Vérification de programmes par Analyse des Relations Linéaires

(et amélioration de précision par accélération)

Laure Gonnord

http://laure.gonnord.org/pro/

Verimag/CITI/INSA
Grenoble/Villeurbanne, France

Vérification de propriétés de programmes numériques

Diverses méthodes :

- La preuve et les assistants de preuve (Coq, Isabelle).
- Le test.
- Le model-checking.

Vérification de propriétés de programmes numériques

Diverses méthodes :

- La preuve et les assistants de preuve (Coq, Isabelle).
- Le test.
- Le model-checking.

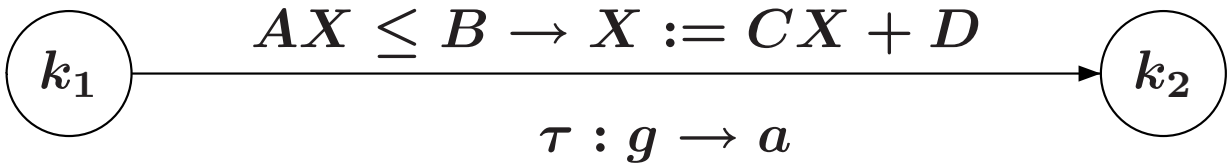
Les propriétés :

- Propriétés de **sûreté**.
- Propriétés numériques : **inéquations linéaires** $2y \leqslant 13$.

▶ limites du model-checking.

Modèle - Notations

Vérification de propriétés **numériques** sur des GFC avec conditions et actions **affines** :

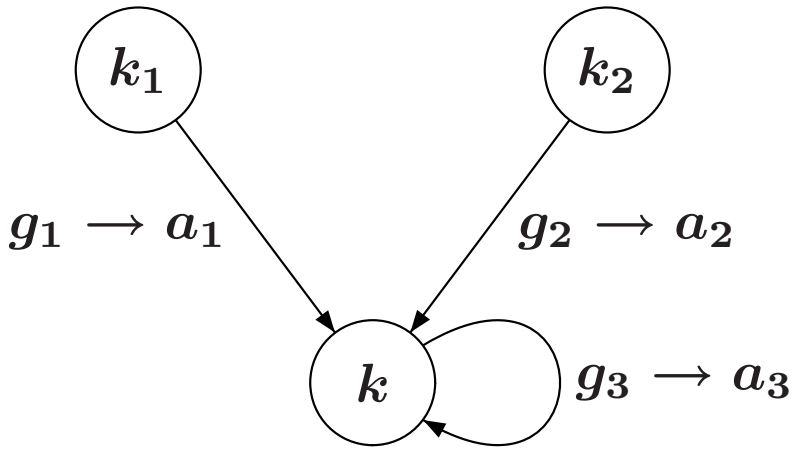


ou encore « automates interprétés », automates « à compteurs ».

- A, C matrices, B, D vecteurs.
- Sémantique « naturelle ».
- On veut des invariants pour **chaque point de contrôle**.

Formalisation du problème

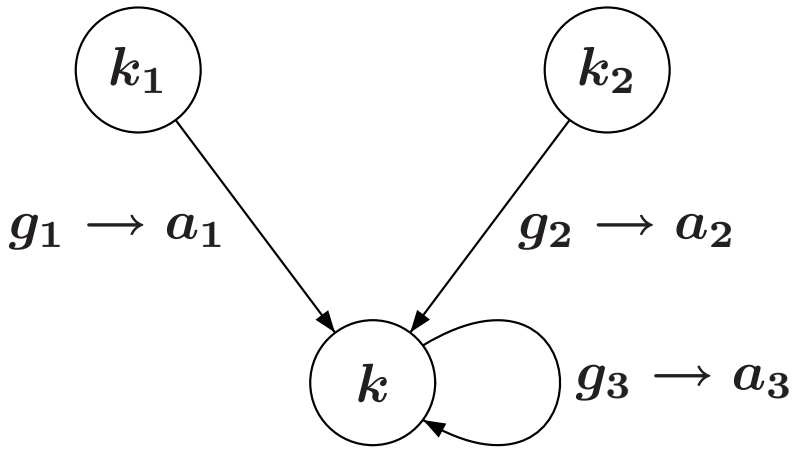
$\mathcal{A}_k$ = ensemble des **valuations** au point k :



$$\mathcal{A}_k = a_1(\mathcal{A}_{k_1} \cap g_1) \cup a_2(\mathcal{A}_{k_2} \cap g_2) \cup a_3(\mathcal{A}_{k_3} \cap g_3)$$

Formalisation du problème

$\mathcal{A}_k$ = ensemble des **valuations** au point k :



$$\mathcal{A}_k = a_1(\mathcal{A}_{k_1} \cap g_1) \cup a_2(\mathcal{A}_{k_2} \cap g_2) \cup a_3(\mathcal{A}_{k_3} \cap g_3)$$

- Système d'équations $X = F(X)$, **point fixe**.
  - Représentation des valuations, calcul.
  - Convergence de la résolution.

Résolution du système de point-fixe

Rappel des problèmes :

- Représentation, calcul
- Convergence de la résolution

Résolution du système de point-fixe

Rappel des problèmes :

- Représentation, calcul **polyèdres convexes**
- Convergence de la résolution **opérateur d'élargissement**

Résolution du système de point-fixe

Rappel des problèmes :

- Représentation, calcul **polyèdres convexes**
- Convergence de la résolution **opérateur d'élargissement**

▶ Résolution **approchée** mais **qui converge**

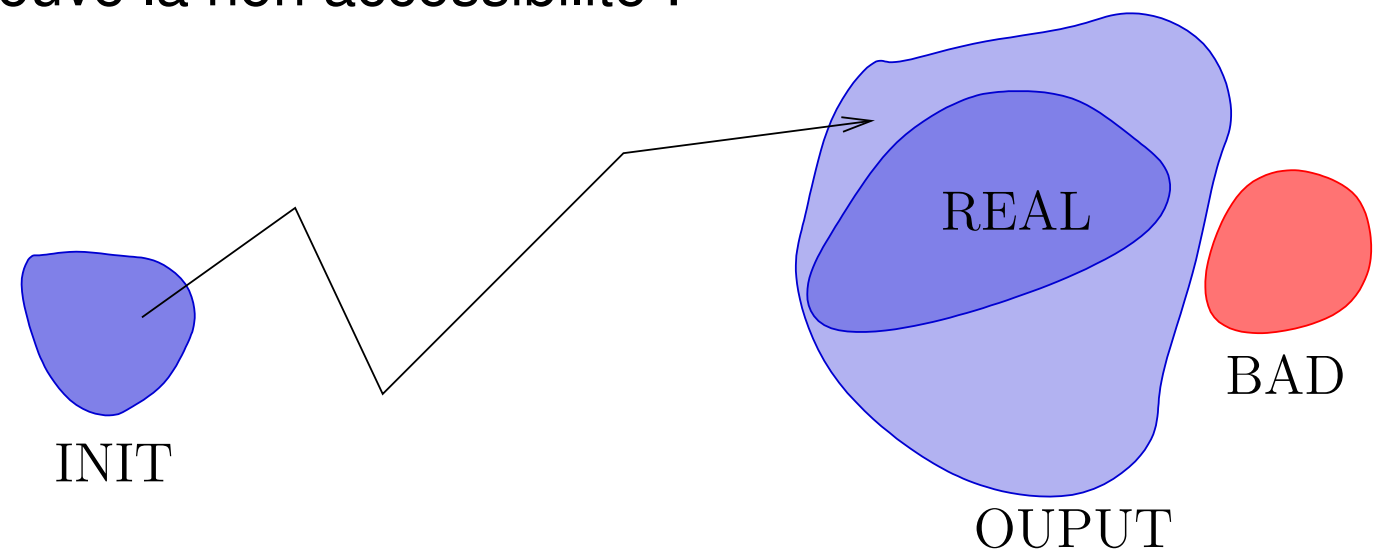
Résolution du système de point-fixe

Rappel des problèmes :

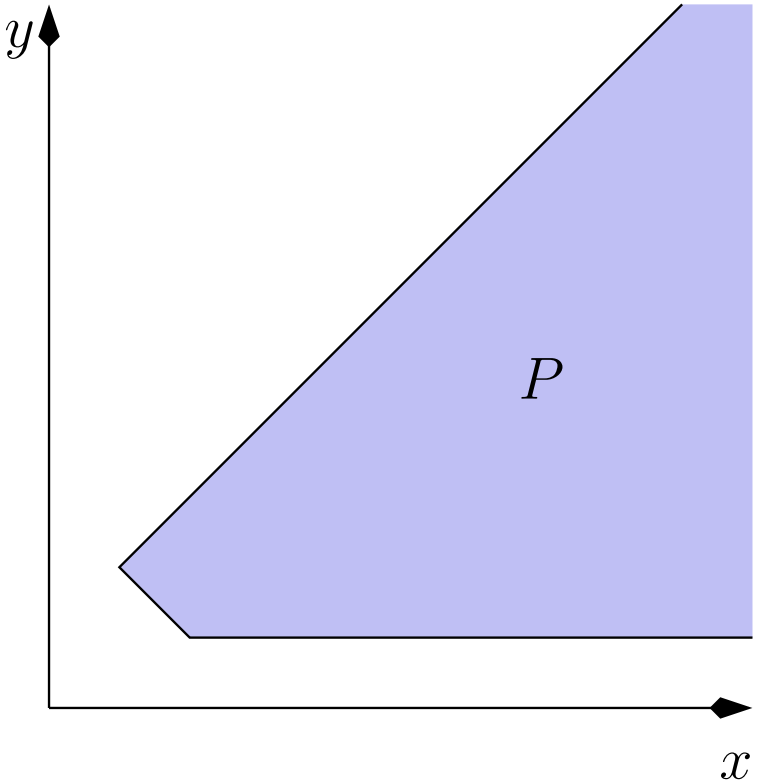
- Représentation, calcul **polyèdres convexes**
- Convergence de la résolution **opérateur d'élargissement**

▶ Résolution **approchée** mais **qui converge**

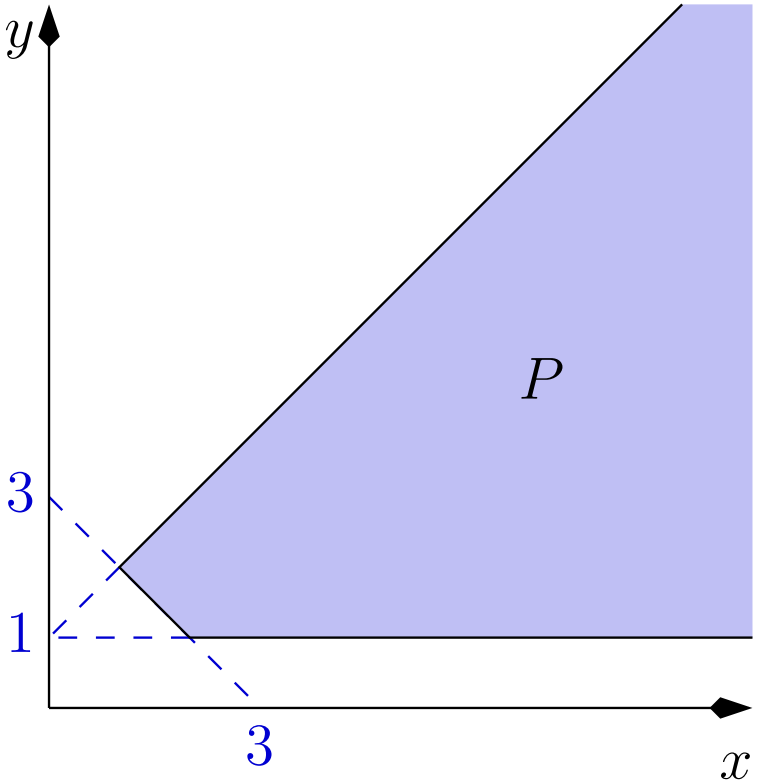
On prouve la non accessibilité :



Le treillis des polyèdres - Double Représentation

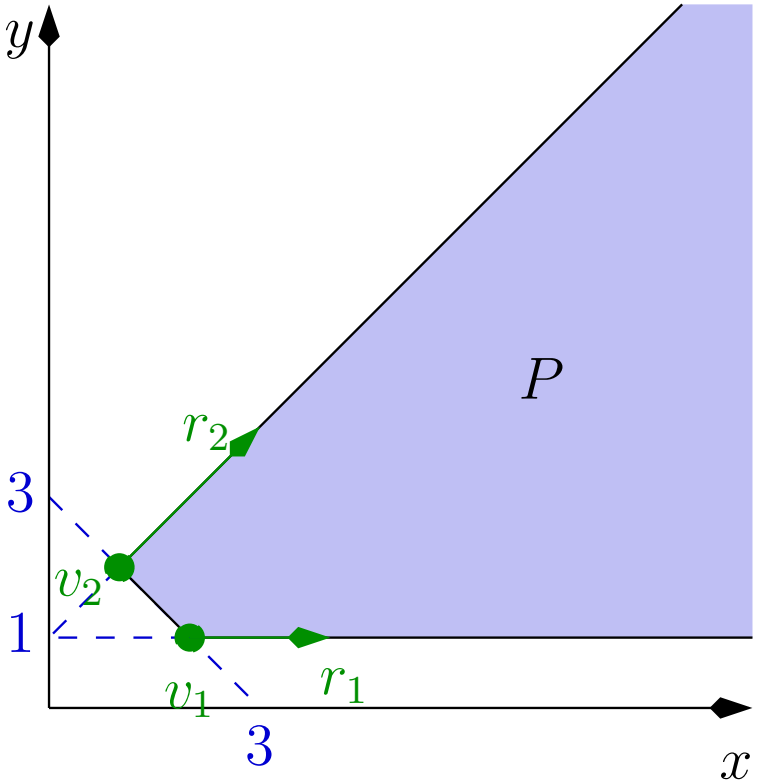


Le treillis des polyèdres - Double Représentation



$$
\begin{aligned}
P &= \{(x,y) \mid \\
&\quad 1 \leqslant y \leqslant x+1 \wedge x+y \geqslant 3\} \\
&= cons\{AX \leqslant b\}
\end{aligned}
$$

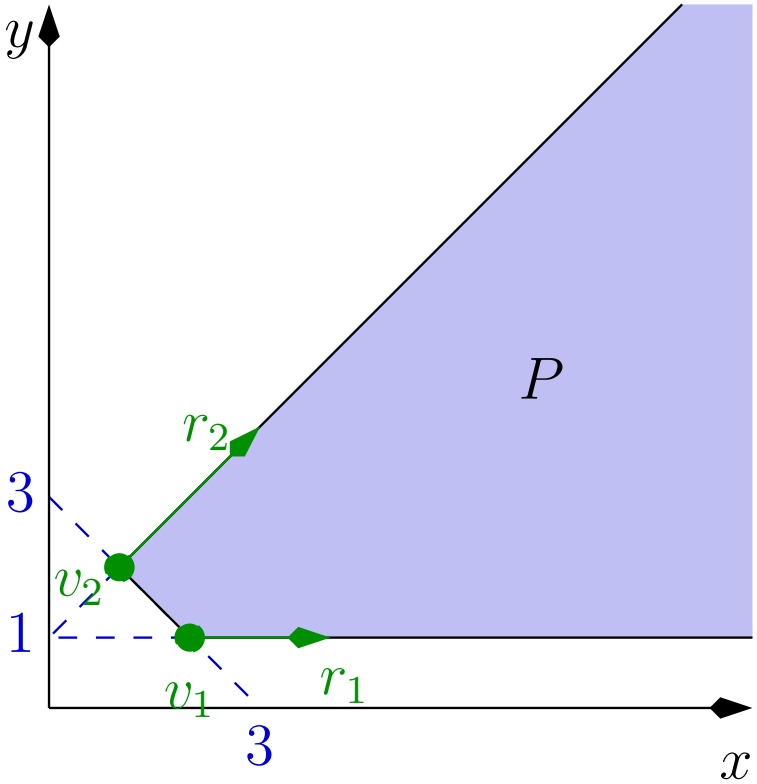
Le treillis des polyèdres - Double Représentation



$$P = \{(x,y) \mid 1 \leqslant y \leqslant x+1 \wedge x+y \geqslant 3\} = cons\{AX \leqslant b\}$$

$$P = \{\lambda v_1 + (1-\lambda)v_2 + \mu_1 r_1 + \mu_2 r_2 \mid \lambda \in [0,1],\ \mu_1, \mu_2 \geqslant 0\} = gen(V,R)\}$$

Le treillis des polyèdres - Double Représentation



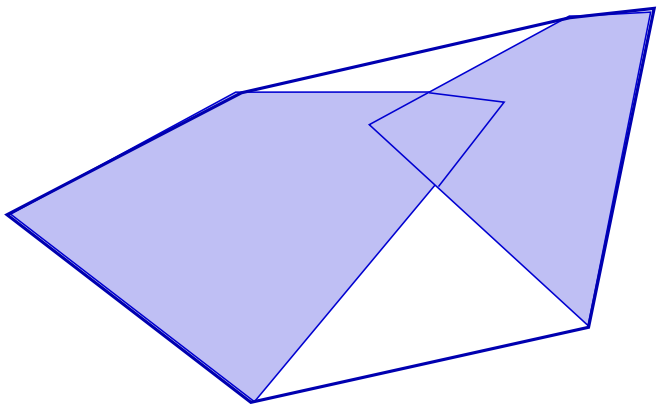
$$P = \{(x,y) \mid 1 \leqslant y \leqslant x+1 \wedge x+y \geqslant 3\} = cons\{AX \leqslant b\}$$

$$P = \{\lambda v_1 + (1-\lambda)v_2 + \mu_1 r_1 + \mu_2 r_2 \mid \lambda \in [0,1],\ \mu_1, \mu_2 \geqslant 0\} = gen(V,R)\}$$

- Deux représentations **finies** et complémentaires (passage de l'une à l'autre).
- Algorithmique disponible.

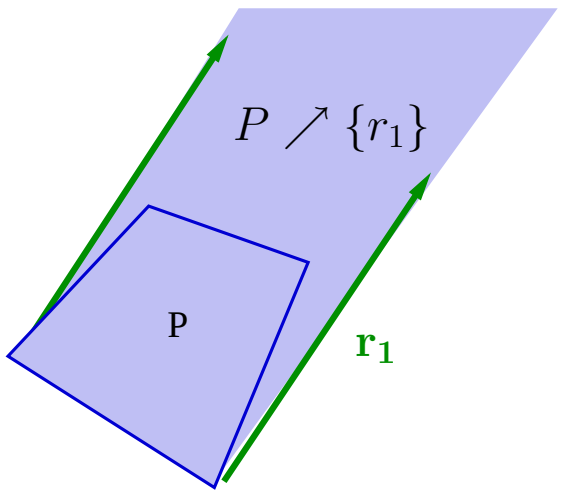
Le treillis des polyèdres convexes (2)

- Intersection, test du vide.
- Transformation affine : $a(P) = \{CX + D \mid X \in P\}$.
- Union convexe (perte de précision) :



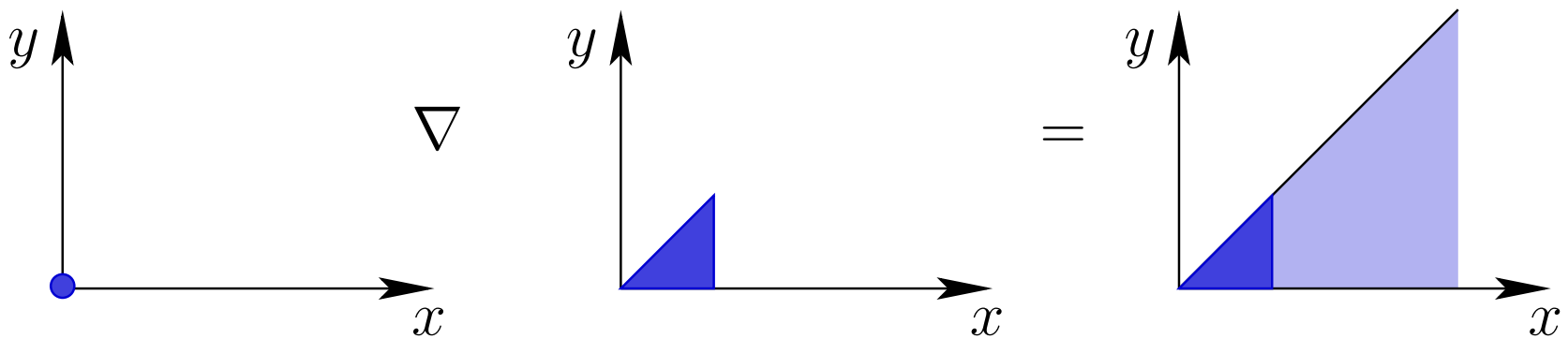
Le treillis des polyèdres convexes (2)

- Intersection, test du vide.
- Transformation affine : $a(P) = \{CX + D \mid X \in P\}$.
- Union convexe (perte de précision) :
- Ajout de rayons
  $P \nearrow R = \{X + \sum_{r_j \in R} \mu_j r_j \mid X \in P, \mu_j \in \mathbb{Q}^+\}$



Le treillis des polyèdres convexes (3)

Élargissement : $P_1 \nabla P_2$: extrapolation de la limite.
Le système de contrainte de $P \nabla Q$ est obtenu en enlevant du système de P les contraintes non satisfaites par Q :

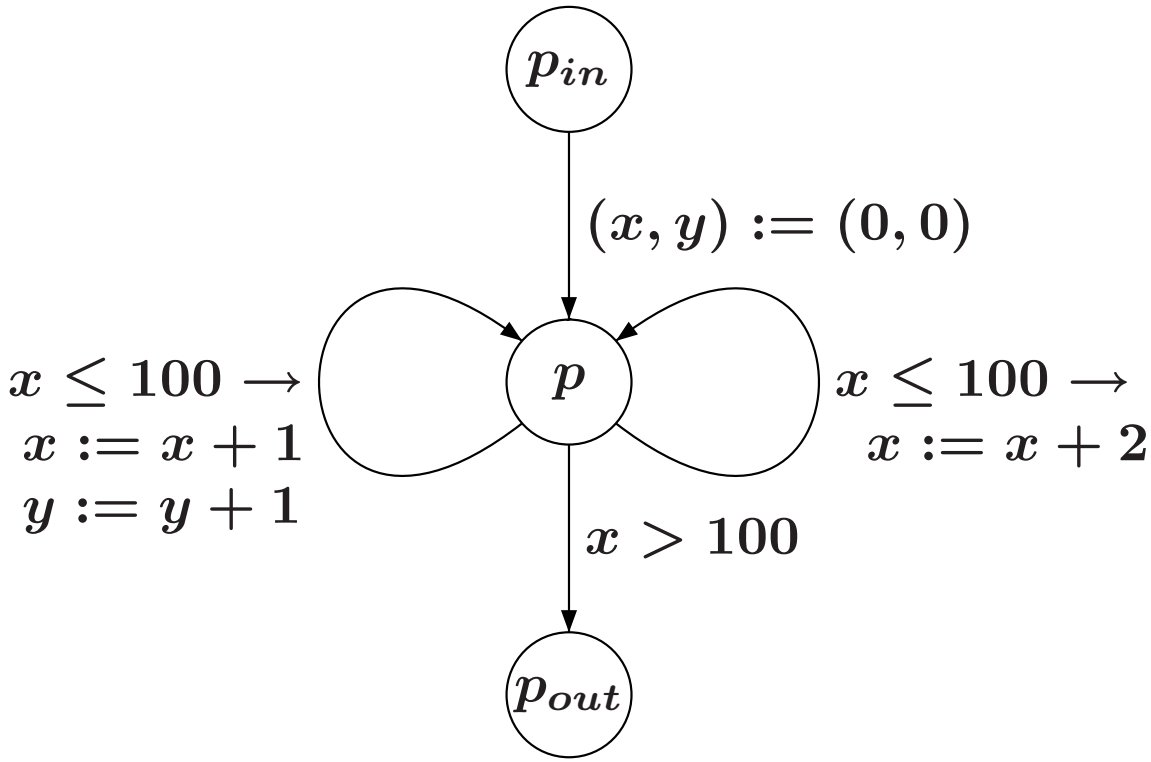


$x = y = 0$ $\quad$ $0 \leqslant y \leqslant x \leqslant 1$ $\quad$ $0 \leqslant y \leqslant x$

