Analyse des systèmes hybrides sous la forme de systèmes de contraintes

Robert Valette, Nicolas Rivière
LAAS-CNRS

Plan

- **Introduction - Exemples**
- **Vérification - Analyse**
- **Scénarios – réseaux de Petri et logique linéaire**
- **Preuve et propagation de contraintes**
- **Conclusion**

Introduction (1)

Qu'est ce qu'un système hybride ?

- **Il s'agit d'un modèle mathématique d'un système**
- **Variables d'état discrètes + variables d'état continues**
- **Dynamique discrète (automate) + continue (equa. dif. + t. dense)**
- **Difficulté de travailler avec les deux approches mathématiques**

Introduction (2)

Association discret / continu nouvelle ?

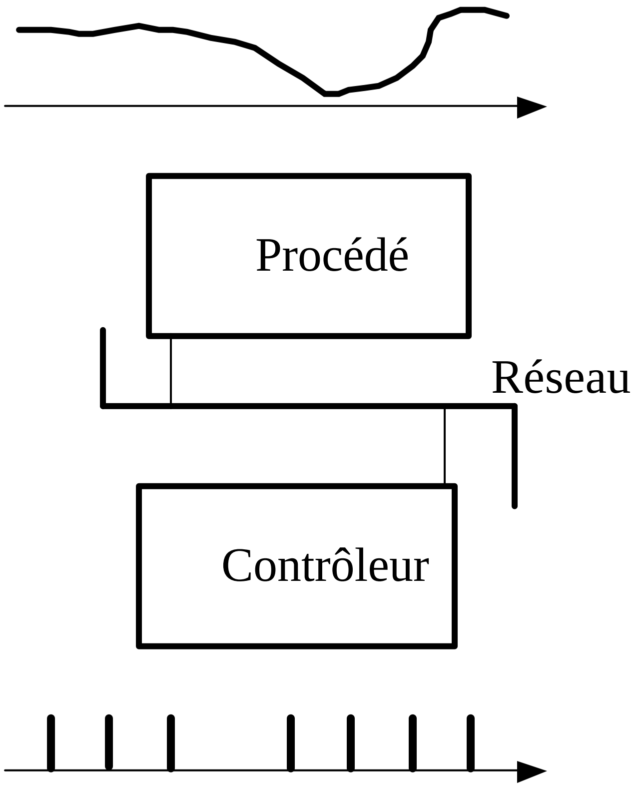
- **Recherche opérationnelle**
  - MILP programmation linéaire en réel (relaxation des contraintes d'intégrité) puis exploration arborescente (« branch and bound »)
  - Calculs de flots dans des graphes
  - Utilisation de graphes potentiels

- **Intelligence Artificielle**
  - Planification de tâches
  - CSP (Constraint Satisfaction Problems), TCSP (Temporal CSP)

Introduction (3)

Exemple 1

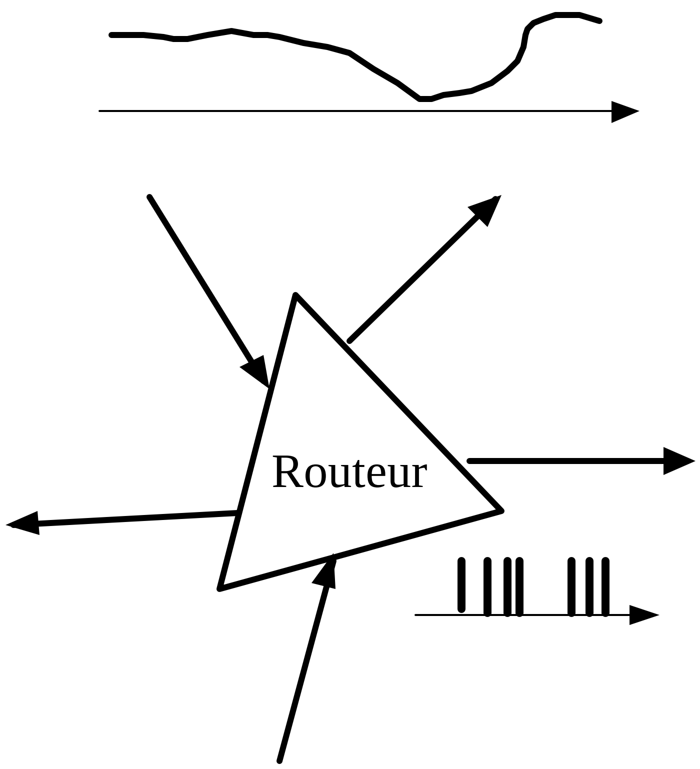
- **Un procédé physique**
- **Un réseau local**
- **On veut analyser si la qualité de service a une influence sur la stabilité**



