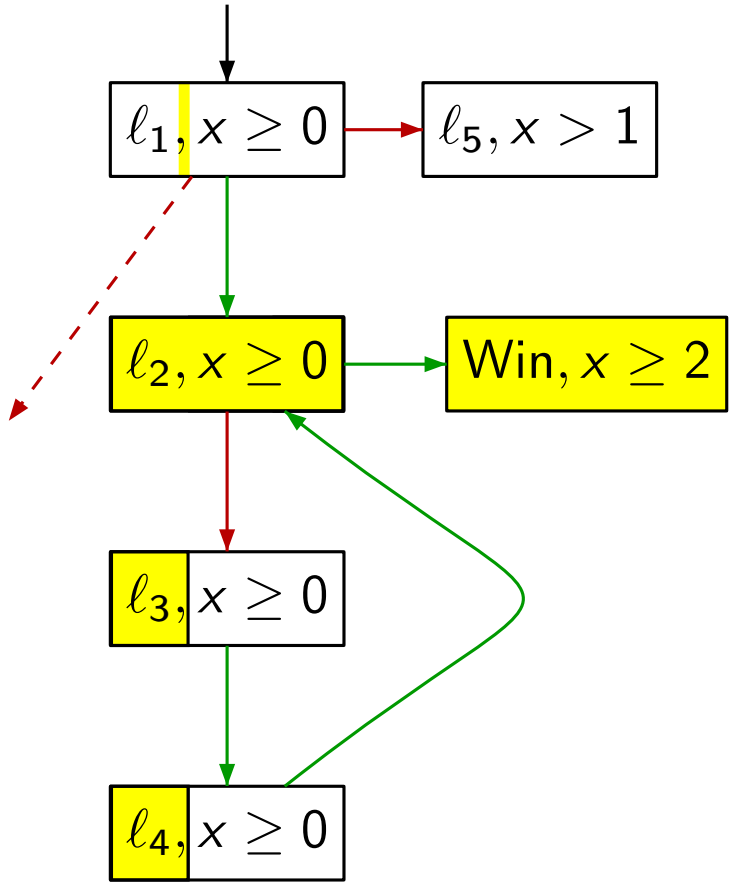




Algorithme en avant pour les états gagnants

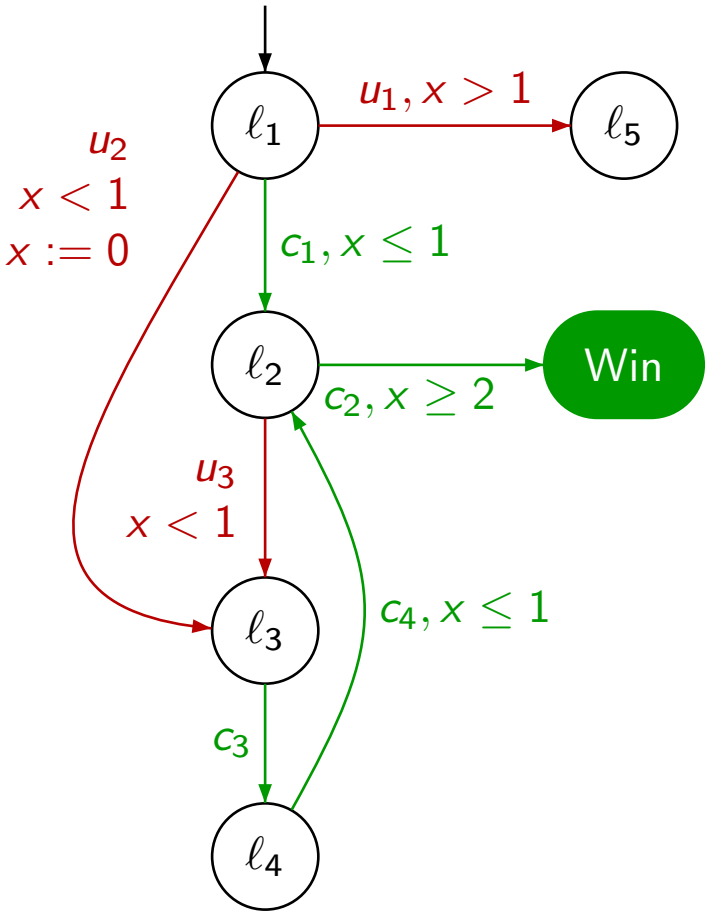
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