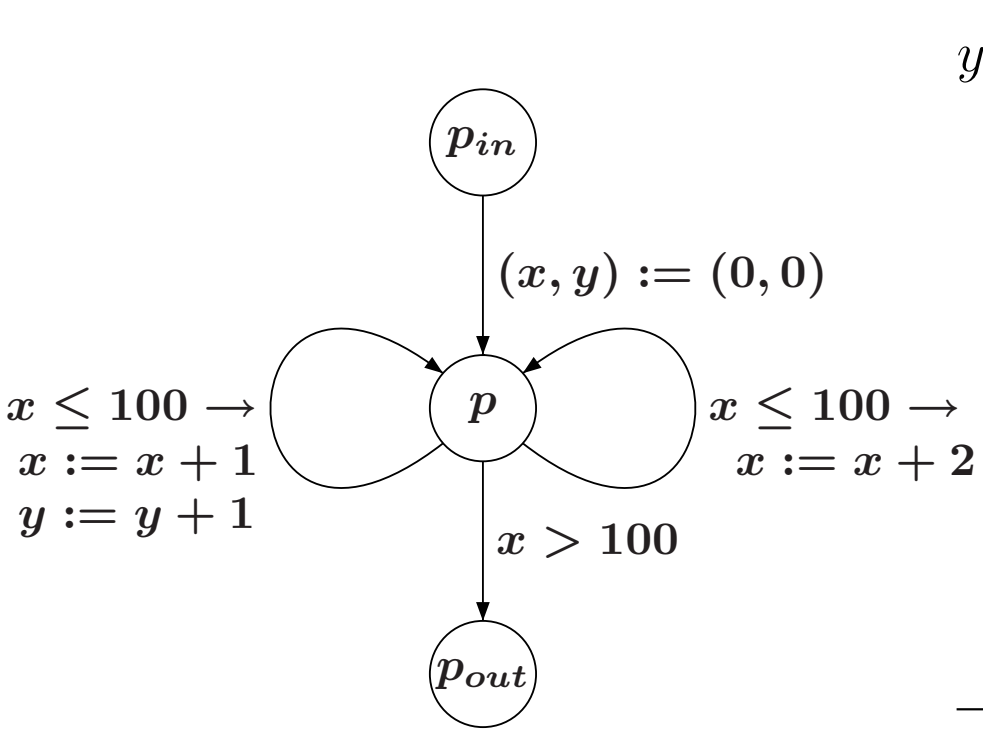
Astuce (!) : $\{x = y = 0\} = \{0 \leqslant y \leqslant x \leqslant 0\}$

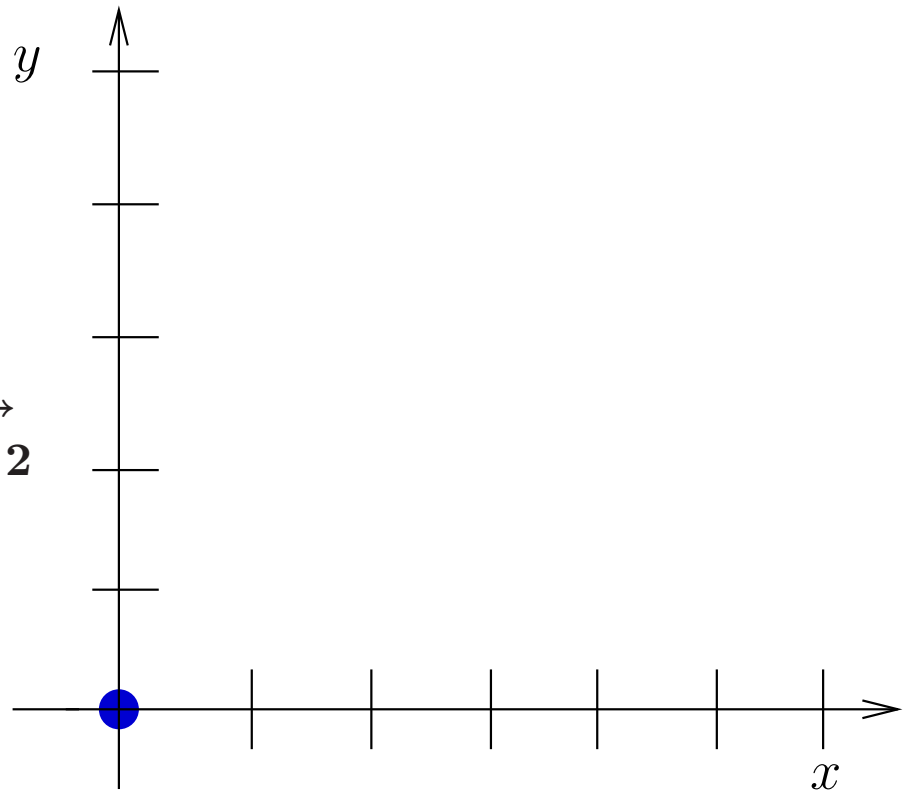
Un exemple - 1

```
x:=0;y:=0
while (x<=100) do
  read(b);
  if b then
        x:=x+2
      else begin
        x:=x+1;
        y:=y+1;
      end;
  endif
endwhile
```

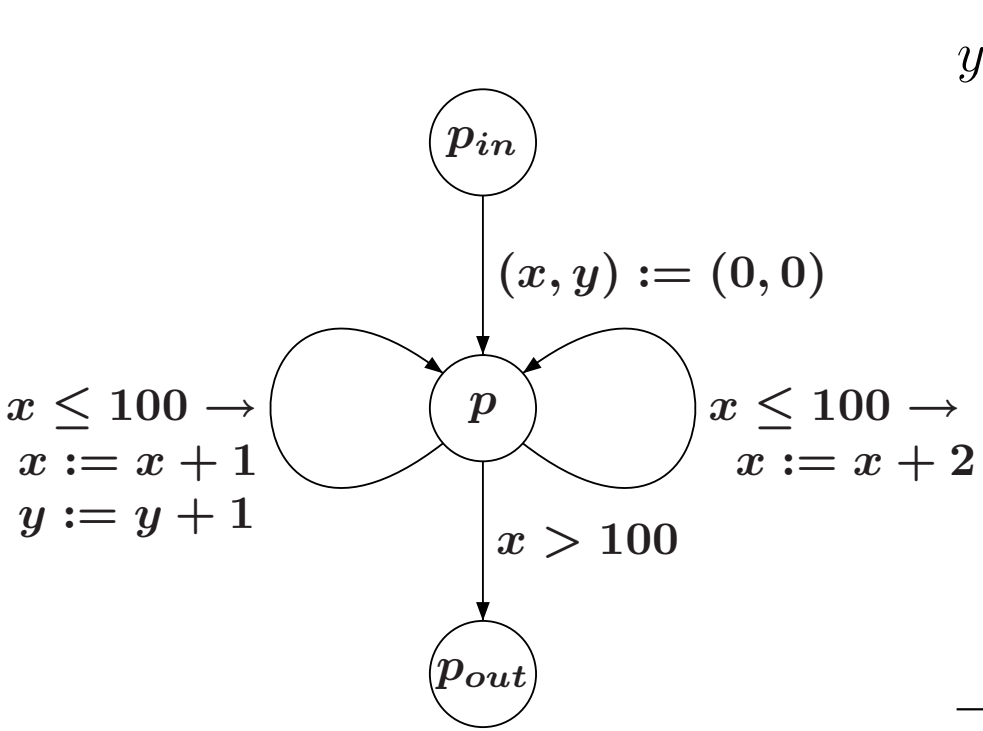


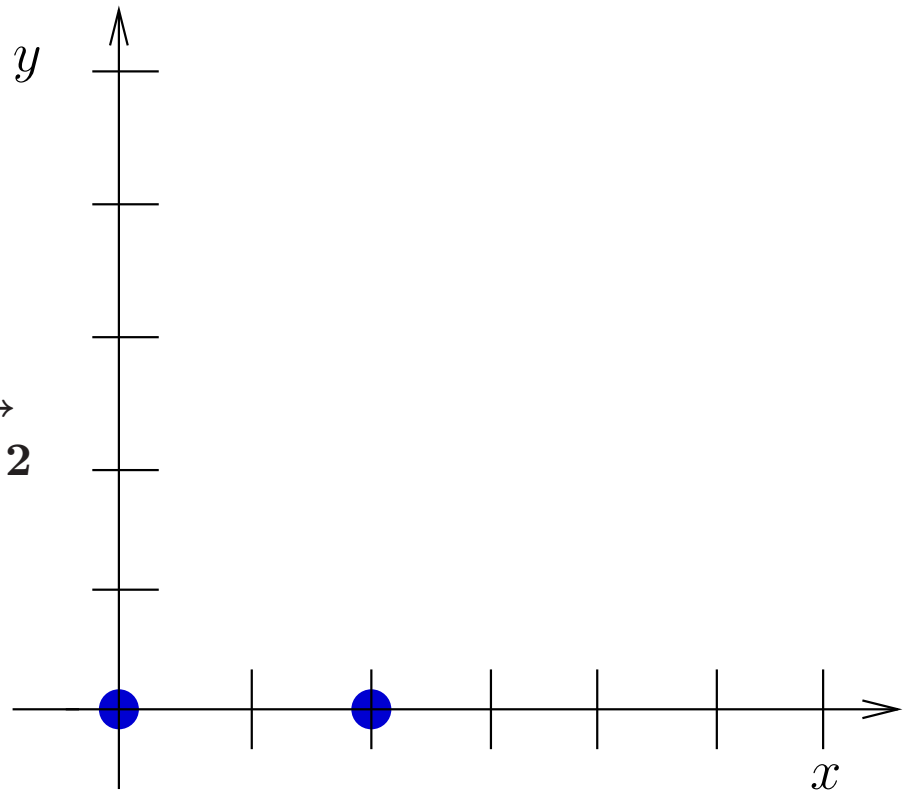
Un exemple - 2


p_{in}
$(x, y) := (0, 0)$
p
$x \leq 100 \rightarrow$
$x := x + 1$
$y := y + 1$
$x \leq 100 \rightarrow$
$x := x + 2$
$x > 100$
p_{out}

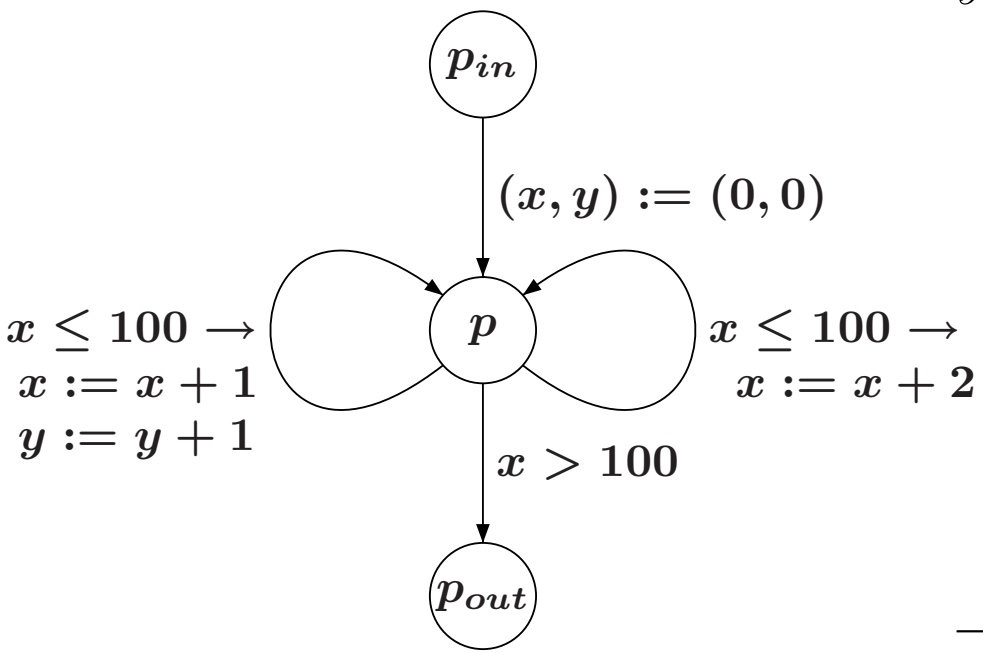

y
x

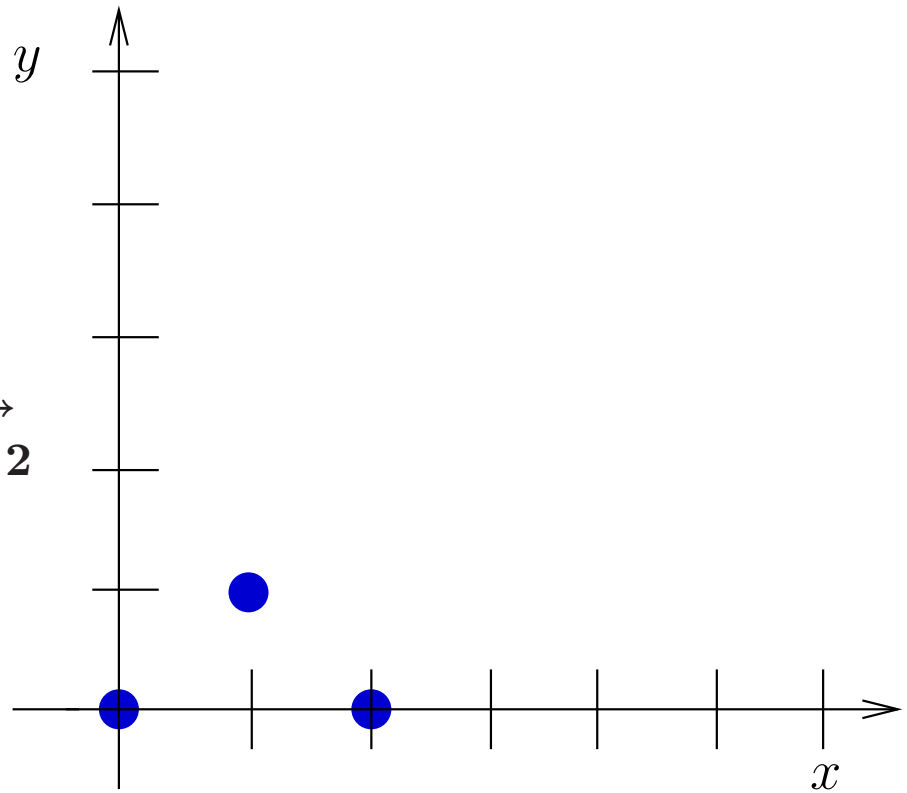
Un exemple - 2


p_{in}
$(x, y) := (0, 0)$
p
$x \leq 100 \rightarrow$
$x := x + 1$
$y := y + 1$
$x \leq 100 \rightarrow$
$x := x + 2$
$x > 100$
p_{out}

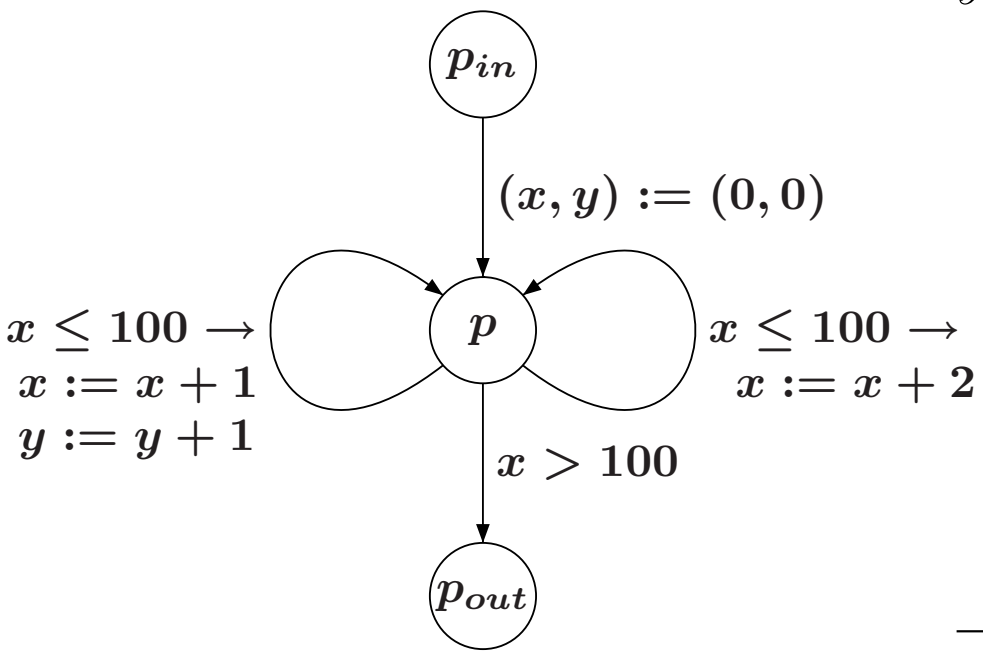

y
x

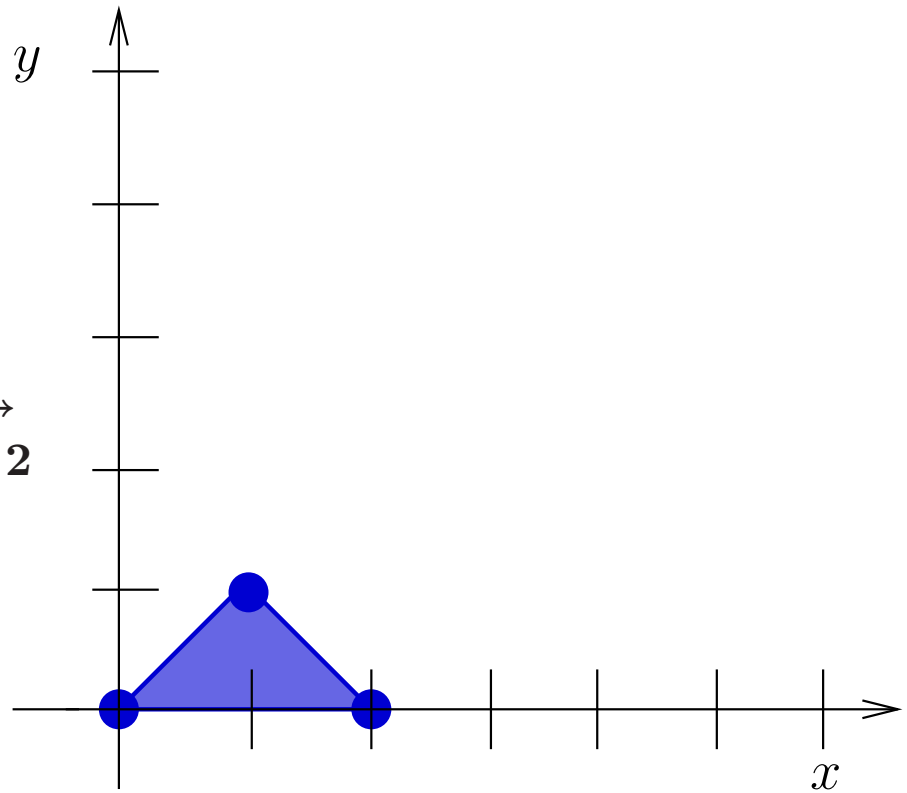
Un exemple - 2


p_{in}
$(x, y) := (0, 0)$
p
$x \leq 100 \rightarrow$
$x := x + 1$
$y := y + 1$
$x \leq 100 \rightarrow$
$x := x + 2$
$x > 100$
p_{out}

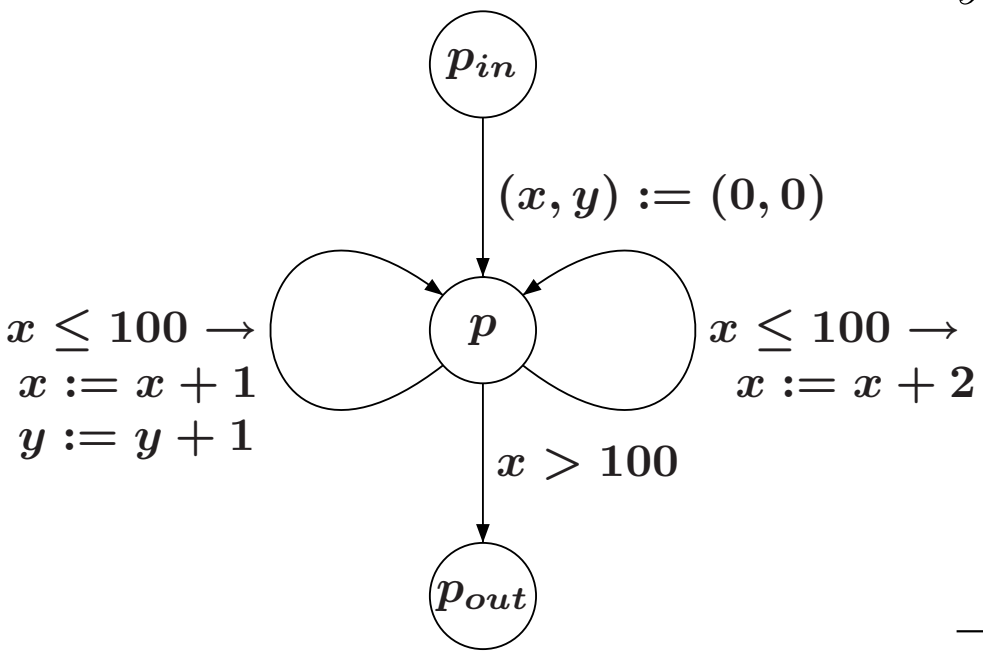

y
x

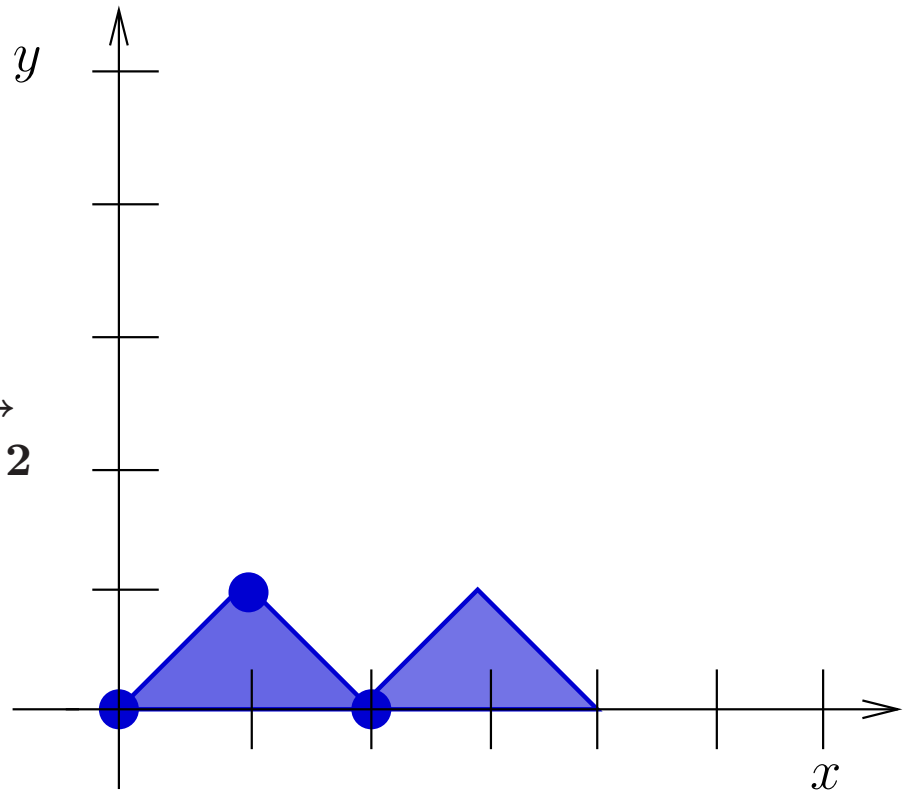
Un exemple - 2


p_{in}
$(x, y) := (0, 0)$
p
$x \leq 100 \rightarrow$
$x := x + 1$
$y := y + 1$
$x \leq 100 \rightarrow$
$x := x + 2$
$x > 100$
p_{out}