Introduction (4)

Exemple 2

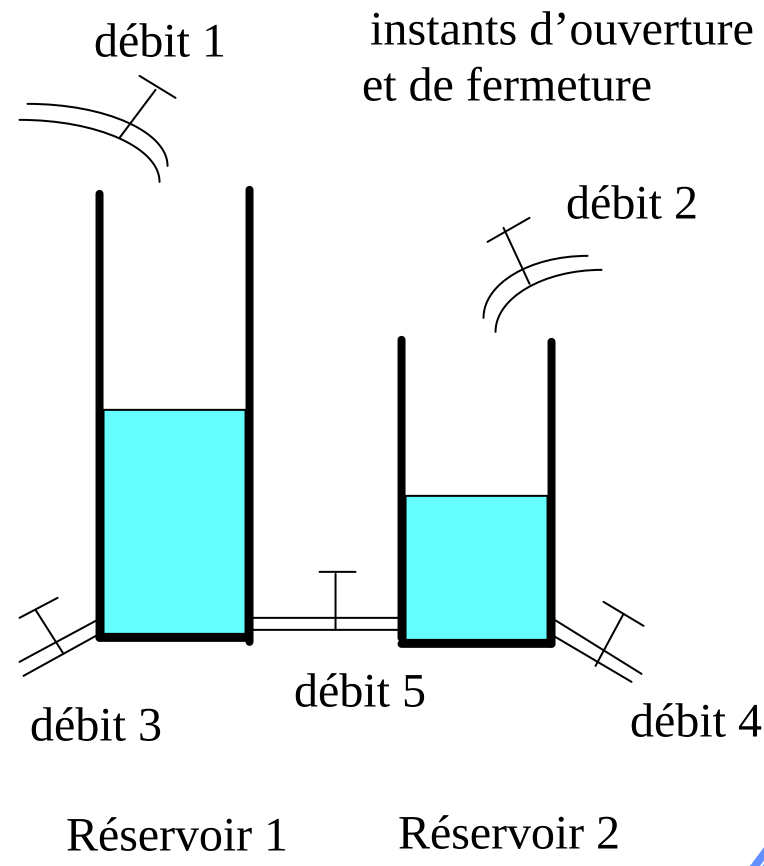
- **Fluidification (coder un entier par un réel) pour faciliter le passage à l'échelle**
- **Modéliser un grand réseau tout en conservant une représentation des protocoles**
- **Planification et ordonnancement d'un atelier**



Introduction (5)