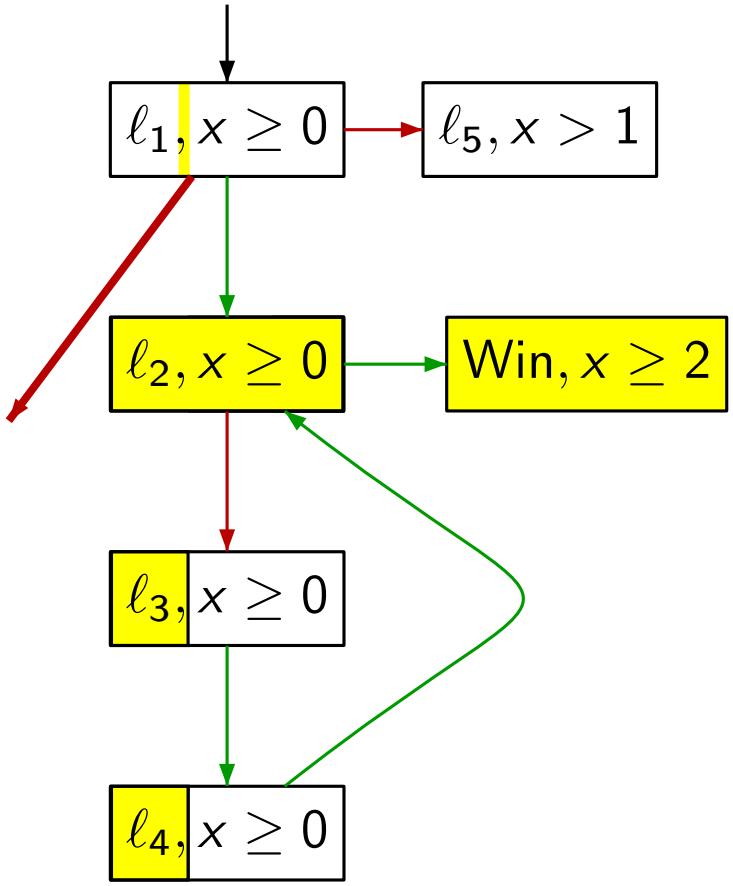




Algorithme en avant pour les états gagnants

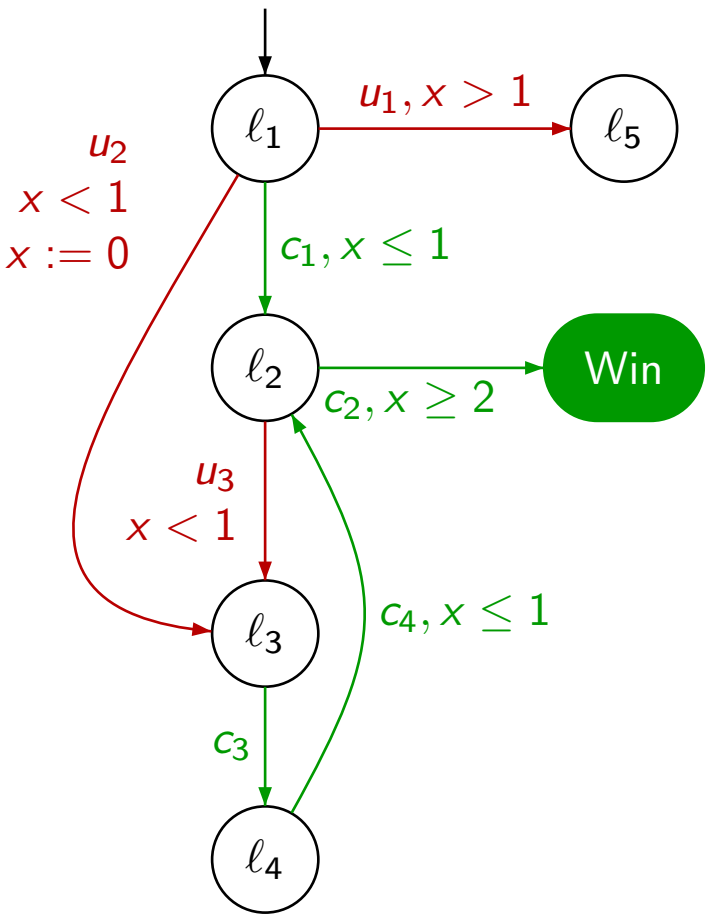
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