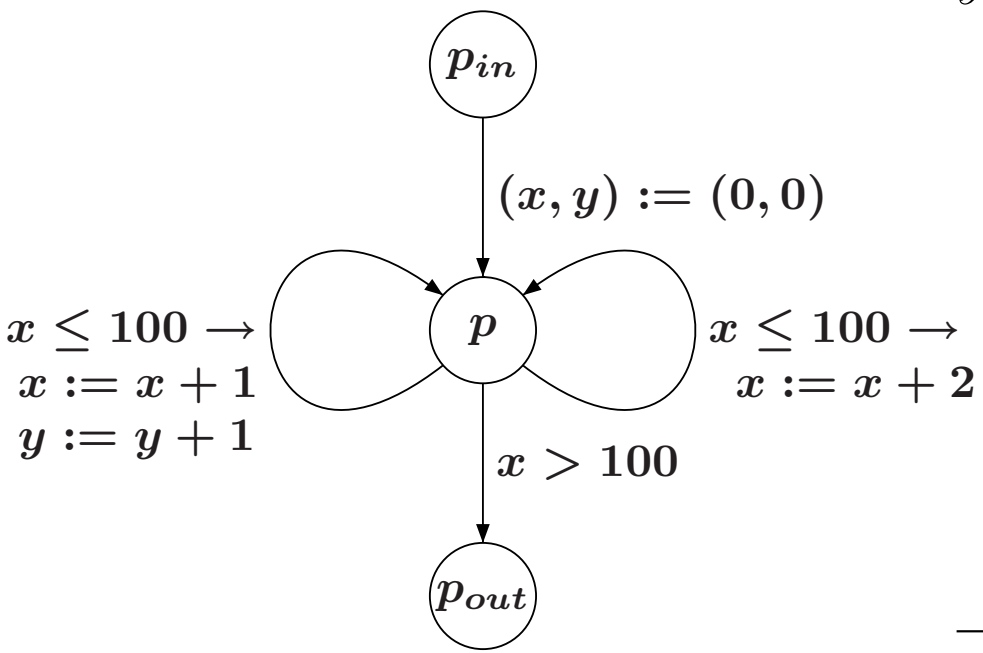

y
x

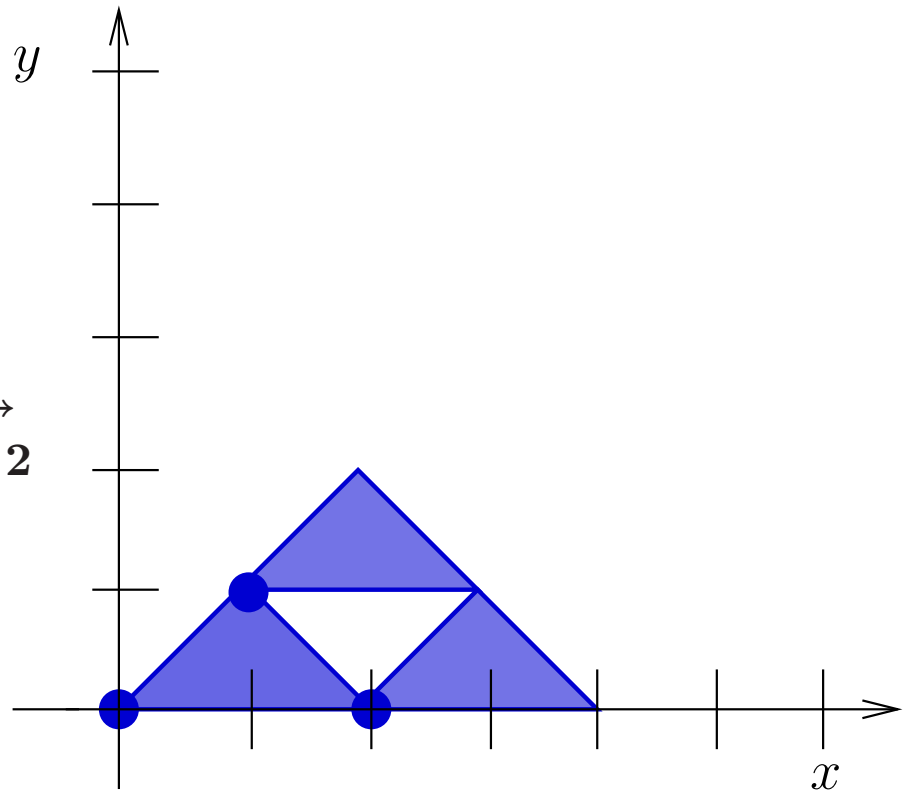
Un exemple - 2


p_{in}
$(x, y) := (0, 0)$
p
$x \leq 100 \rightarrow$
$x := x + 1$
$y := y + 1$
$x \leq 100 \rightarrow$
$x := x + 2$
$x > 100$
p_{out}

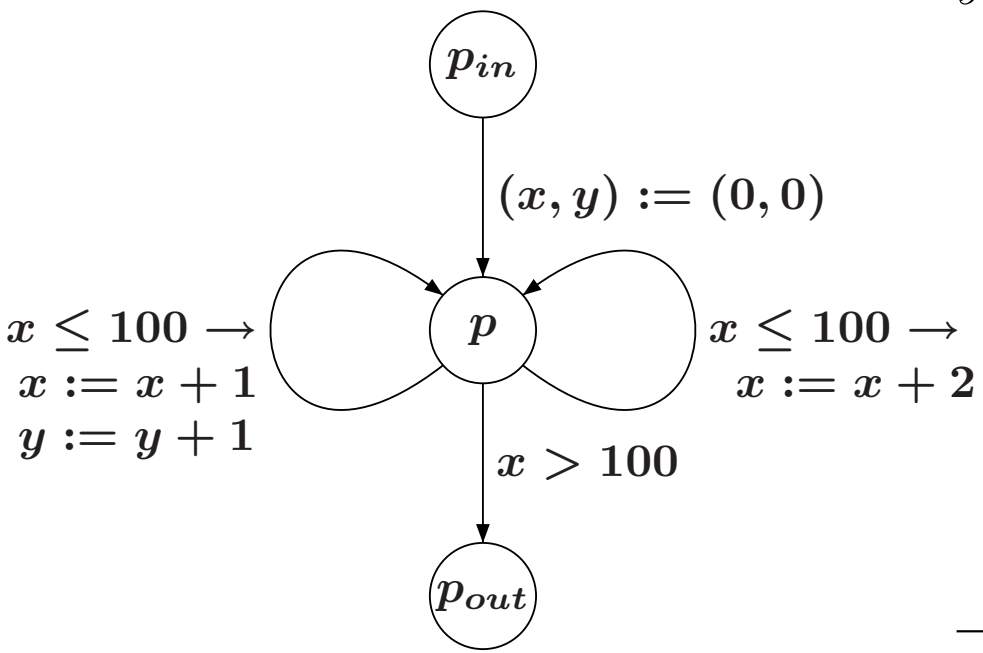

y
x

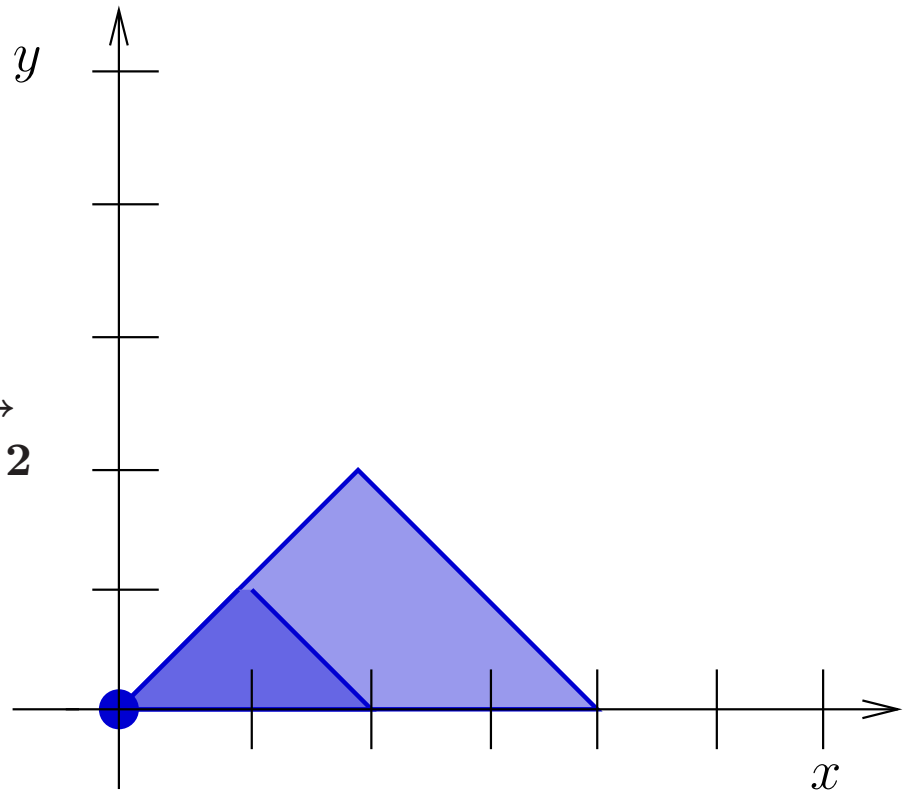
Un exemple - 2


p_{in}
$(x, y) := (0, 0)$
p
$x \leq 100 \rightarrow$
$x := x + 1$
$y := y + 1$
$x \leq 100 \rightarrow$
$x := x + 2$
$x > 100$
p_{out}

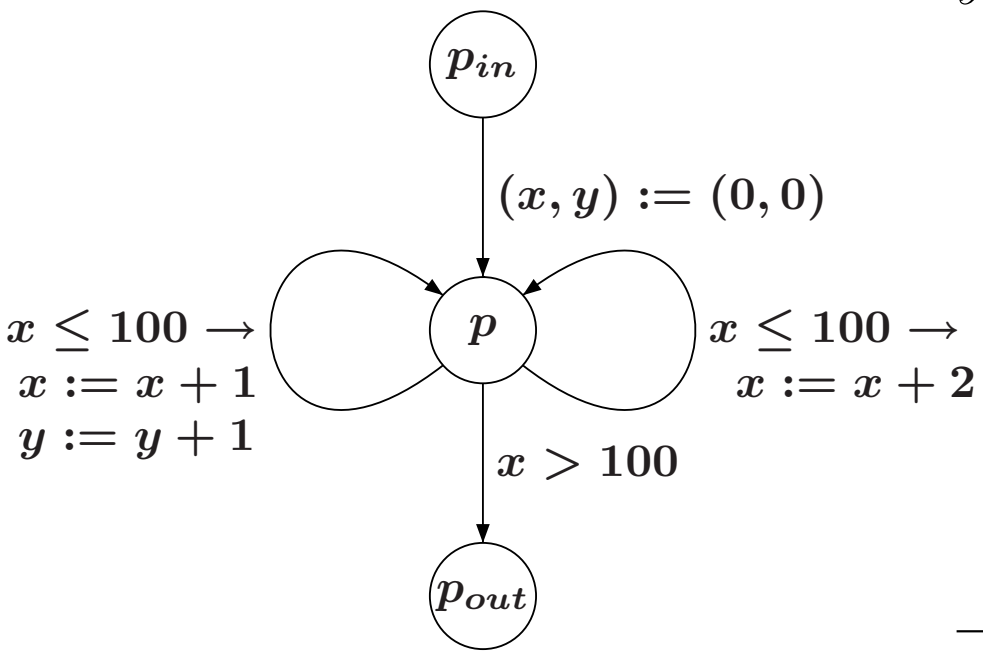

y
x

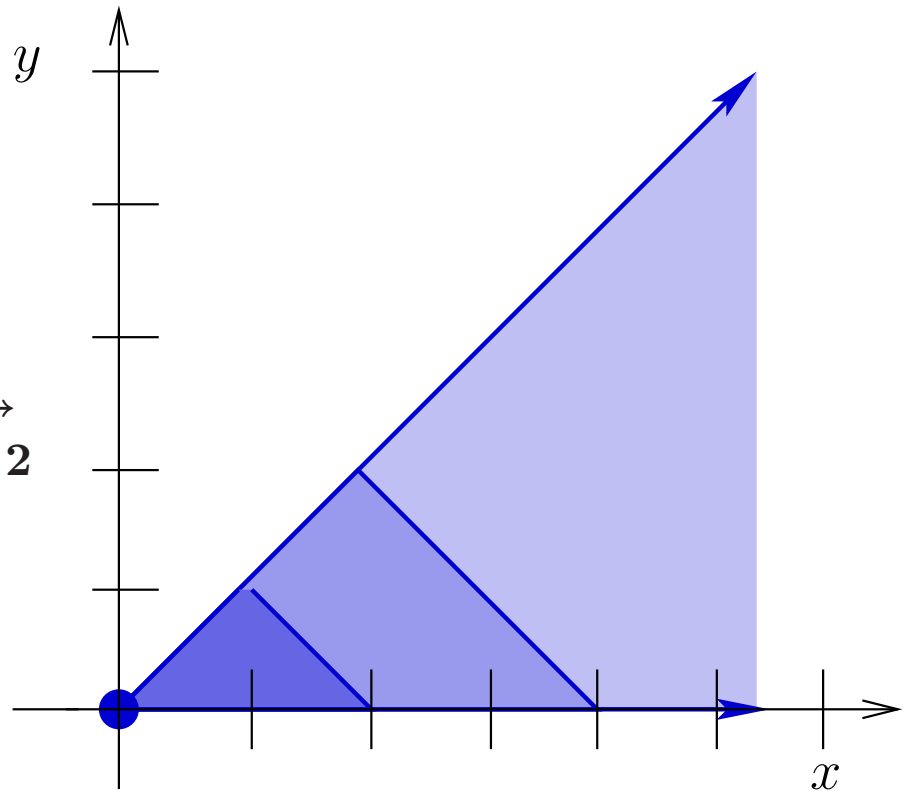
Un exemple - 2


p_{in}
$(x, y) := (0, 0)$
p
$x \leq 100 \rightarrow$
$x := x + 1$
$y := y + 1$
$x \leq 100 \rightarrow$
$x := x + 2$
$x > 100$
p_{out}


y
x

Un exemple - 2


p_{in}
$(x, y) := (0, 0)$
p
$x \leq 100 \rightarrow$
$x := x + 1$
$y := y + 1$
$x \leq 100 \rightarrow$
$x := x + 2$
$x > 100$
p_{out}


y
x

Les problèmes de l'Analyse des Relations Linéaires

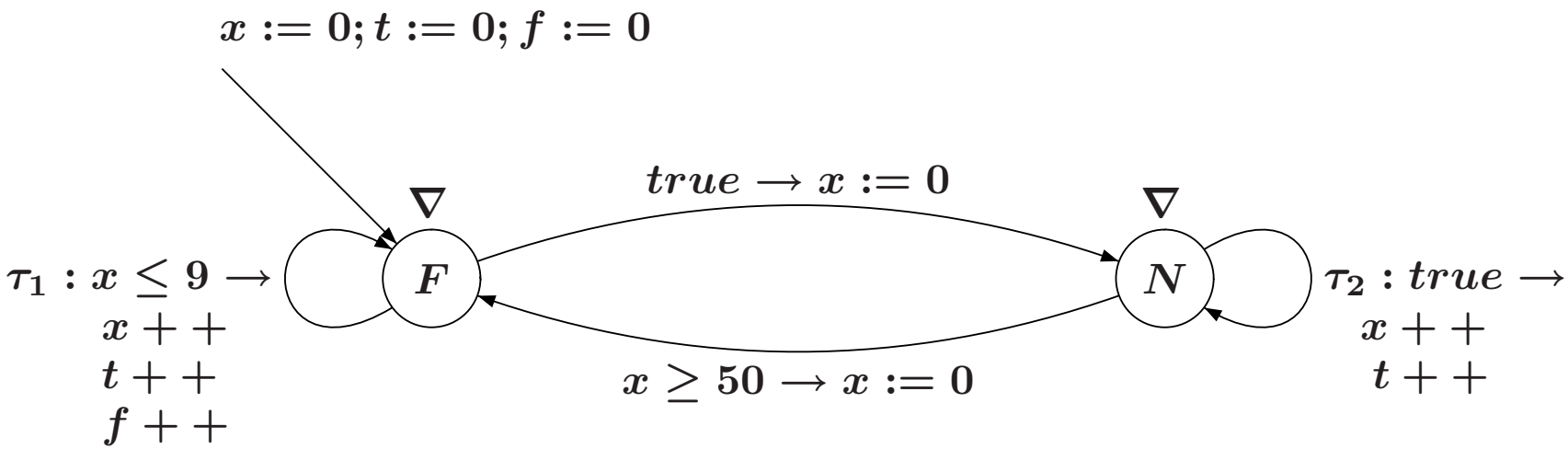
Sources de complexité :

- nombre de points de contrôle.
- nombre de variables numériques.

Sources d'approximation :

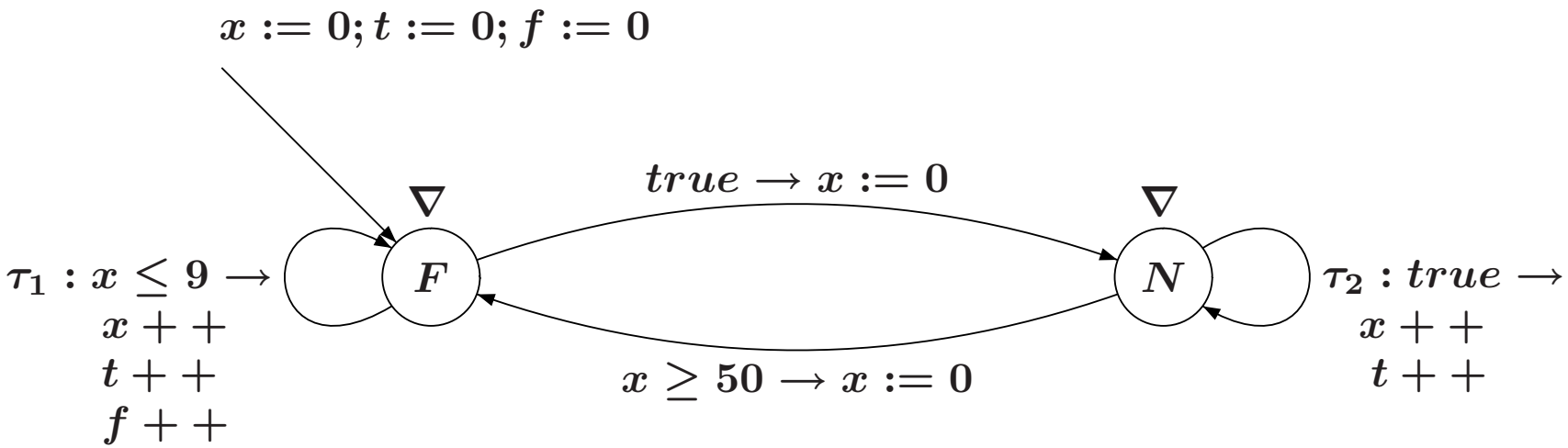
- Enveloppe convexe.
- **Élargissement**.

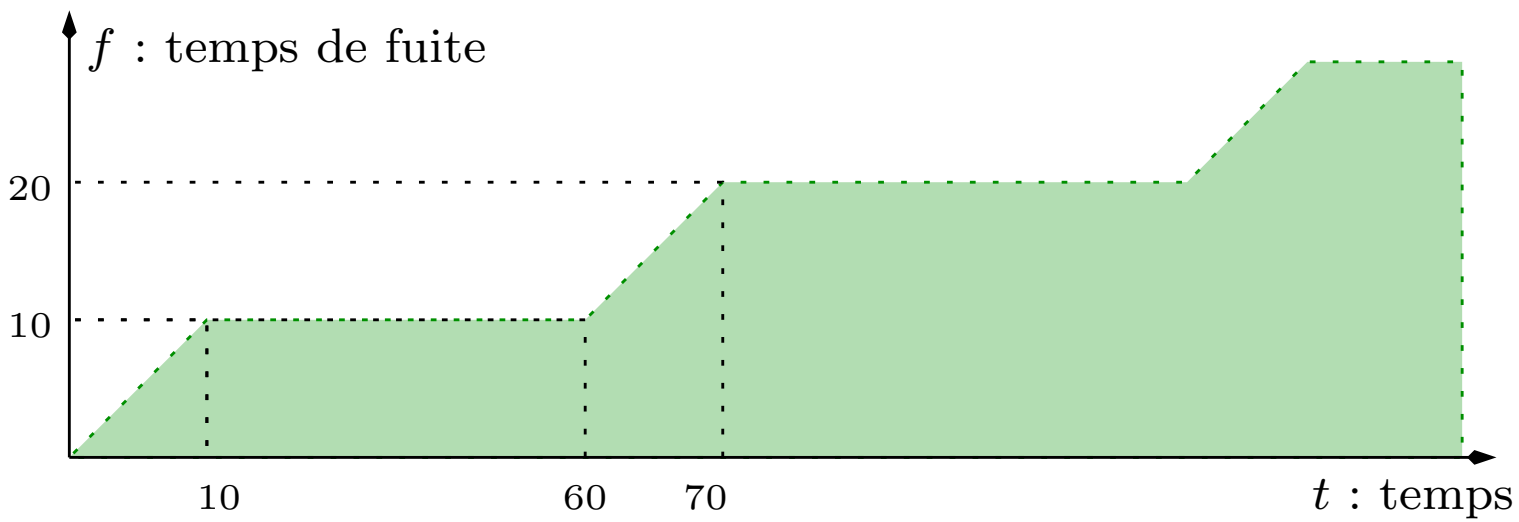
L'exemple de la chaudière - 1



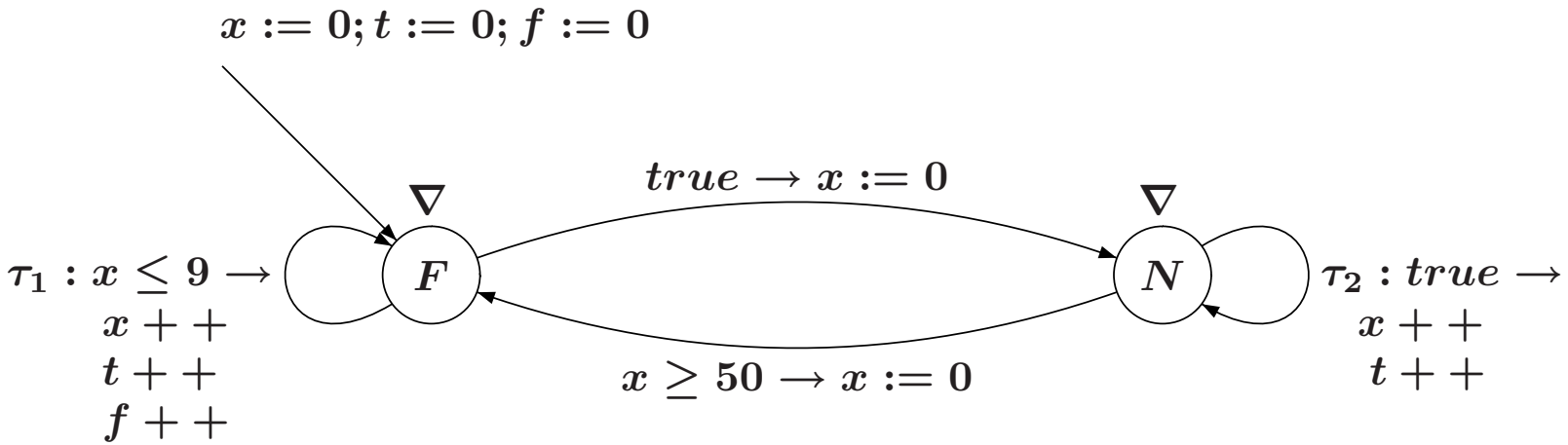
- f le temps de fuite global.
- t le temps global.
- x variable locale.