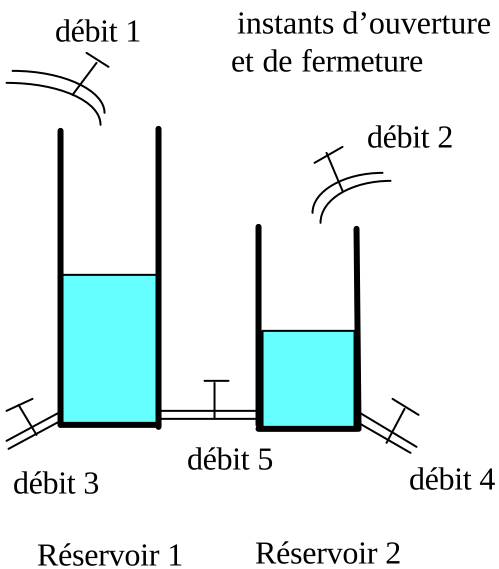
Exemple 3

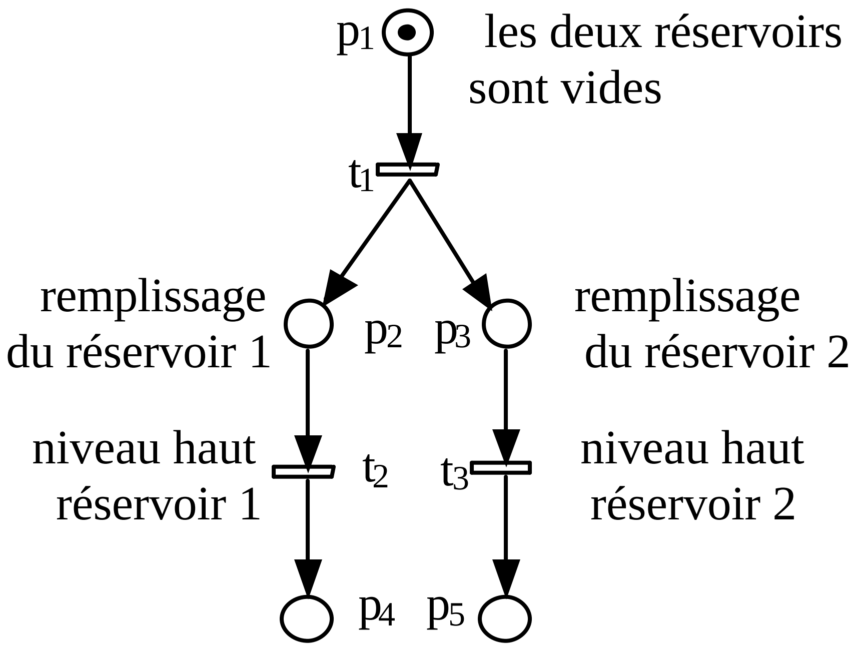
- **Commande discrète et continue d’un procédé**
- **Contraintes continues découlant de la physique**
- **Actionneurs ouvert ou fermé + valeur (codée par un réel)**



Vérification (1)

- **Montrer que le niveau haut du réservoir 2 est atteint avant le niveau haut du réservoir 1**