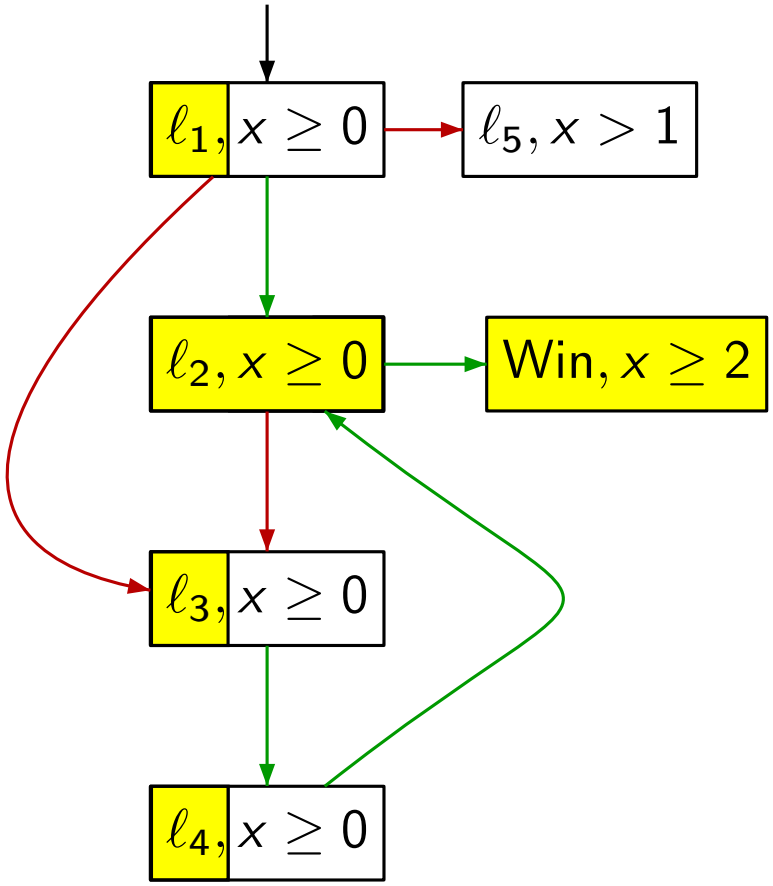




Algorithme en avant pour les états gagnants

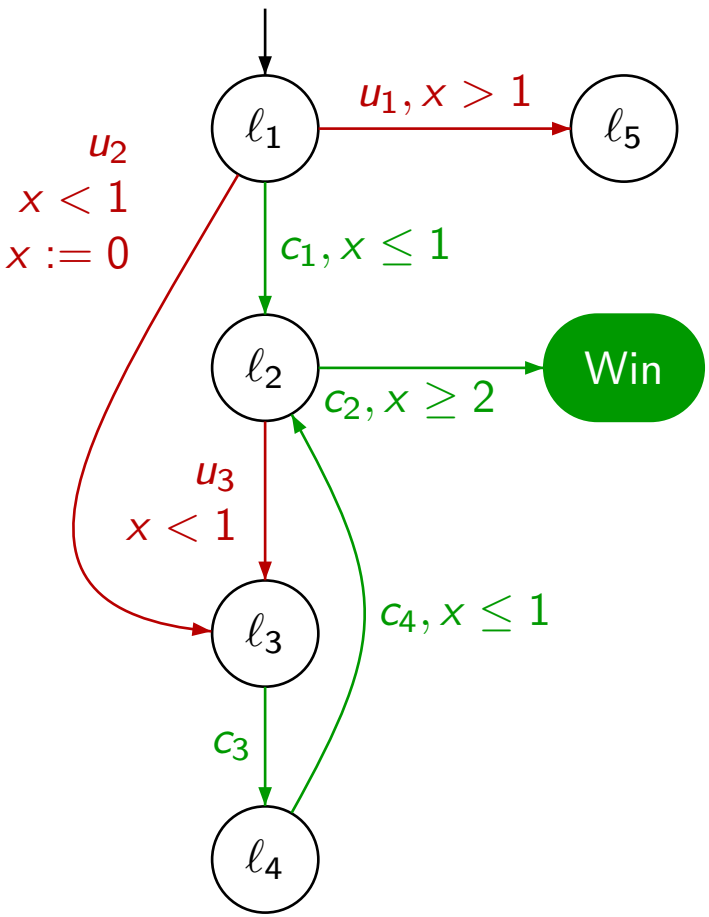
[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]