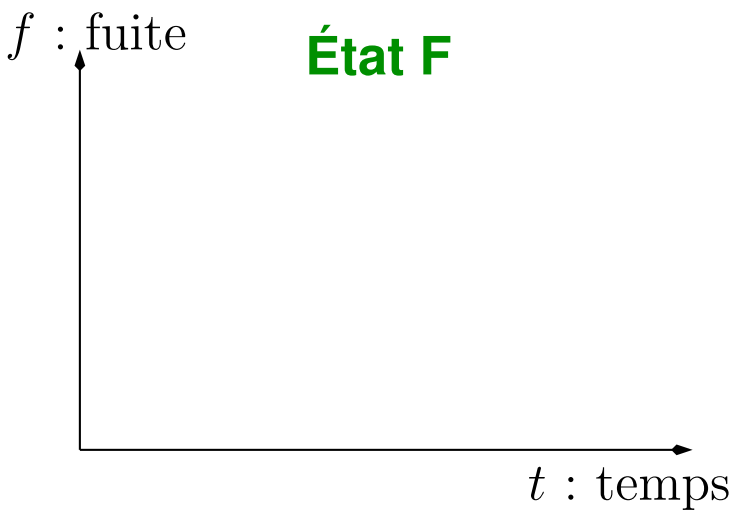
La chaudière 2 - Comportement réel

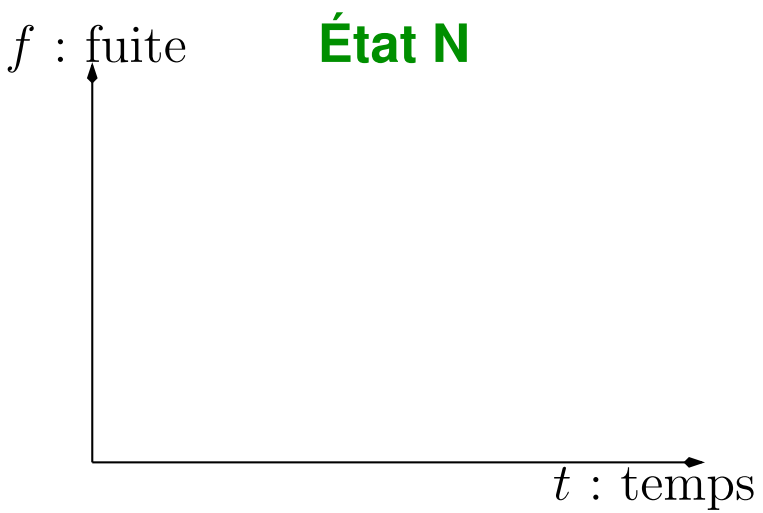




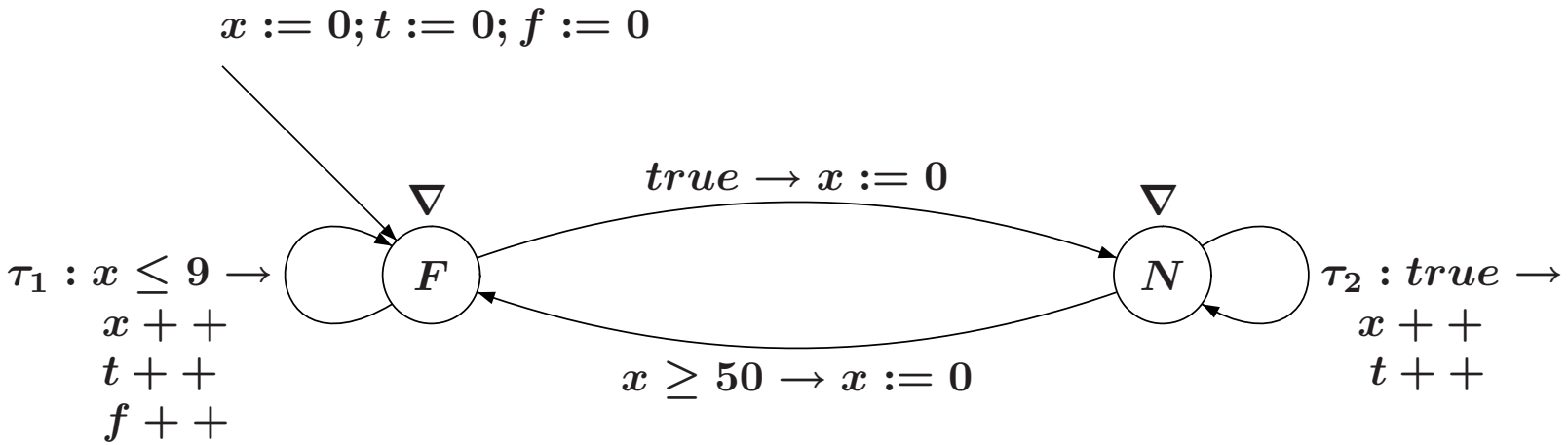
La chaudière 3 - Analyse des Relations Linéaires

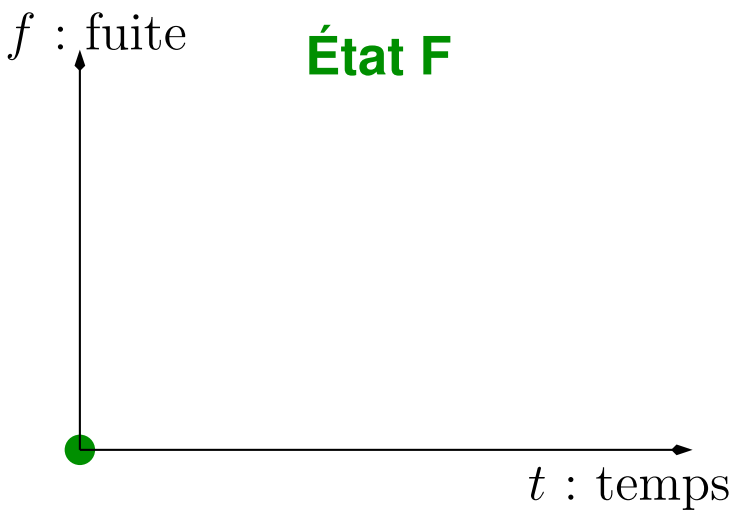


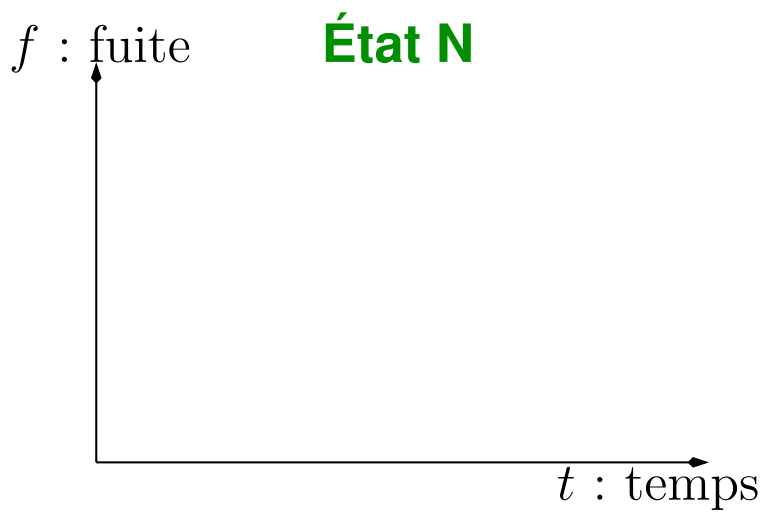




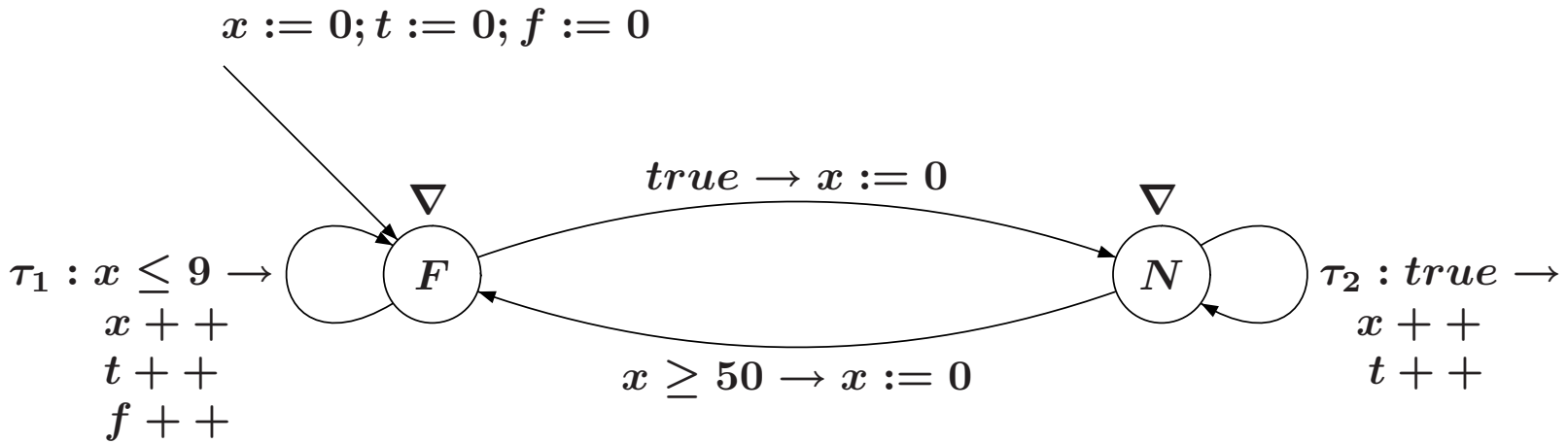
La chaudière 3 - Analyse des Relations Linéaires

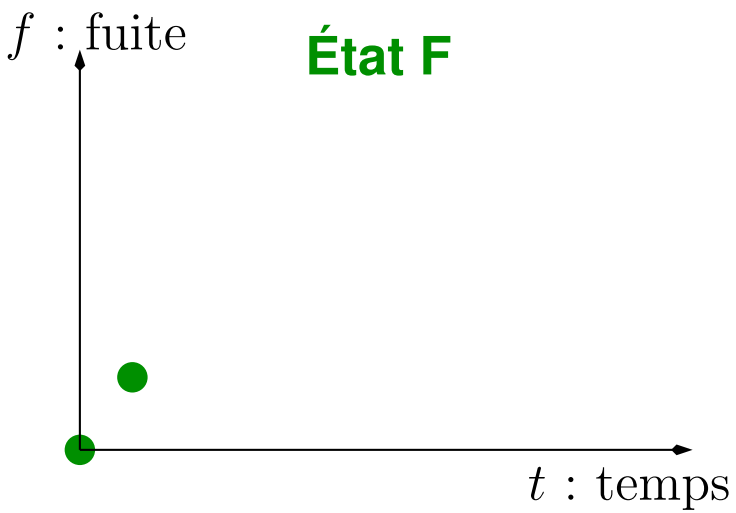


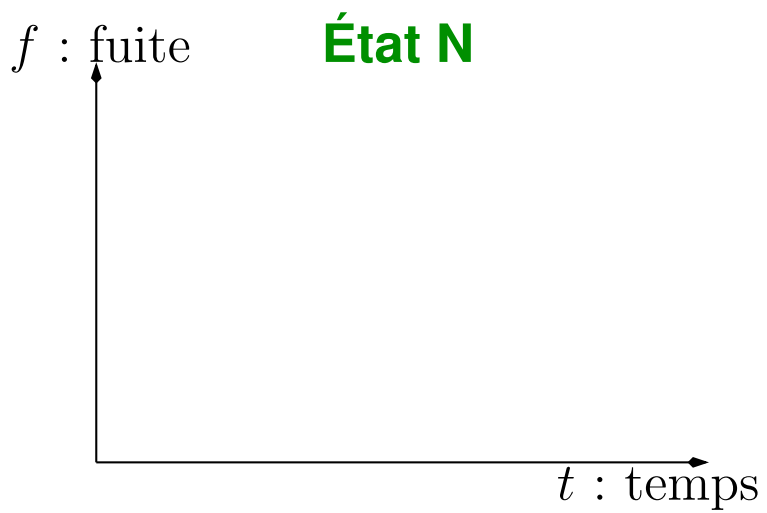




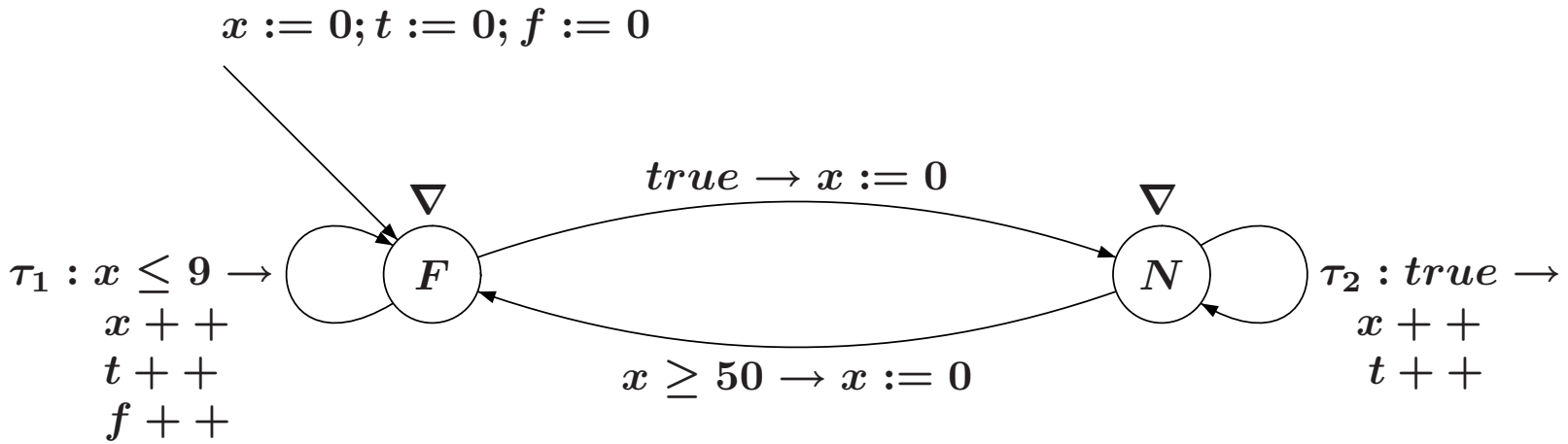
La chaudière 3 - Analyse des Relations Linéaires

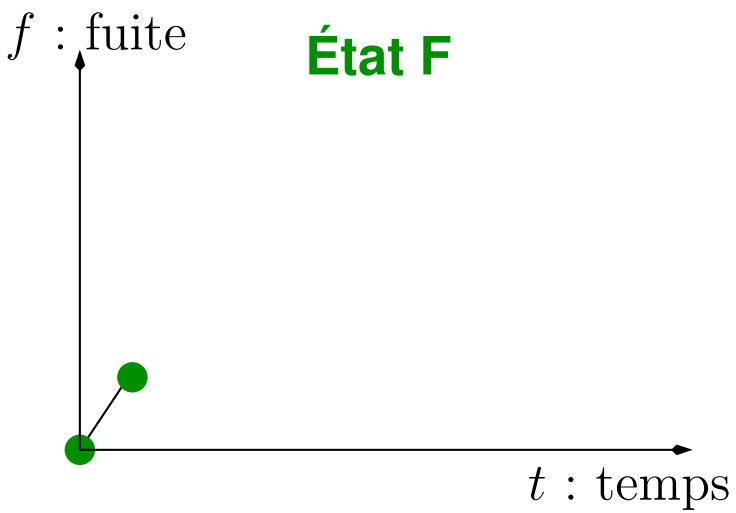


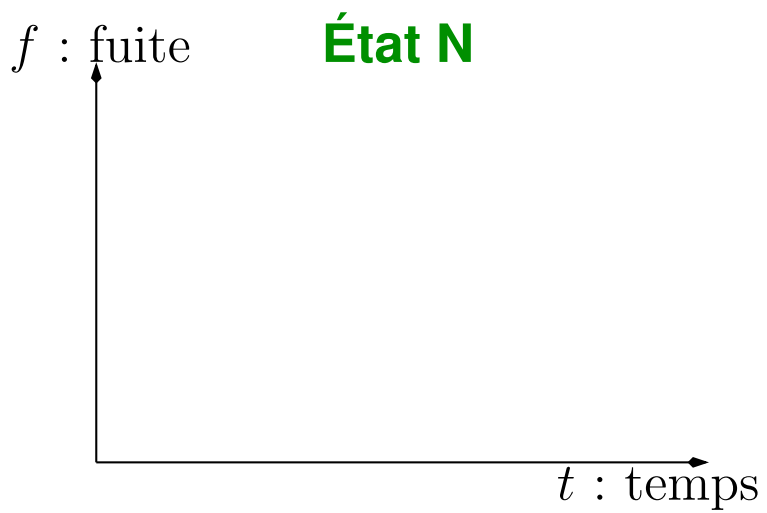




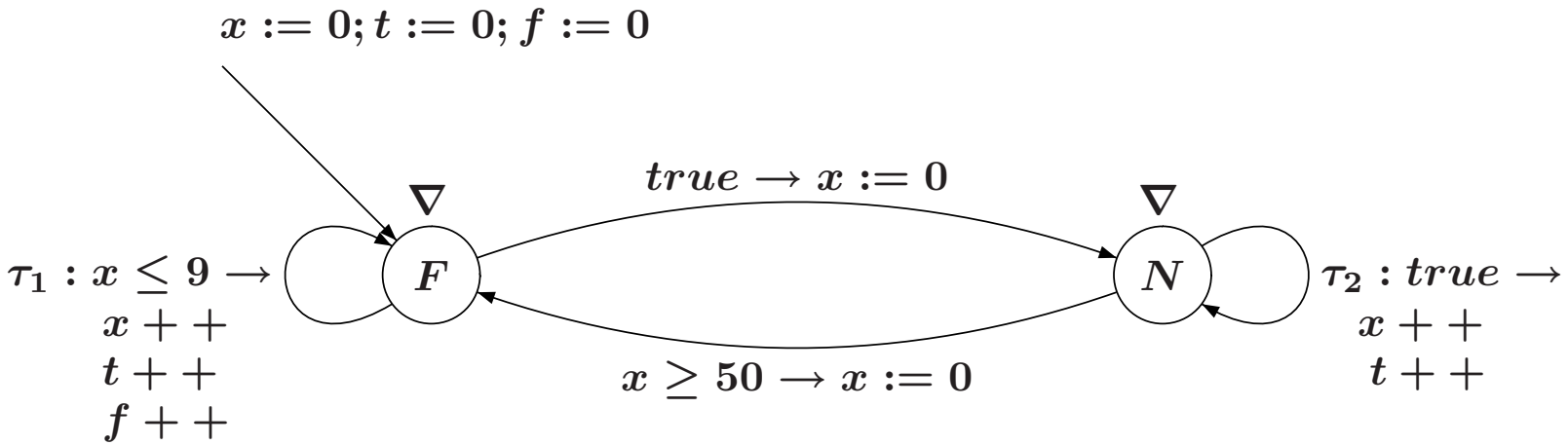
La chaudière 3 - Analyse des Relations Linéaires

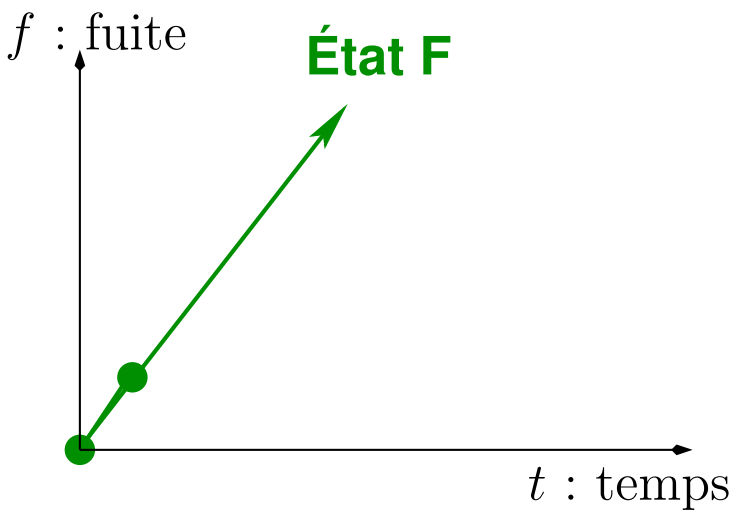


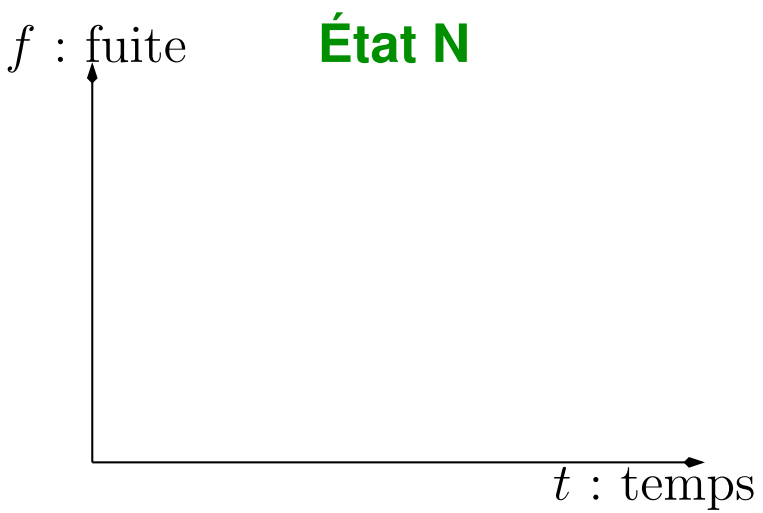




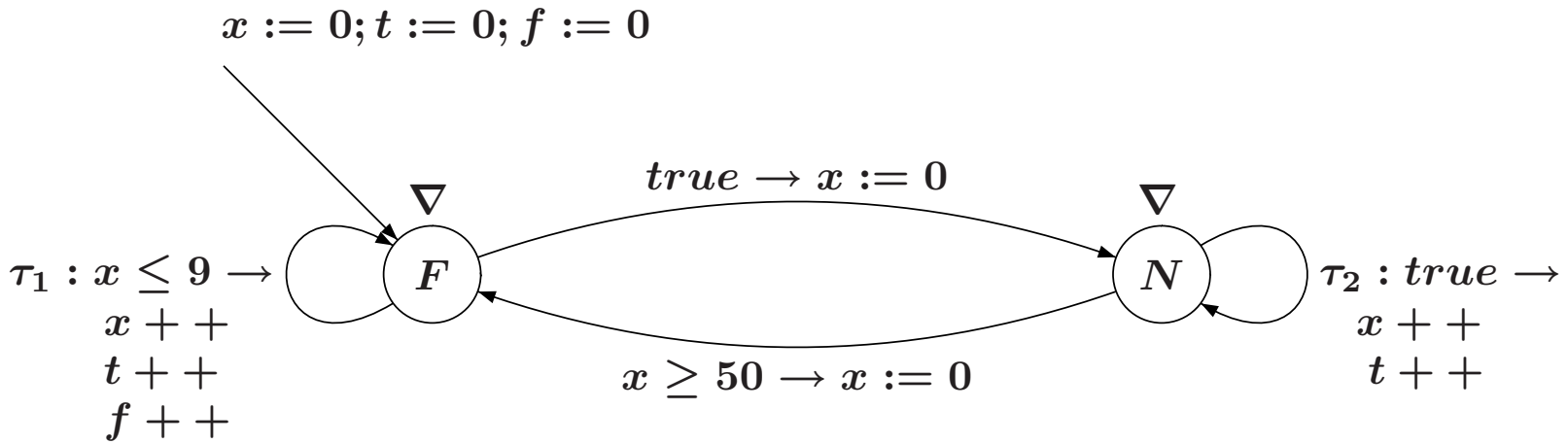
La chaudière 3 - Analyse des Relations Linéaires