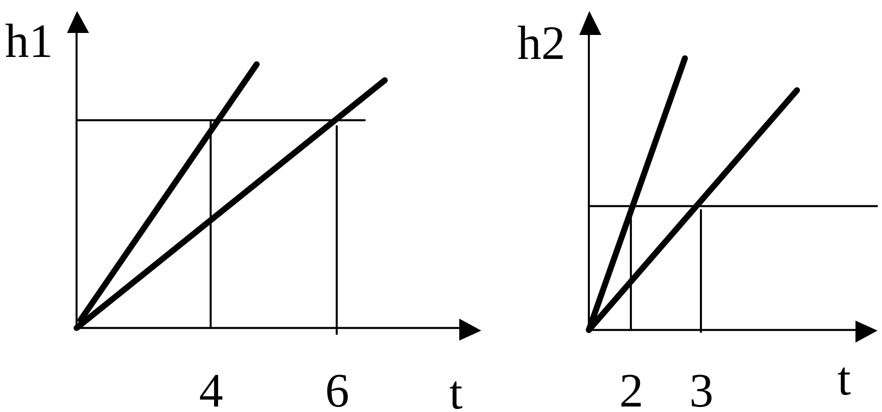


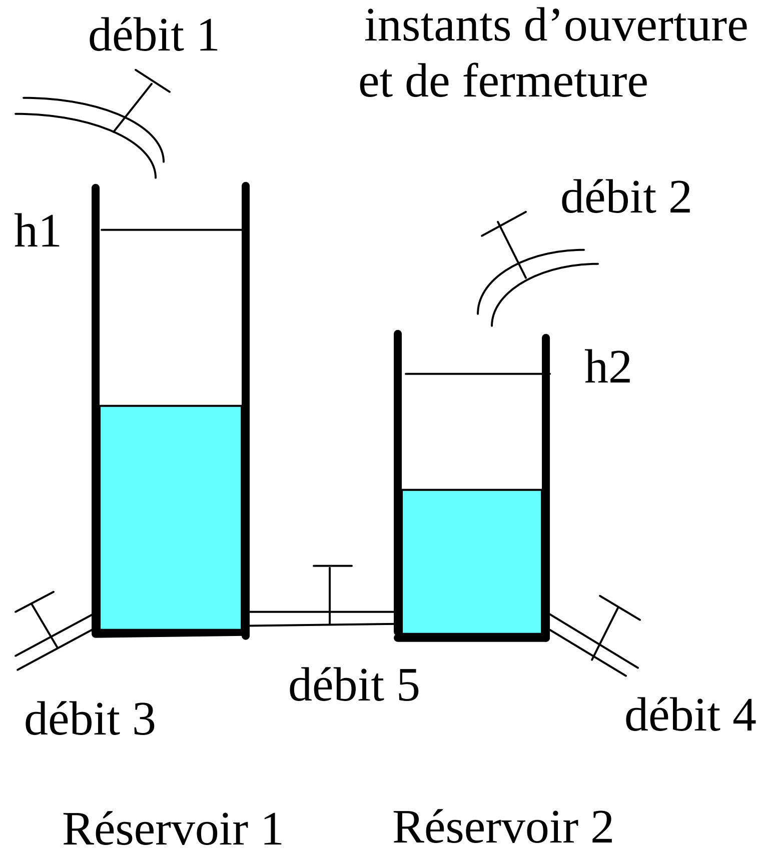


Marquage (p3 p4) inaccessible

Vérification (2)

- **Abstraction temporelle de la dynamique continue**
  - Combien de temps pour atteindre h1 et h2 suivant les débits 1, 2, 3, 4 et 5





Vérification (3)

- **Passer de la vérification à l'analyse : quelles contraintes les paramètres doivent-ils vérifier pour que la propriété soit vraie?**
- **Approche classique : approximer un comportement dynamique complexe par un ensemble de comportements linéaires.**
- **Les systèmes à événements discrets linéaires sont les « graphes d'événements » (alg. max +).**
- **Recouvrir la dynamique par un ensemble de graphes d'événements = notion de scénario**

Qu'est ce qu'un scénario ?

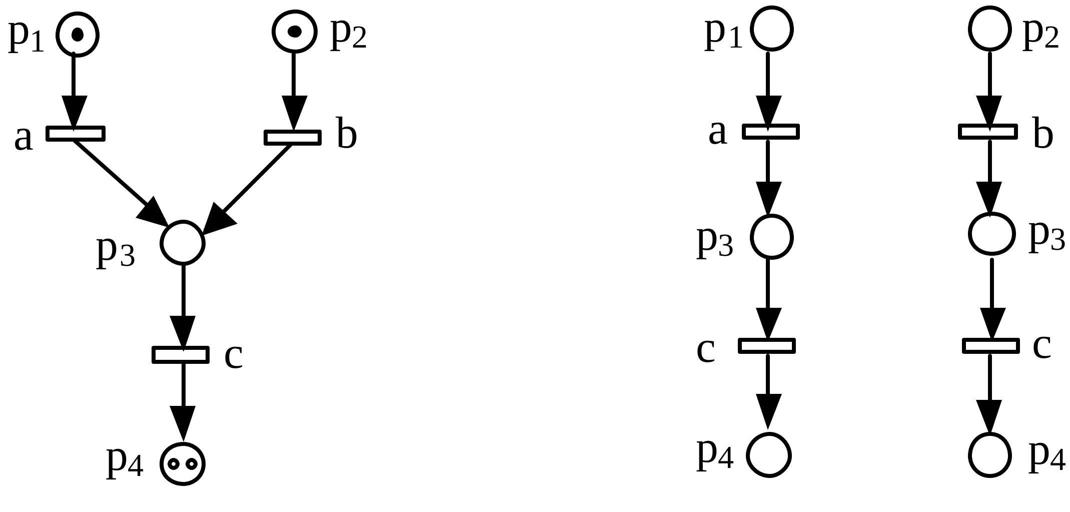
Un ensemble de définitions possibles :