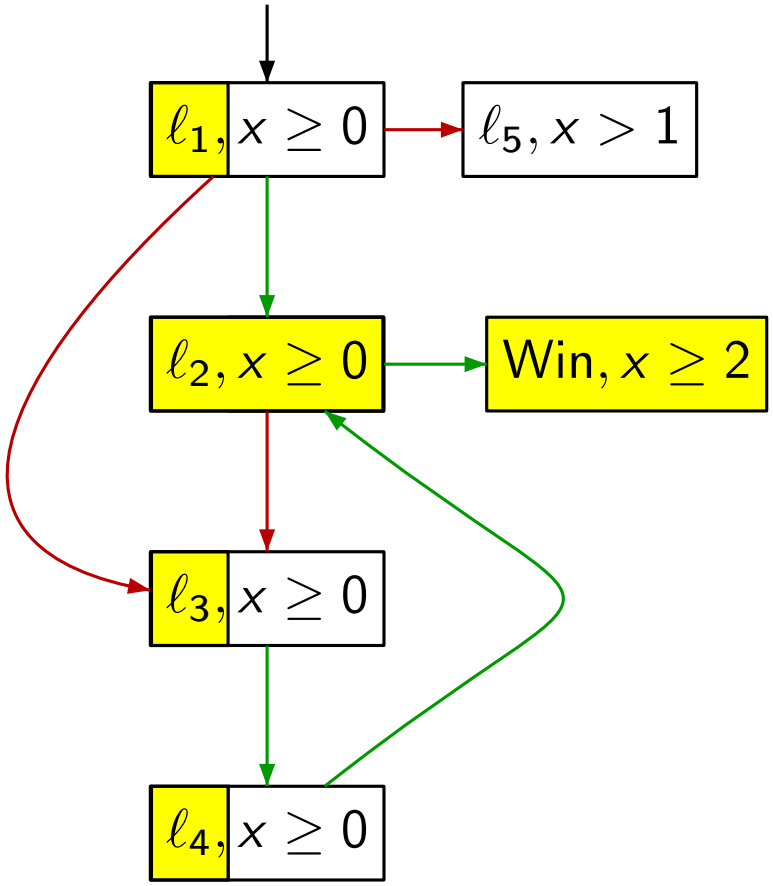




Algorithme en avant pour les états gagnants

[Cassez, David, Fleury, Larsen, Lime - CONCUR'05]





➜ Implanté dans TiGa, une extension de Uppaal

Quelques faits marquants

- Cours sur la synthèse de systèmes temporisés à l'école GAMES (réseau européen sur les jeux)
- Exposé d'introduction au contrôle temporisé à l'AS 155 du RTP 24
- Session invitée CORTOS à MSR'05
  - Introduction au contrôle des systèmes temps-réel
  - Observation partielle des systèmes temporisés
  - Implémentabilité des automates temporisés
- Co-organisation de GDV'06, workshop de CAV'06
- Et enfin...

Une page de pub...

Soumettez à CORTOS'06, workshop de CONCUR'06

(Bonn, août 2006)

`http://www.lsv.ens-cachan.fr/aci-cortos/workshop-concur06/`