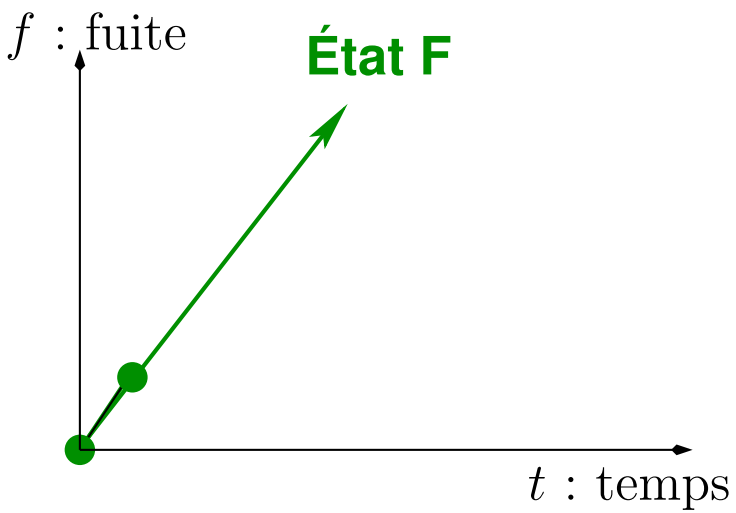


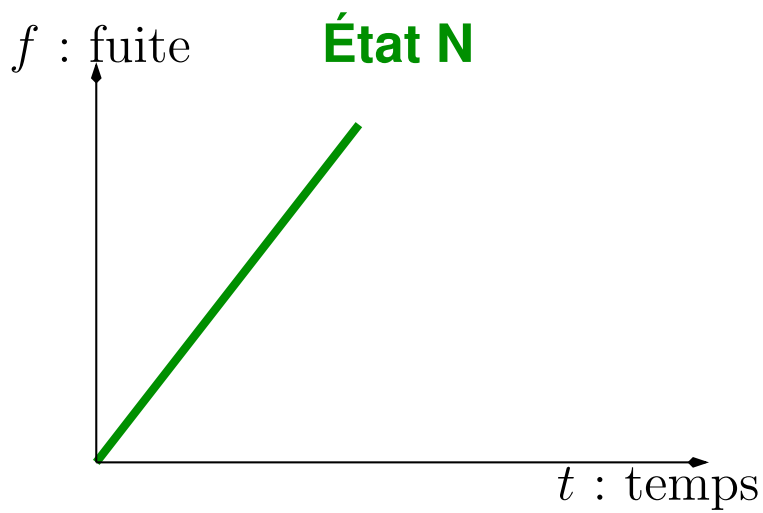




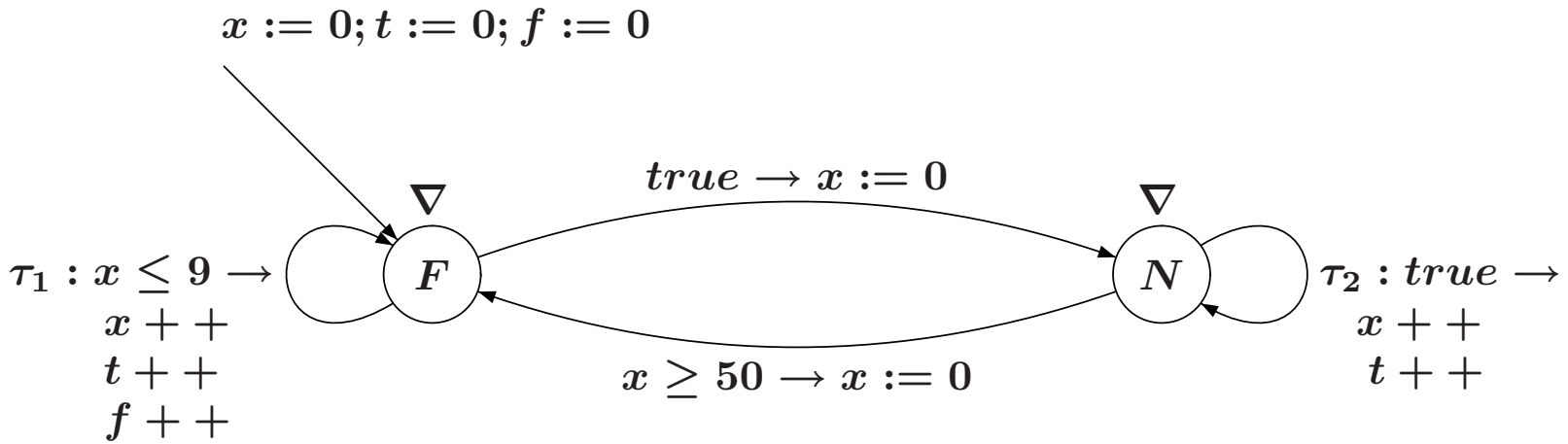
La chaudière 3 - Analyse des Relations Linéaires

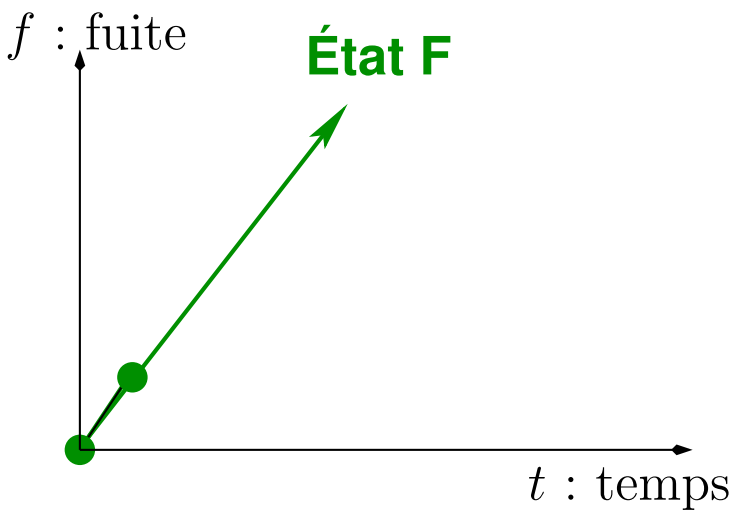


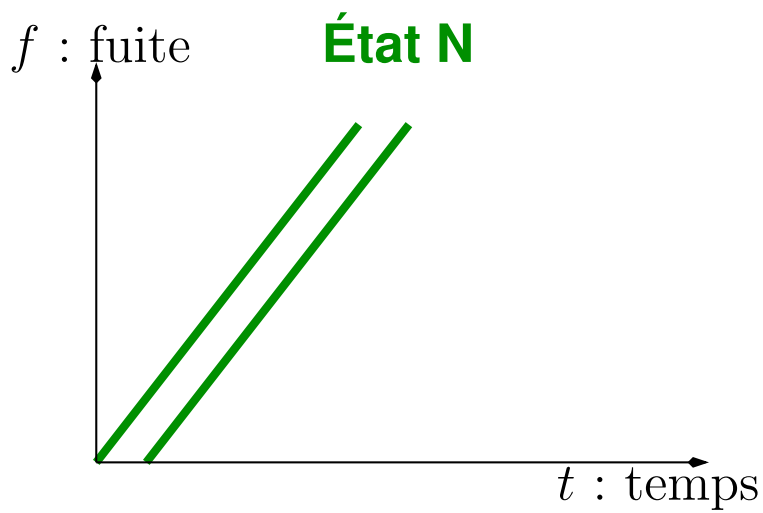




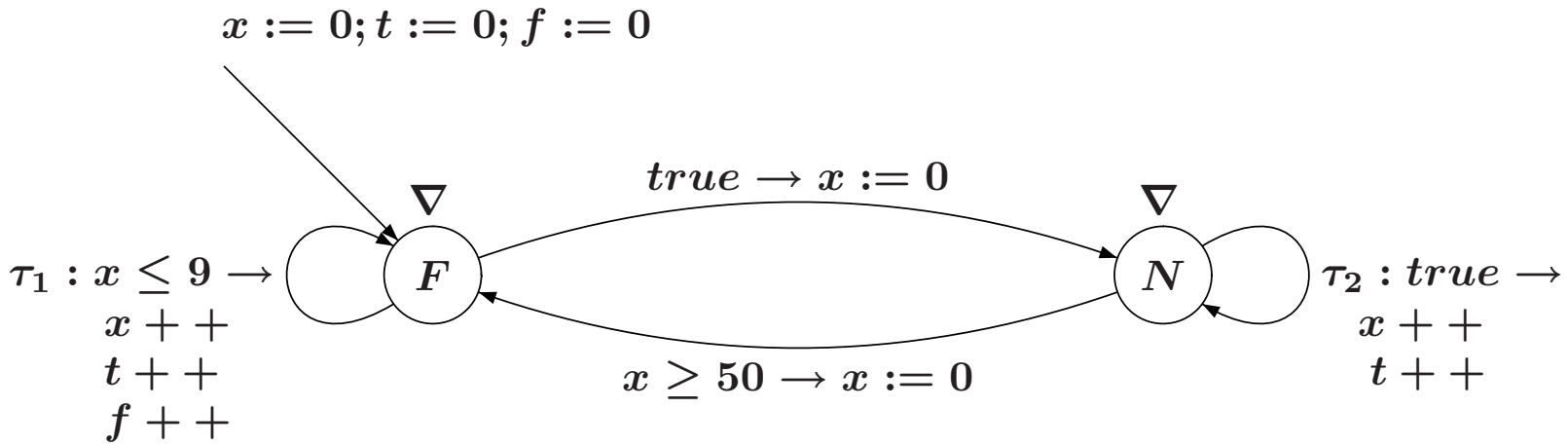
La chaudière 3 - Analyse des Relations Linéaires

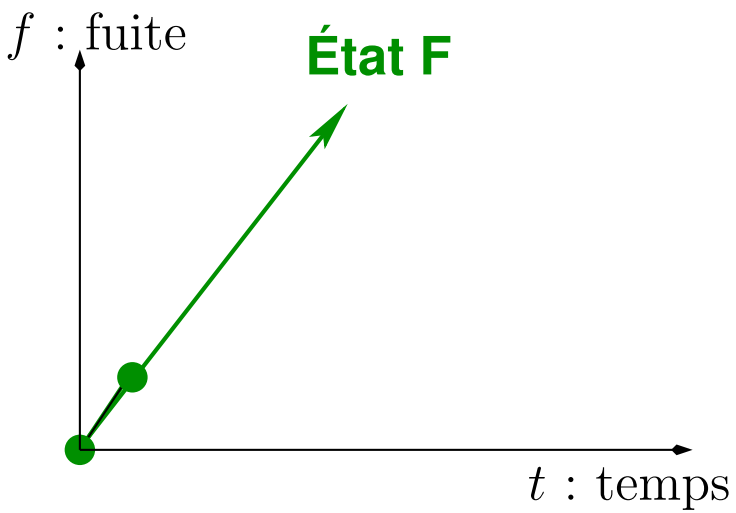


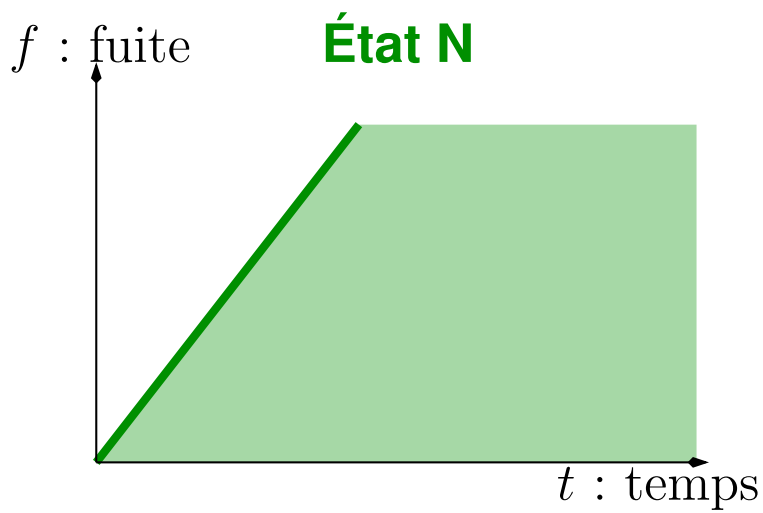




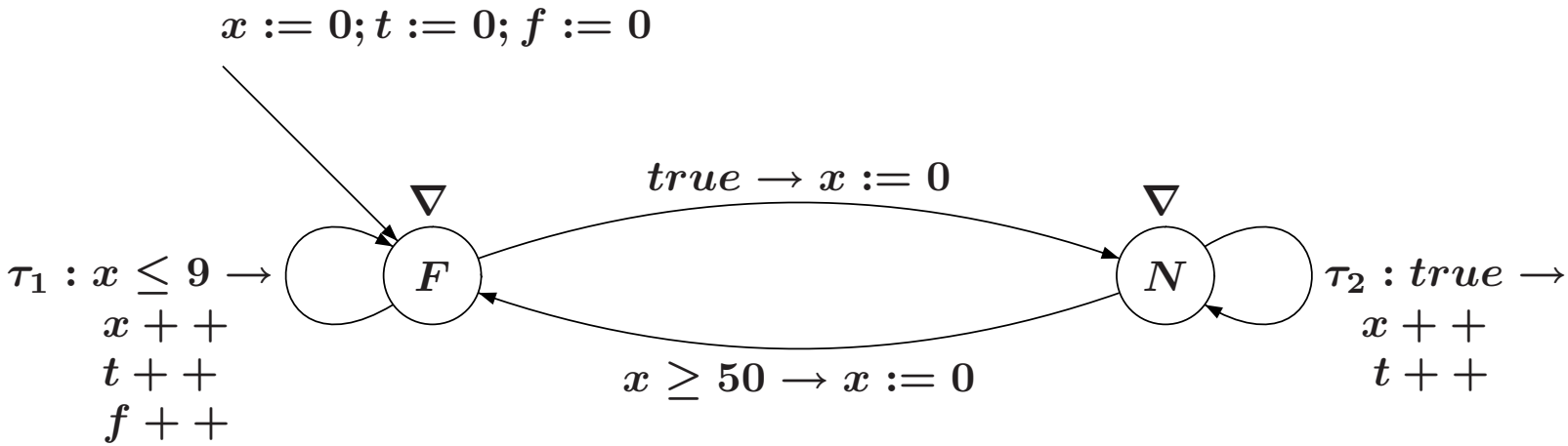
La chaudière 3 - Analyse des Relations Linéaires

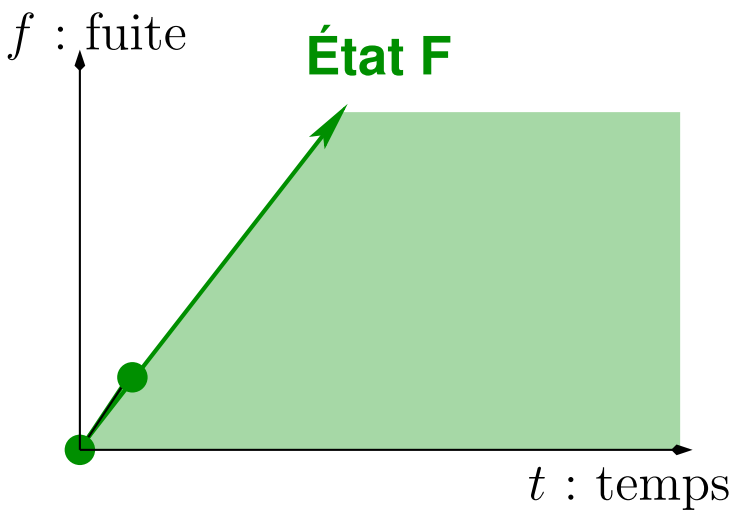


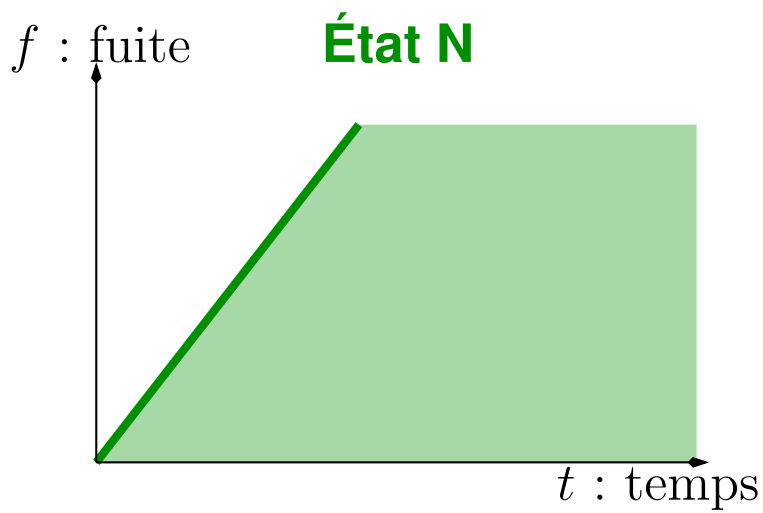




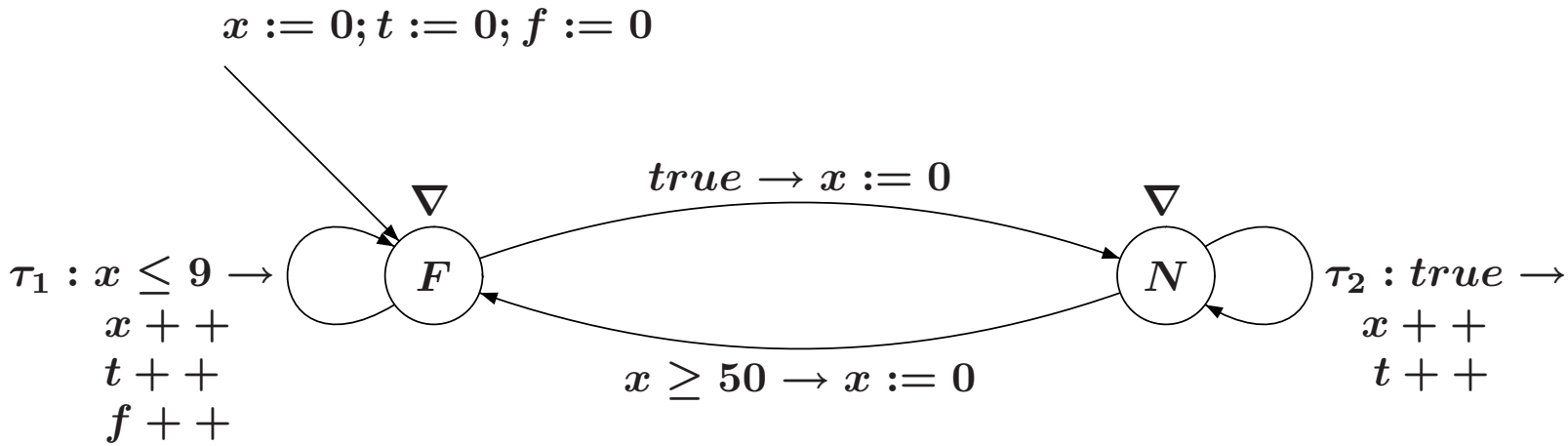
La chaudière 3 - Analyse des Relations Linéaires

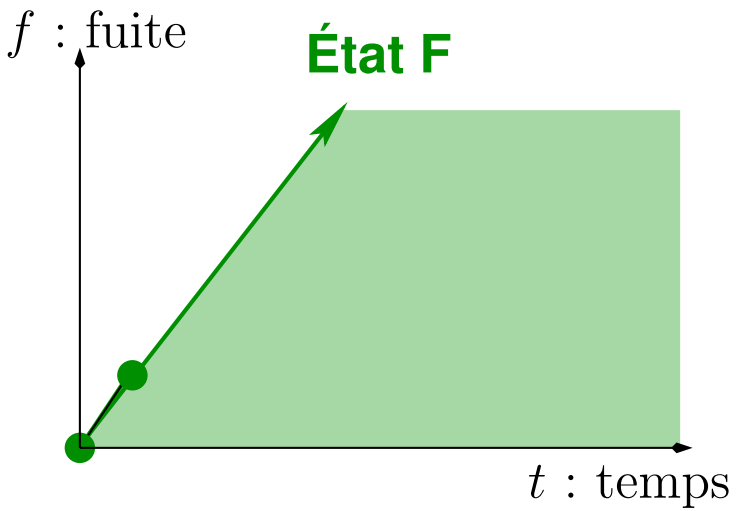


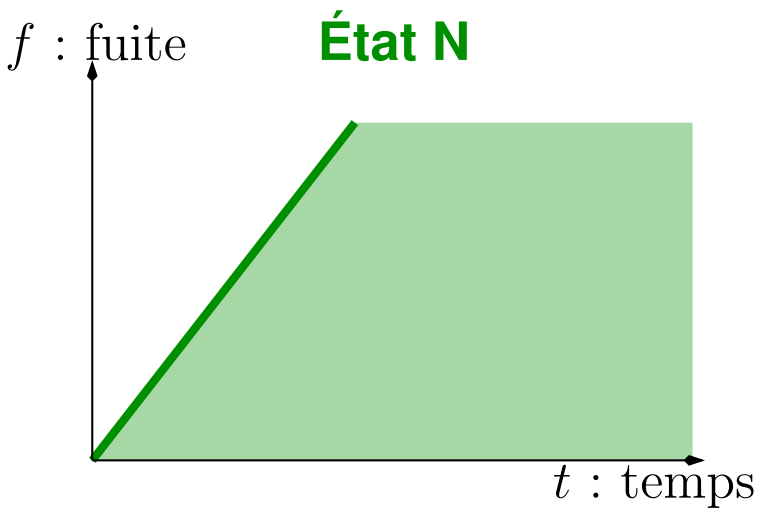




La chaudière 3 - Analyse des Relations Linéaires

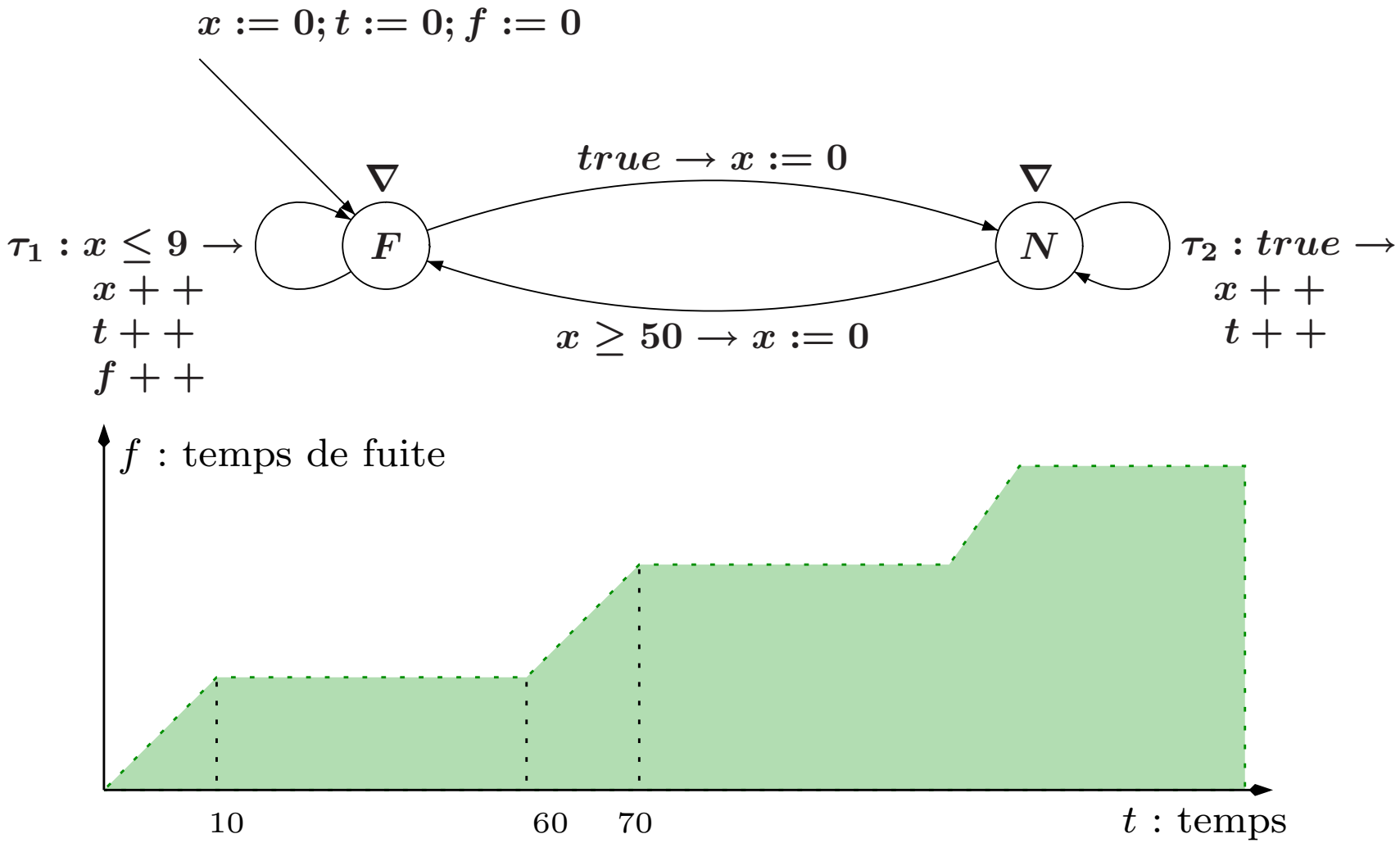




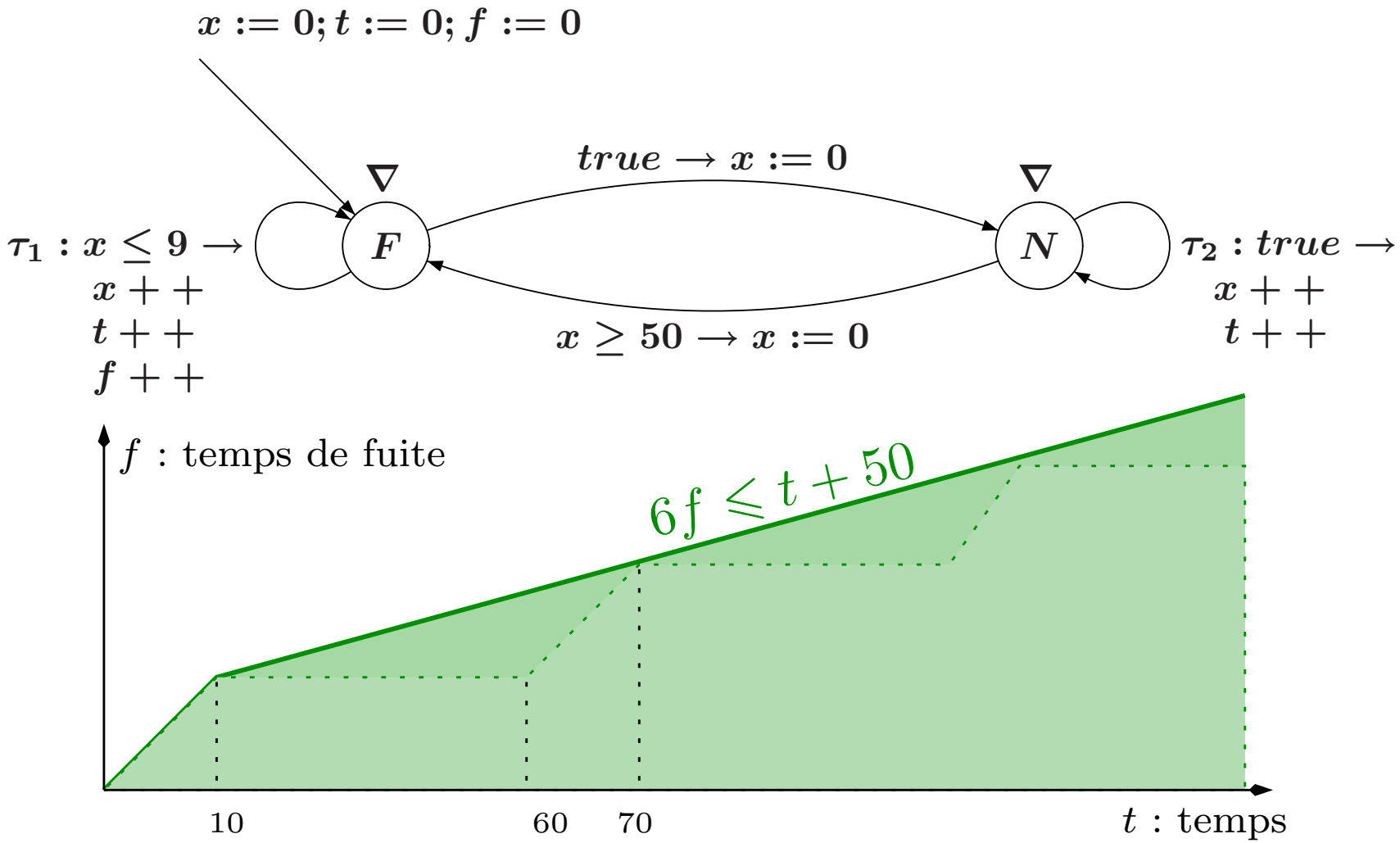


- Convergence, approximation supérieure, mais manque de précision.

La chaudière - Invariant voulu



La chaudière - Invariant voulu



Amélioration de la précision

Des méthodes existent mais sont **adhoc** (en général).

- Regardons les méthodes **exactes (accélération)** :
  - On calcule l'effet exact des boucles sur des ensembles d'**entiers**.
  - Codage sous forme d'automates représentant des formules de Presburger, par ex : $\exists k, x = y + 2k$.

Amélioration de la précision

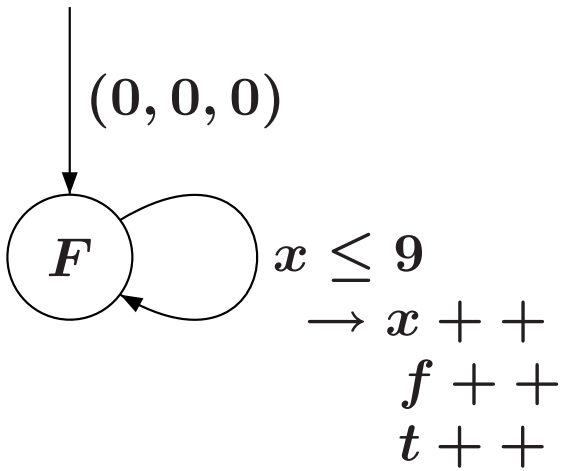
Des méthodes existent mais sont **adhoc** (en général).

- Regardons les méthodes **exactes (accélération)** :
  - On calcule l'effet exact des boucles sur des ensembles d'**entiers**.
  - Codage sous forme d'automates représentant des formules de Presburger, par ex : $\exists k, x = y + 2k$.

- Inconvénients : classes restreintes de programmes, haute complexité.

Exemple de la chaudière (3)

La boucle est « accélérable » :



- Effet **exact** : $\exists i \in \mathbb{N}, x = f = t = i, 0 \leqslant i \leqslant 10$

Accélération et Analyse des Relations Linéaires

Définition de la notion d'accélération abstraite qui :

- Permet d'obtenir des approximations supérieures à faible coût.
- Se combine bien avec l'élargissement.

Accélération et Analyse des Relations Linéaires

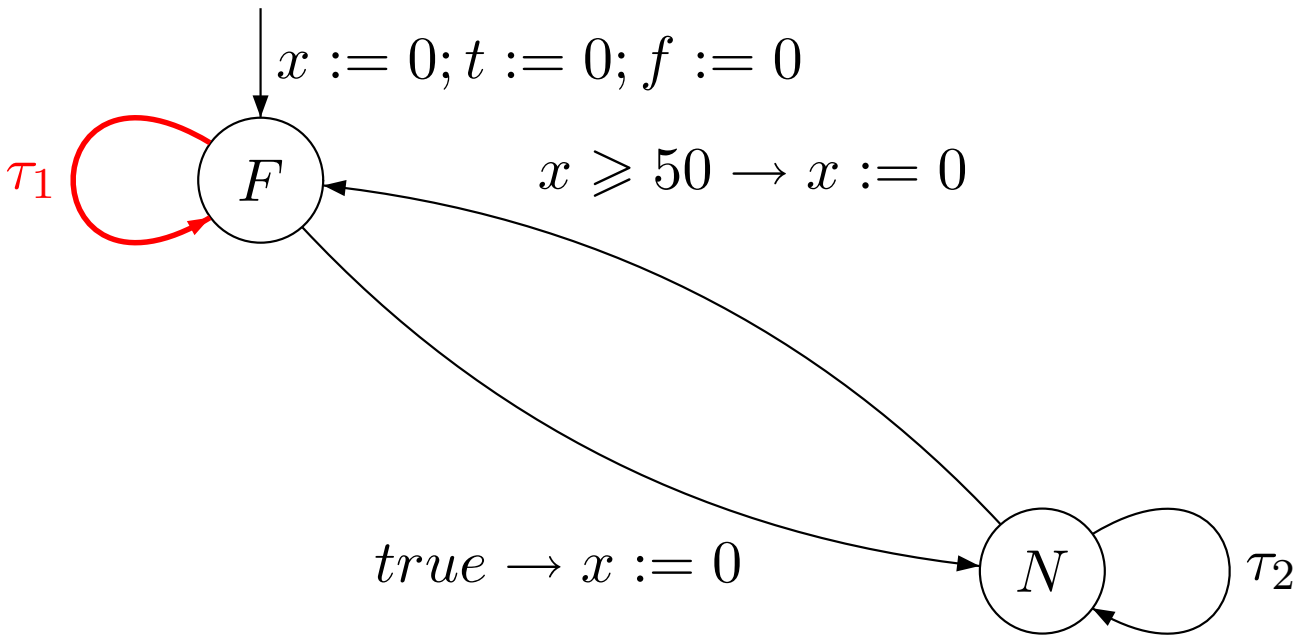
Définition de la notion d'accélération abstraite qui :

- Permet d'obtenir des approximations supérieures à faible coût.
- Se combine bien avec l'élargissement.

- cf SAS 2006

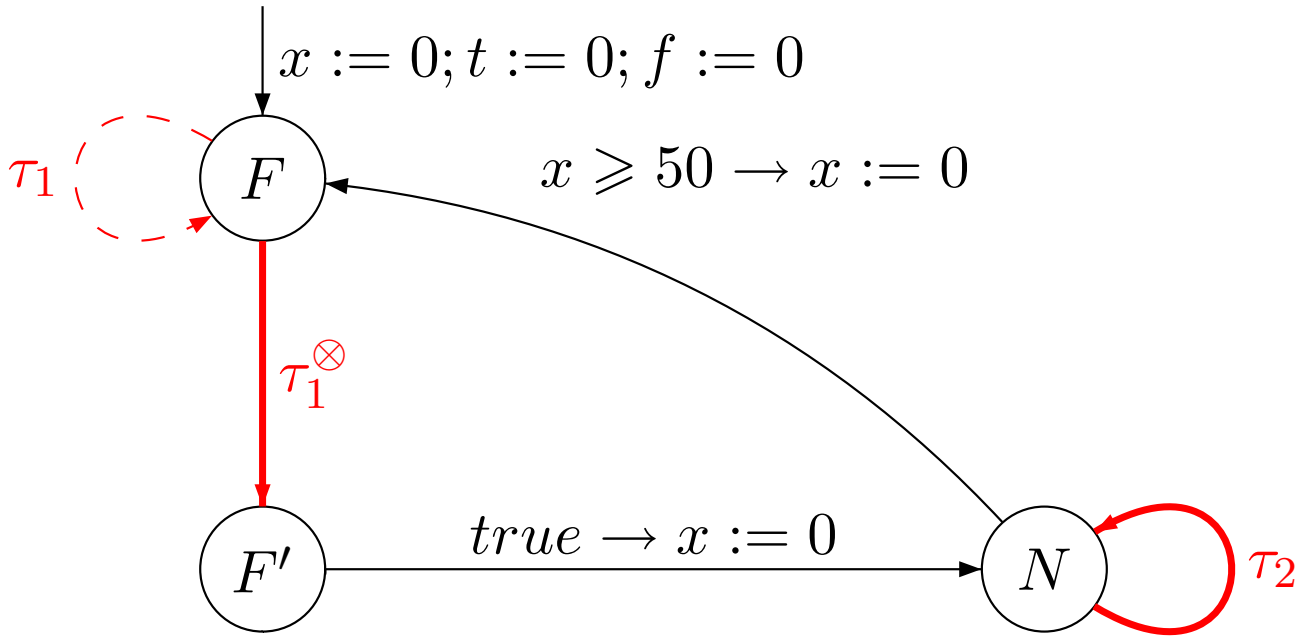
Accélération et partitionnement

On remplace les boucles ($\tau_i : g_i \rightarrow a_i$)



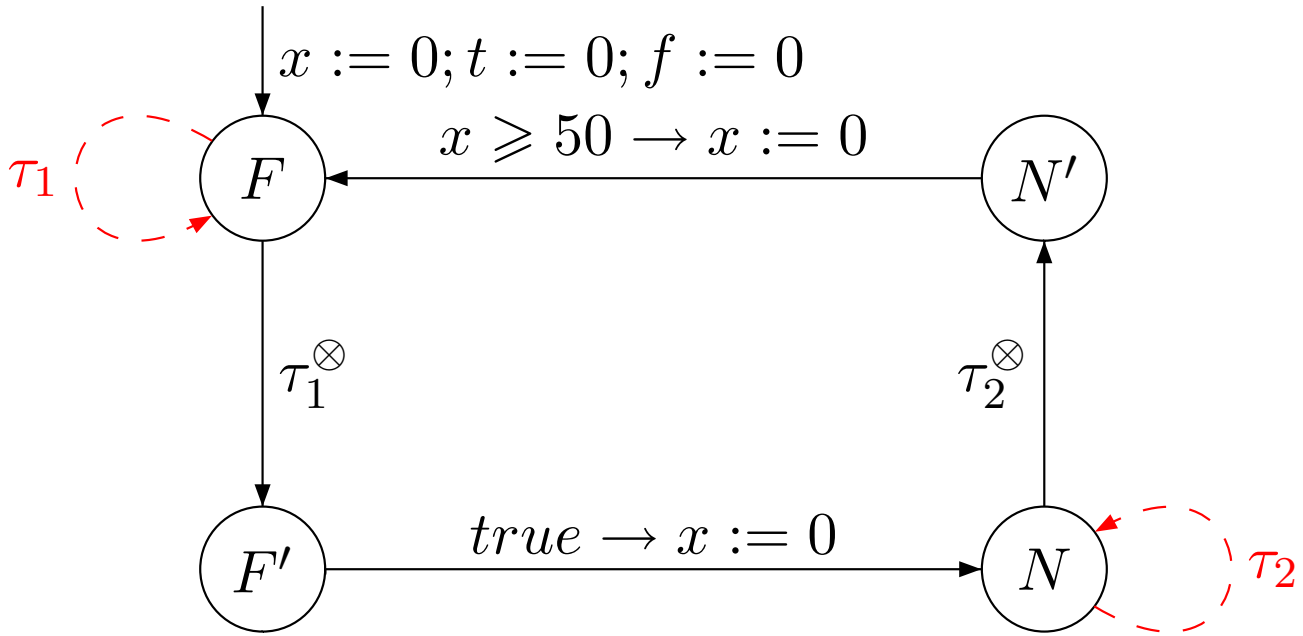
Accélération et partitionnement

On remplace les boucles ($\tau_i : g_i \rightarrow a_i$)



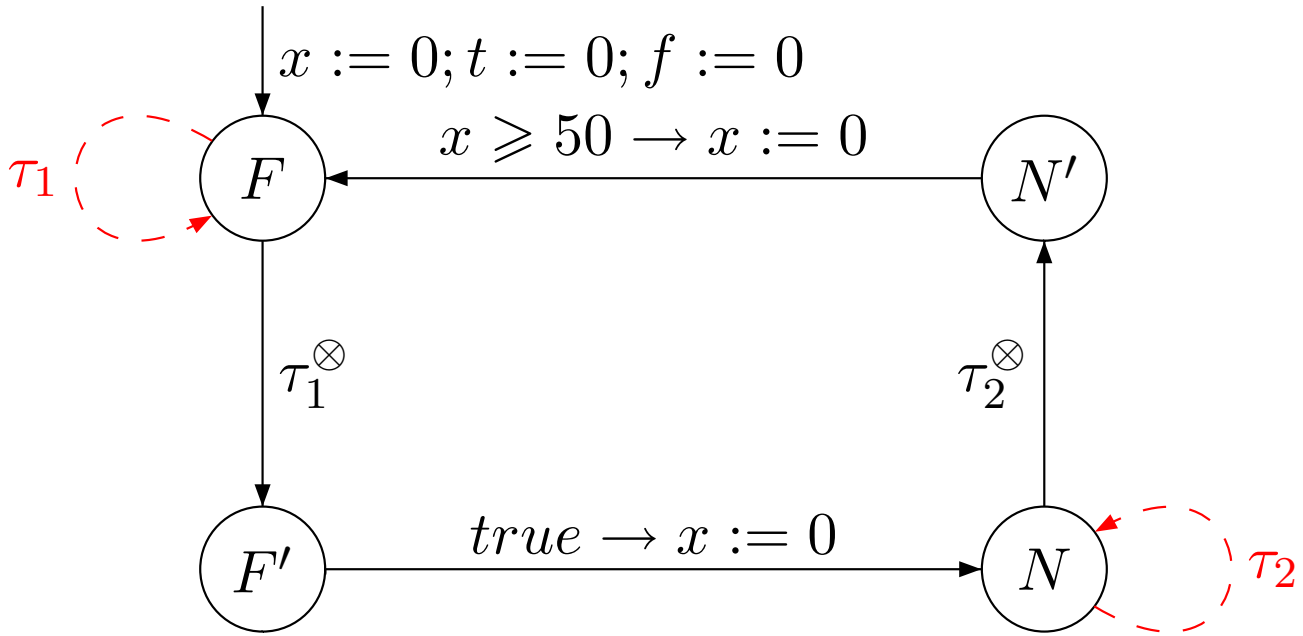
Accélération et partitionnement

On remplace les boucles ($\tau_i : g_i \rightarrow a_i$)



Accélération et partitionnement

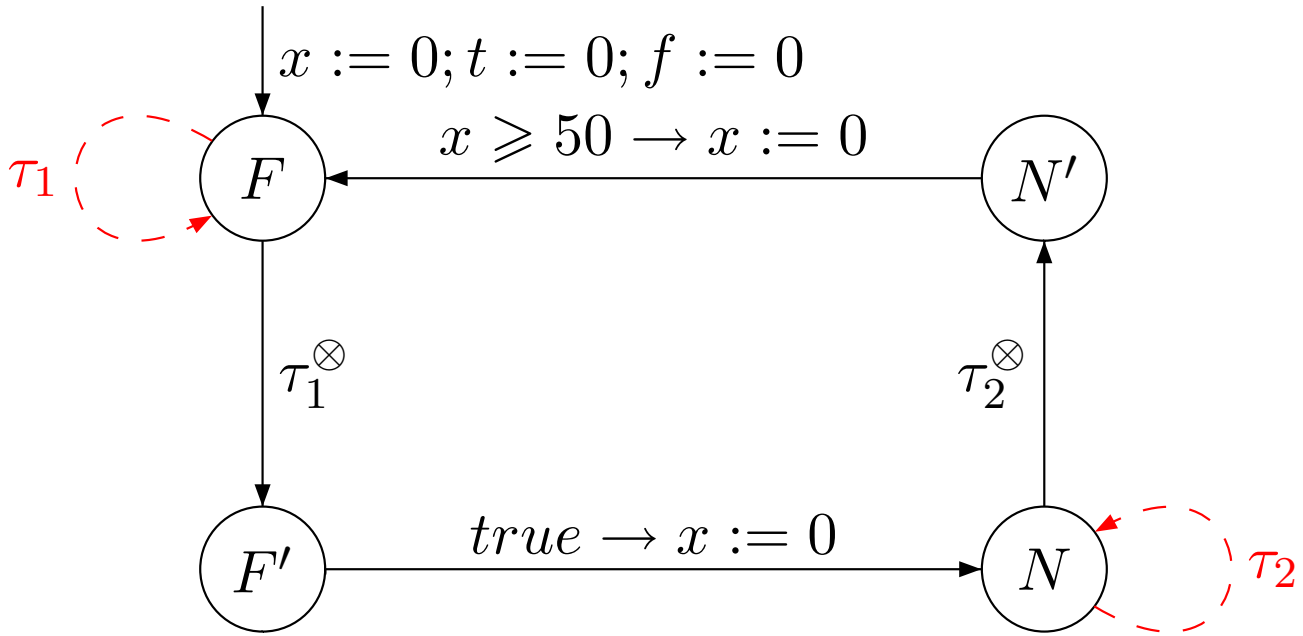
On remplace les boucles ($\tau_i : g_i \rightarrow a_i$)



- $\tau_i^{\otimes}$ résume l'effet d'une application de τ_i un **nombre quelconque de fois**

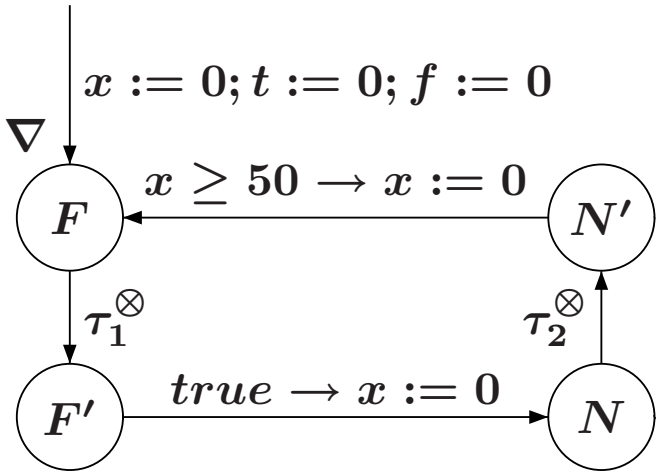
Accélération et partitionnement

On remplace les boucles ($\tau_i : g_i \rightarrow a_i$)

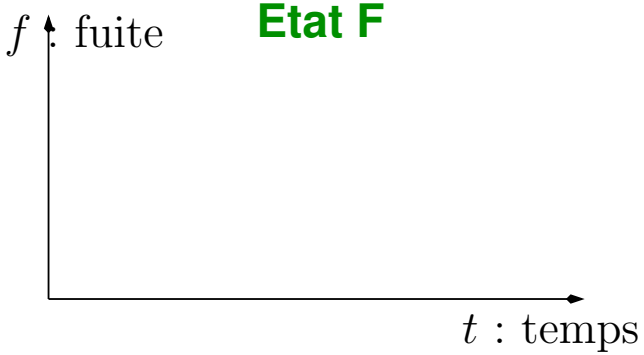


- $\tau_i^{\otimes}$ résume l'effet d'une application de τ_i un **nombre quelconque de fois**
- Boucle englobante : **accélérée** ou **élargie**.

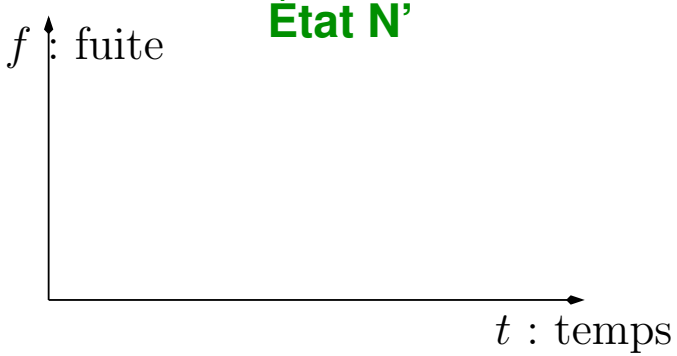
Le retour de la chaudière



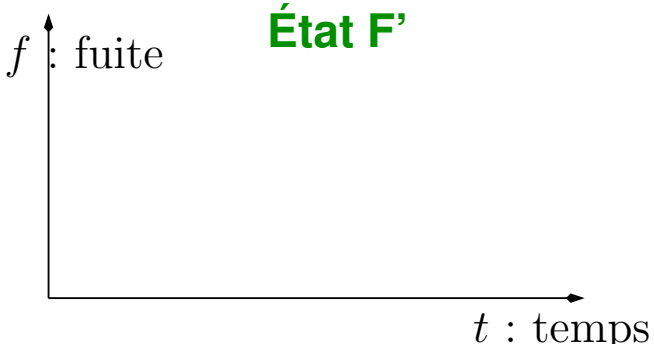
- $\tau_1^{\otimes}$ = “ajoute le rayon $(1, 1, 1)$ tant que $x \leqslant 10$”
- $\tau_2^{\otimes}$ = “ajoute le rayon $(1, 0, 1)$”



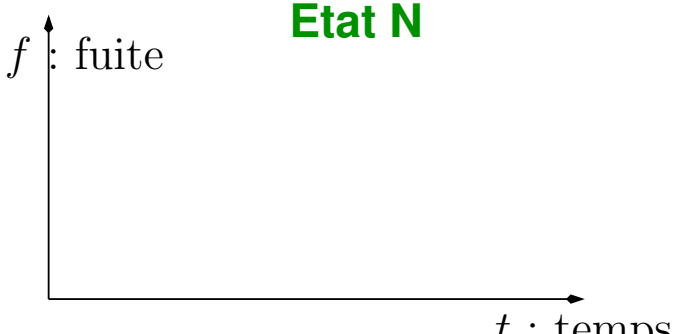
État F



État N’

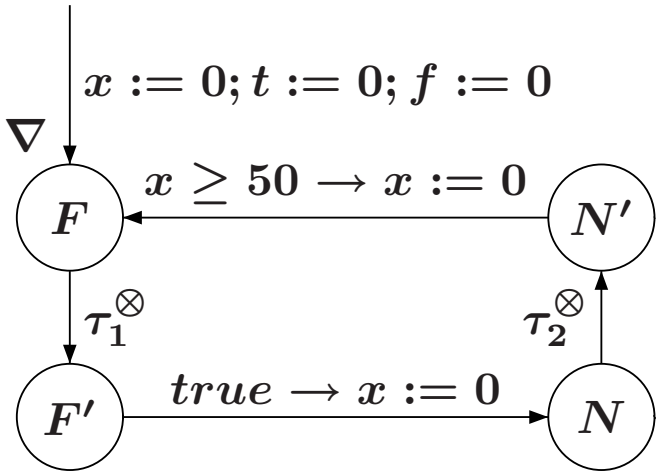


État F’

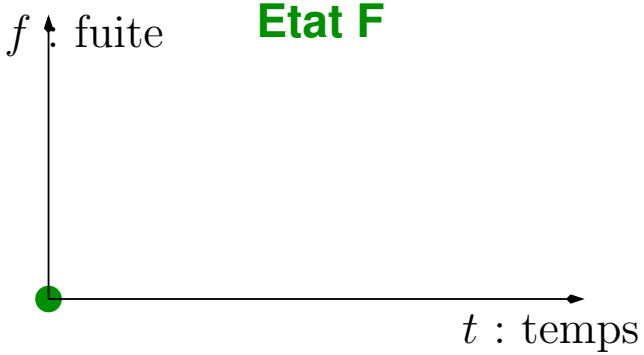


État N

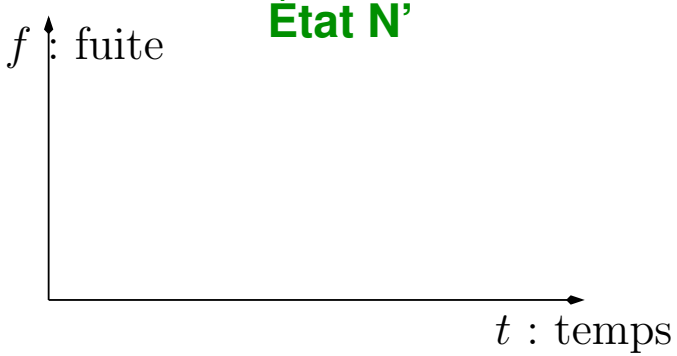
Le retour de la chaudière



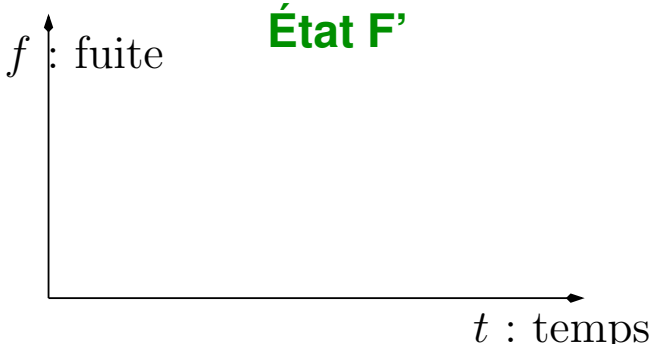
- $\tau_1^{\otimes}$ = “ajoute le rayon $(1, 1, 1)$ tant que $x \leqslant 10$”
- $\tau_2^{\otimes}$ = “ajoute le rayon $(1, 0, 1)$”



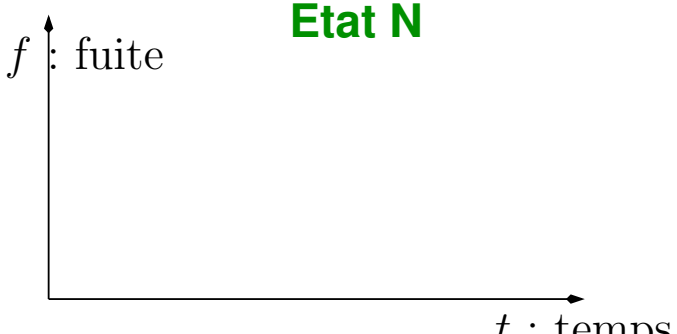
État F



État N’

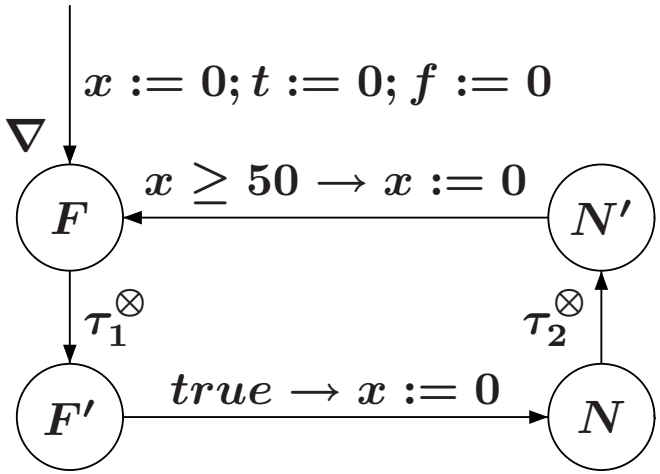


État F’



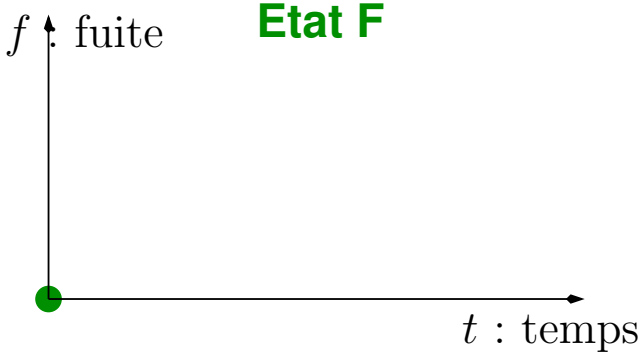
État N

Le retour de la chaudière

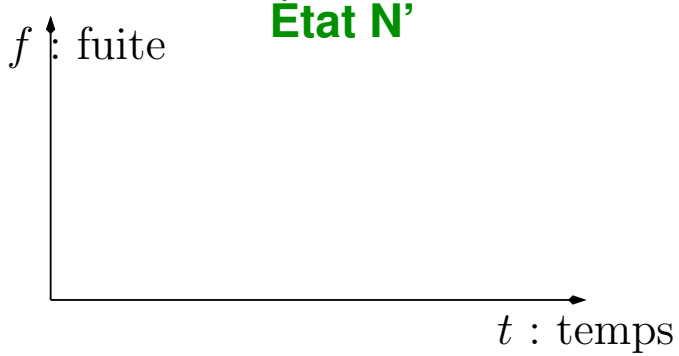


- $\tau_1^{\otimes}$ = “ajoute le rayon $(1, 1, 1)$ tant que $x \leqslant 10$”
- $\tau_2^{\otimes}$ = “ajoute le rayon $(1, 0, 1)$”

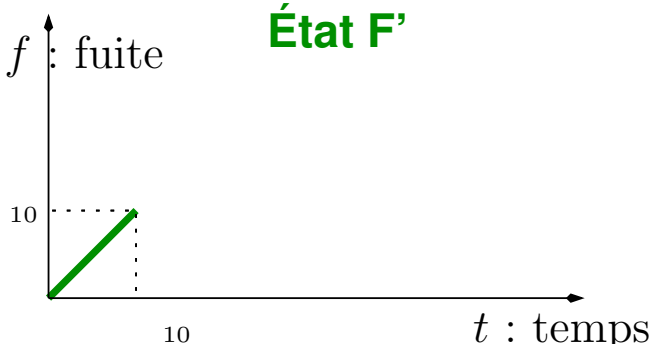
État F



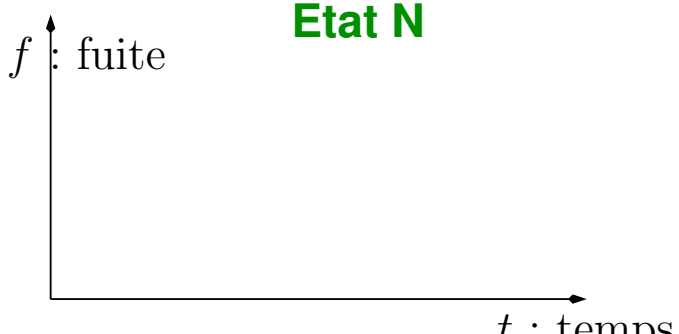
État N’



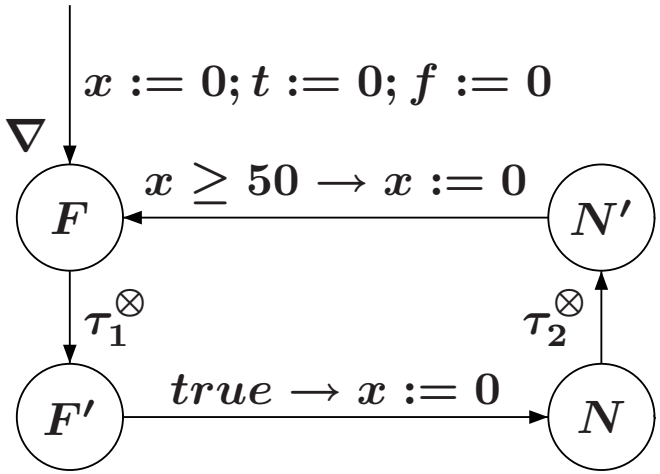
État F’



État N

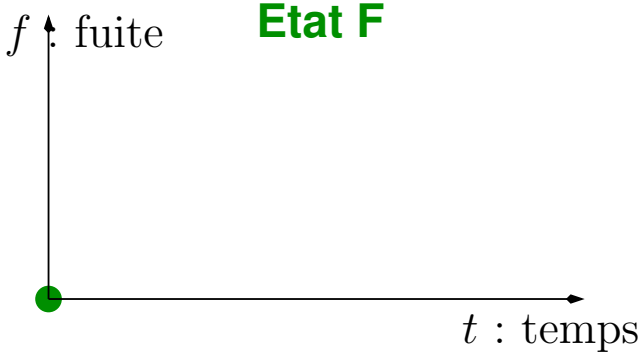


Le retour de la chaudière

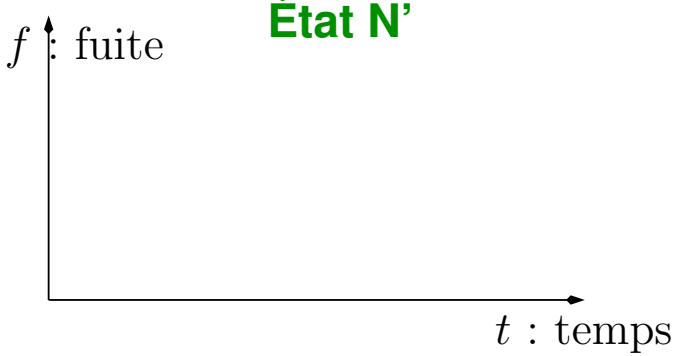


- $\tau_1^{\otimes}$ = “ajoute le rayon $(1, 1, 1)$ tant que $x \leqslant 10$”
- $\tau_2^{\otimes}$ = “ajoute le rayon $(1, 0, 1)$”

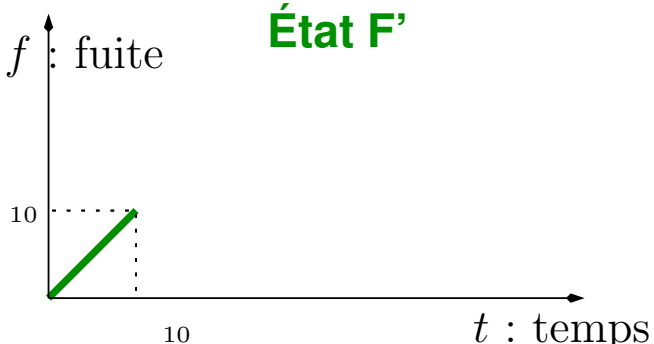
État F



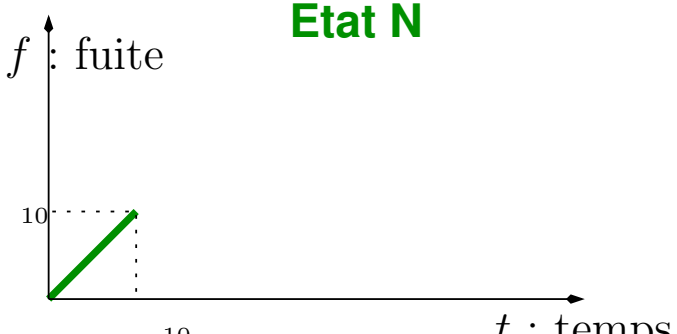
État N’



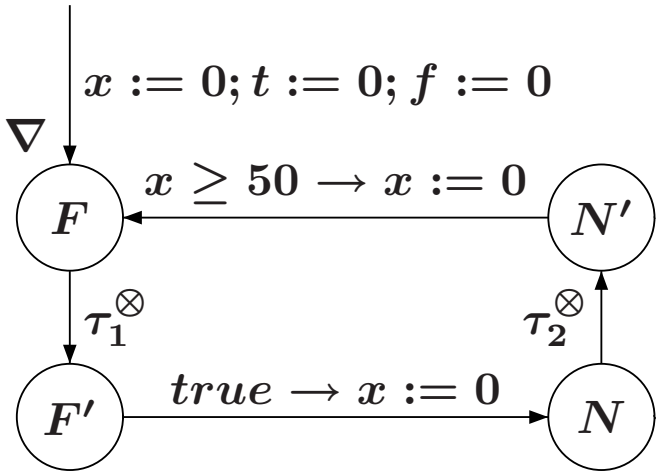
État F’



État N

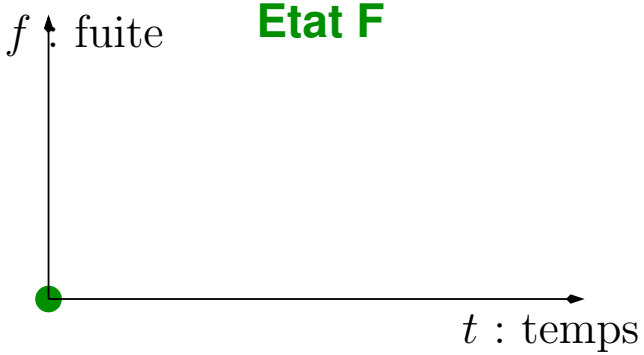


Le retour de la chaudière

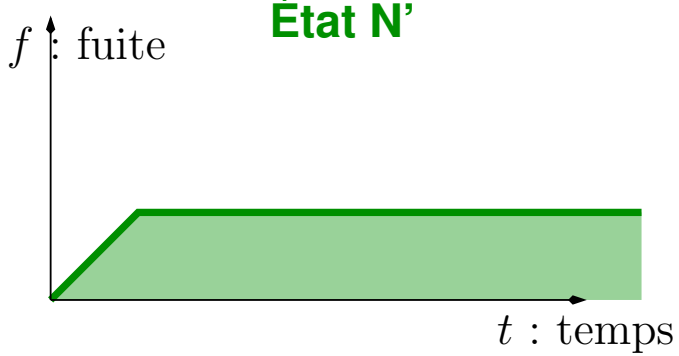


- $\tau_1^{\otimes}$ = “ajoute le rayon $(1, 1, 1)$ tant que $x \leqslant 10$”
- $\tau_2^{\otimes}$ = “ajoute le rayon $(1, 0, 1)$”

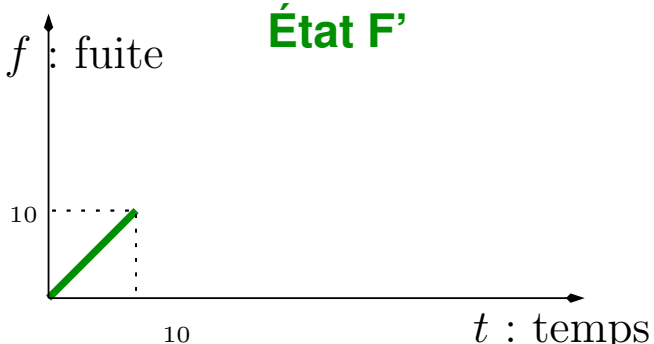
État F



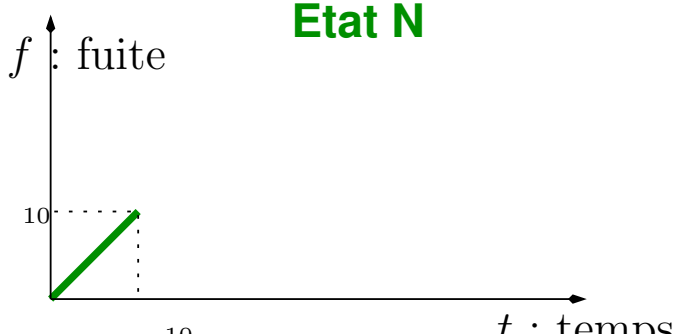
État N’



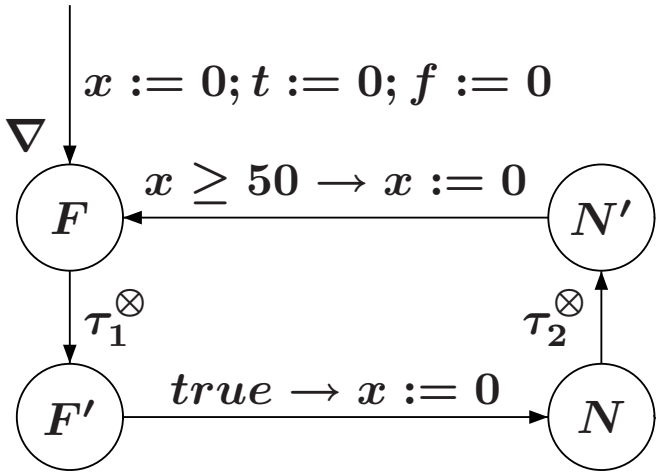
État F’



État N

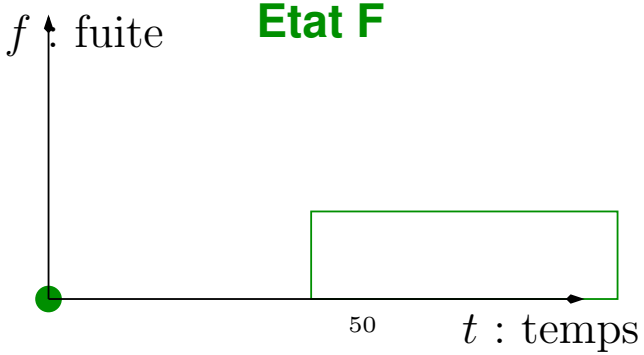


Le retour de la chaudière

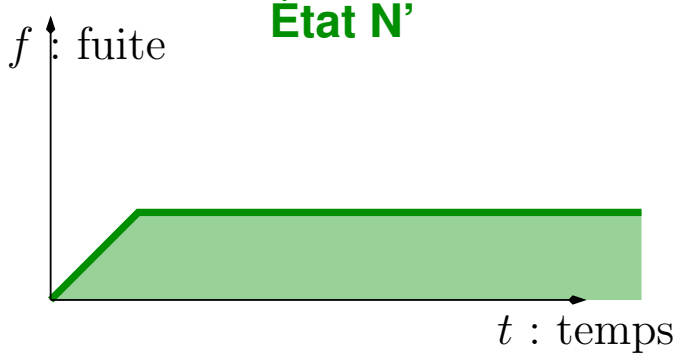


- $\tau_1^{\otimes}$ = “ajoute le rayon $(1, 1, 1)$ tant que $x \leqslant 10$”
- $\tau_2^{\otimes}$ = “ajoute le rayon $(1, 0, 1)$”

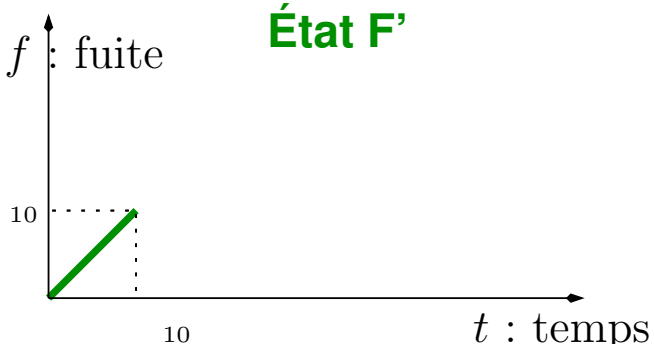
État F



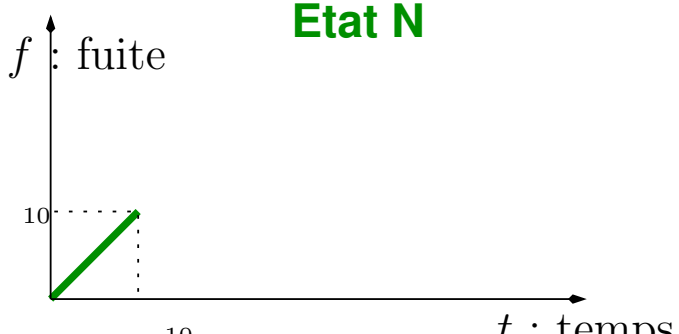
État N’



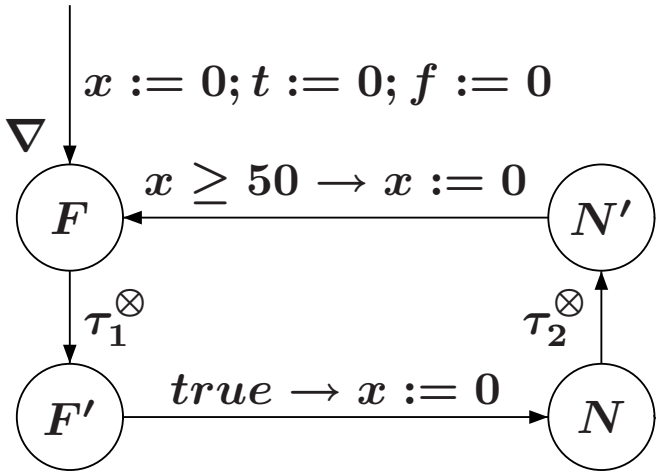
État F’



État N

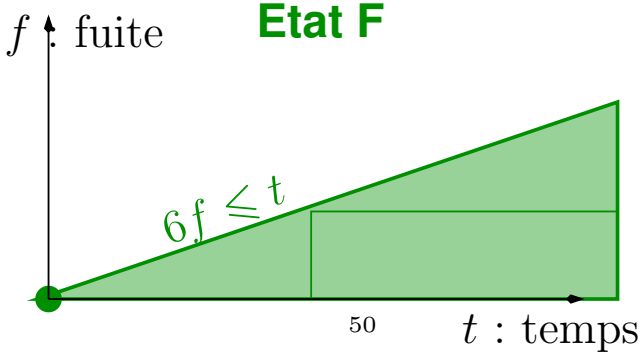


Le retour de la chaudière

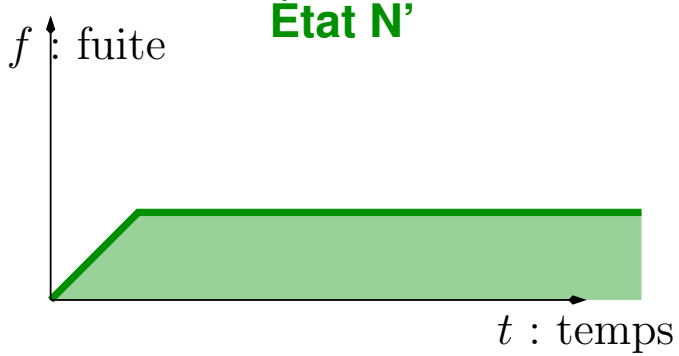


- $\tau_1^{\otimes}$ = “ajoute le rayon $(1, 1, 1)$ tant que $x \leqslant 10$”
- $\tau_2^{\otimes}$ = “ajoute le rayon $(1, 0, 1)$”

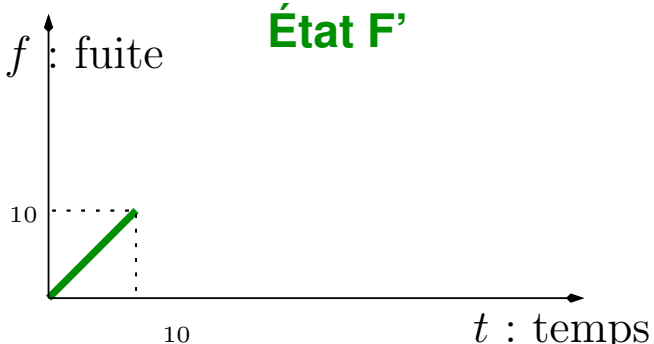
État F



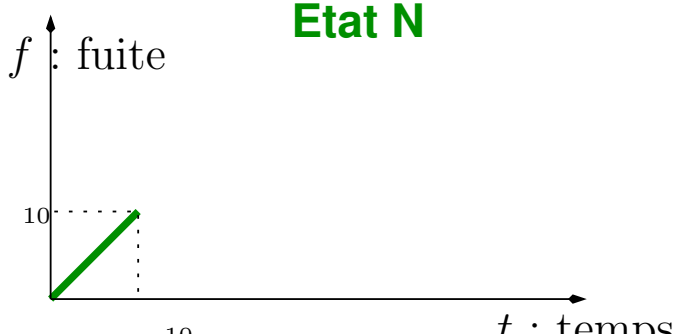
État N’



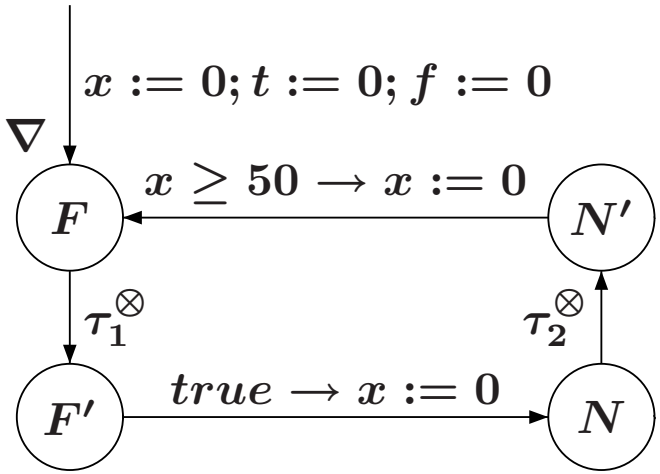
État F’



État N

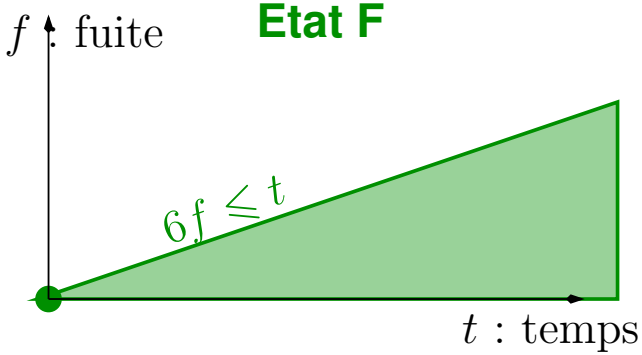


Le retour de la chaudière

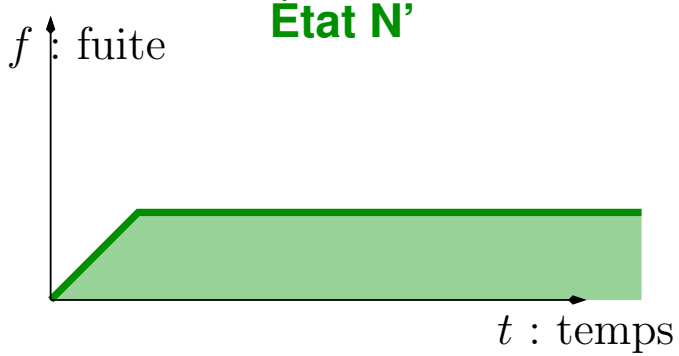


- $\tau_1^{\otimes}$ = “ajoute le rayon $(1, 1, 1)$ tant que $x \leqslant 10$”
- $\tau_2^{\otimes}$ = “ajoute le rayon $(1, 0, 1)$”

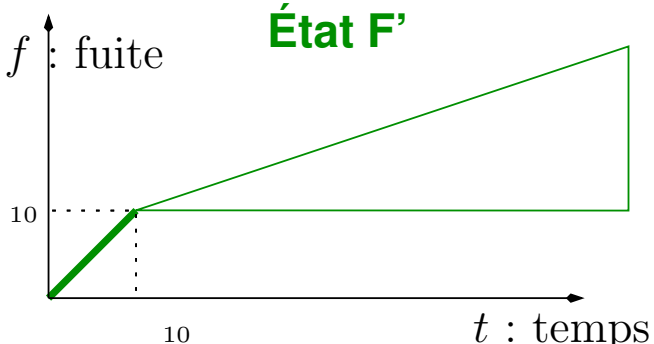
État F



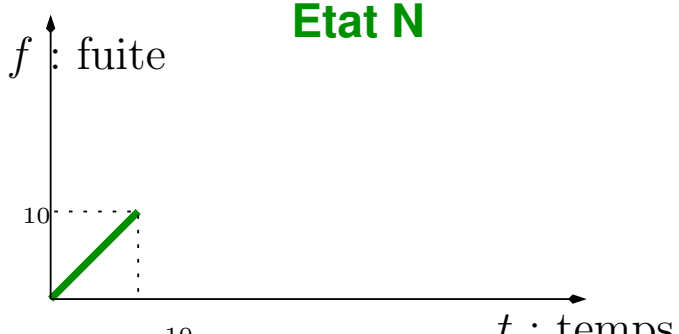
État N’



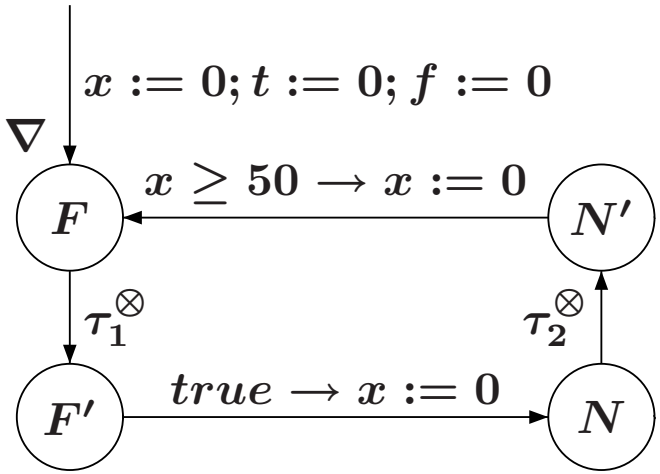
État F’



État N

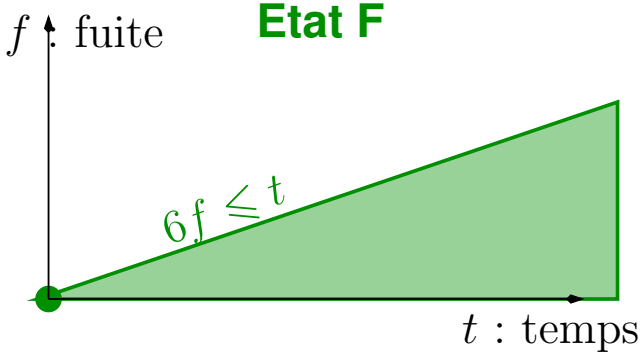


Le retour de la chaudière

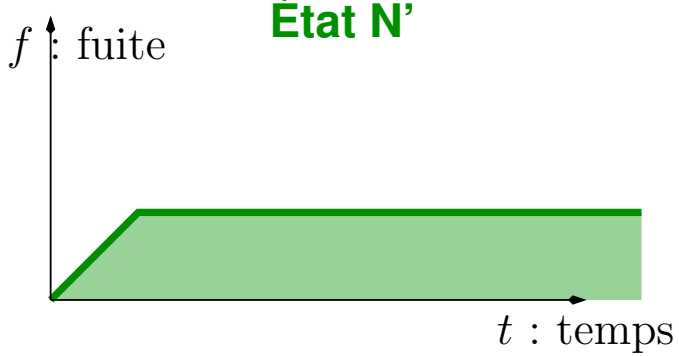


- $\tau_1^{\otimes}$ = “ajoute le rayon $(1, 1, 1)$ tant que $x \leqslant 10$”
- $\tau_2^{\otimes}$ = “ajoute le rayon $(1, 0, 1)$”

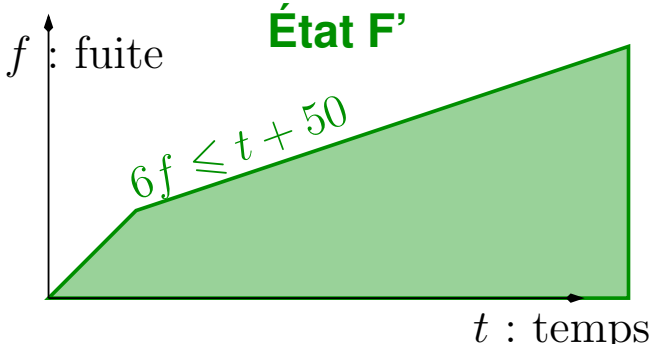
État F



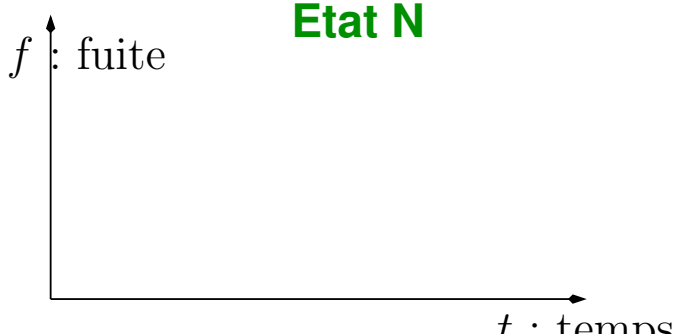
État N’



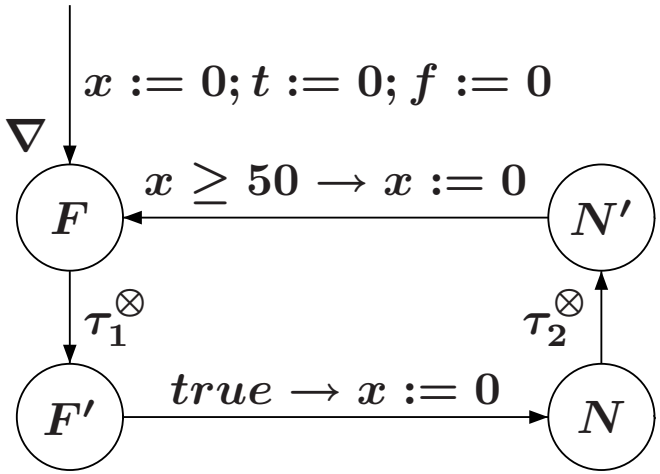
État F’



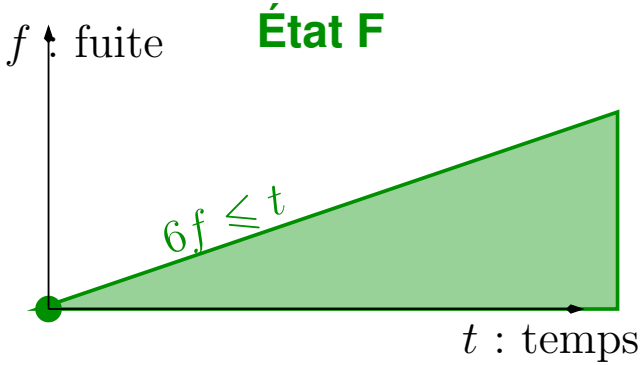
État N

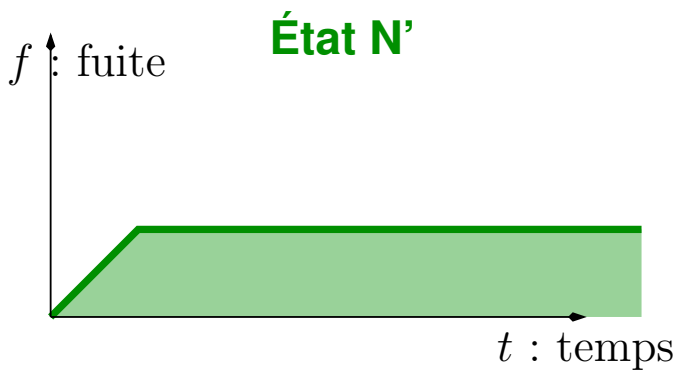


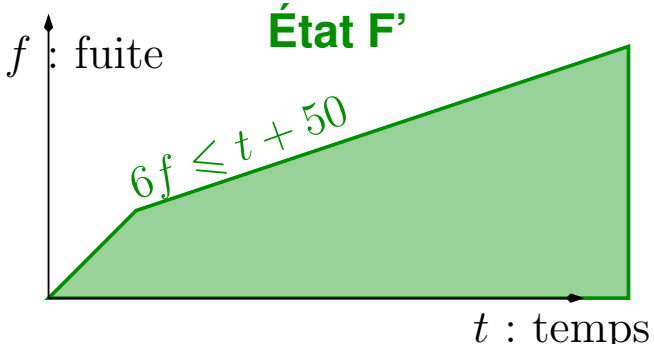
Le retour de la chaudière

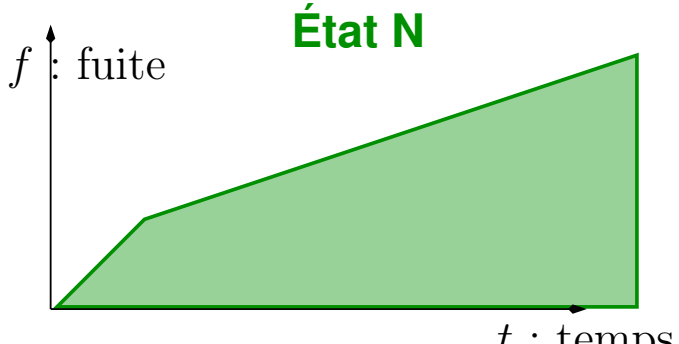


- $\tau_1^{\otimes}$ = “ajoute le rayon $(1, 1, 1)$ tant que $x \leqslant 10$”
- $\tau_2^{\otimes}$ = “ajoute le rayon $(1, 0, 1)$”

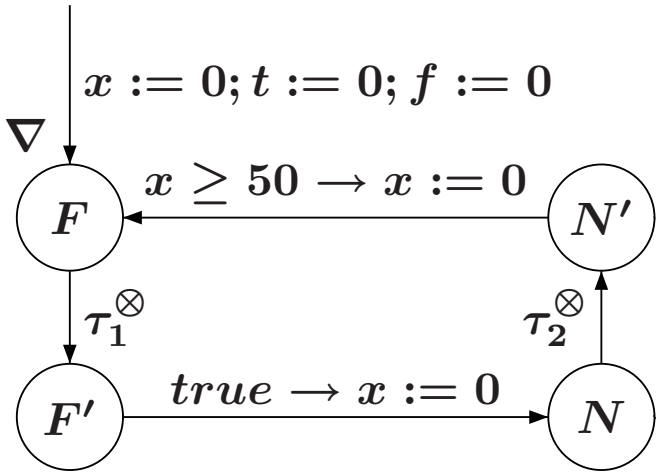




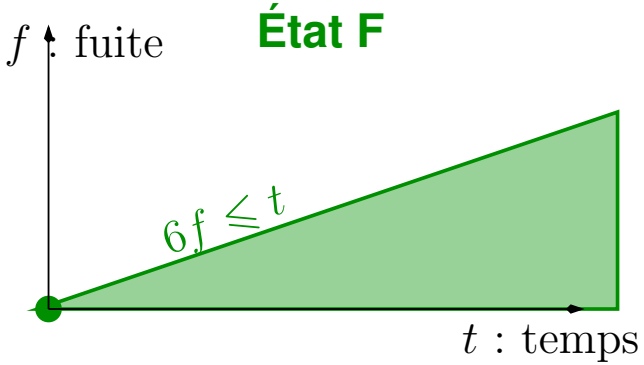


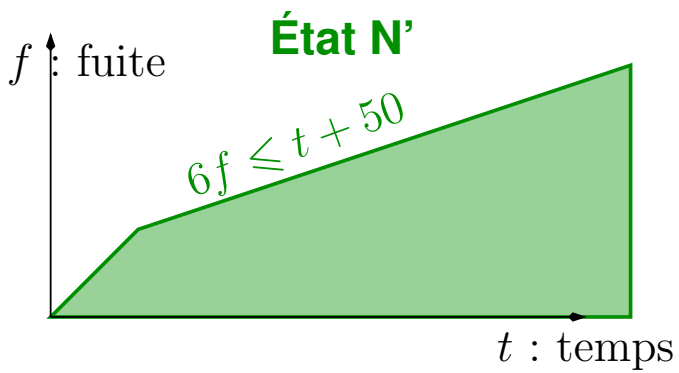


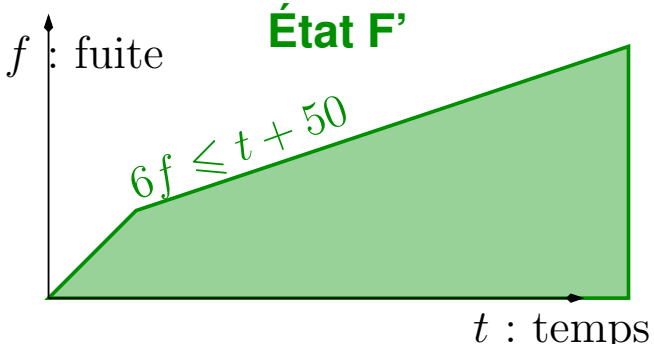
Le retour de la chaudière

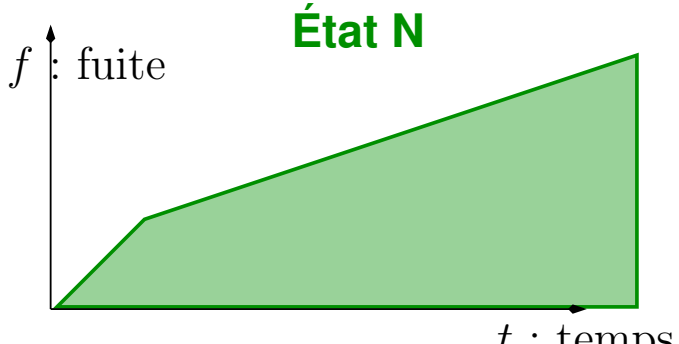


- $\tau_1^{\otimes}$ = “ajoute le rayon $(1, 1, 1)$ tant que $x \leqslant 10$”
- $\tau_2^{\otimes}$ = “ajoute le rayon $(1, 0, 1)$”









Caractéristiques d'Aspic

ASPIC : Accelerated Symbolic Polyhedral Invariant Computation

- Un langage textuel d'automates (Fast) avec ou sans but de preuve (formule)
- Calcul classique + accélérations.
- Sorties : invariants + diagnostic.

Caractéristiques d'Aspic

ASPIC : Accelerated Symbolic Polyhedral Invariant Computation

- Un langage textuel d'automates (Fast) avec ou sans but de preuve (formule)
- Calcul classique + accélérations.
- Sorties : invariants + diagnostic.

▶ `http://laure.gonnord.org/pro/aspic/aspic.html`

Résultats expérimentaux

Quelques applications

- Accessibilité dans des automates à compteurs (sémantique de SystemC), une centaine de points de contrôle, J. Cornet.
- Propriétés numériques d'automates modélisant une consommation d'énergie de (réseaux de) capteurs, L. Samper et F. Maraninchi.
- Vérification de programmes manipulant des listes, R. Iosif et S. Perarnau.

Résultats expérimentaux

Quelques applications

- Accessibilité dans des automates à compteurs (sémantique de SystemC), une centaine de points de contrôle, J. Cornet.
- Propriétés numériques d'automates modélisant une consommation d'énergie de (réseaux de) capteurs, L. Samper et F. Maraninchi.
- Vérification de programmes manipulant des listes, R. Iosif et S. Perarnau.

▶ Cf ma thèse et le futur papier de journal.

Hop !

Merci.