- **Liste d'événements**
  - Étiquetage des événements (tous différents ou instances d'un événement)
- **Ordre d'apparition de ces événements**
  - Séquence (ordre total) ou ordre partiel
- **Caractère fini ou répétitif**
  - Nombre fini d'événements entre deux états ou définition d'un langage (par exemple régulier)

Processus fini (de réseau de Petri) (1)

- **Obtenu par « dépliage » (unfoldings) du réseau de Petri**
- **Structure identique aux graphes d'événements avec places sources (M_O : min) et place puits (M_f : max)**
- **Étiquetage : nom des places pour les jetons et nom des transitions pour les événements**
- **Sémantique opérationnelle des réseaux de Petri avec parallélisme vrai (sans entrelacement)**
- **Surtout utilisé avec $M_f = M_O$ pour recouvrir les marquages accessibles. Mais également scénario fini.**

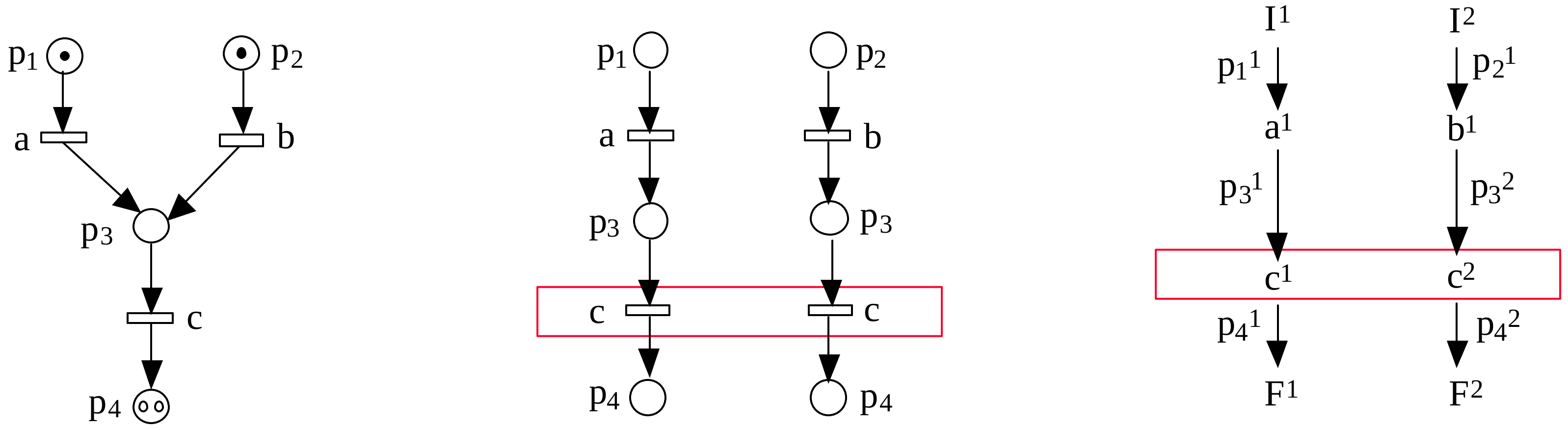
Processus fini (de réseau de Petri) (2)



Un réseau de Petri et son processus fini entre deux marquages

Graphes de précédence

- **On pourrait l'appeler processus fini doublement étiqueté ou ordre partiel doublement étiqueté (nous utilisons parfois le nom ordre partiel)**
- **On différentie les instances de jeton et les instances de franchissement de transition car il n'y a pas de volonté de fonc. répétitif (notre approche)**



Réseau de Petri, processus et ordre graphe de précédence

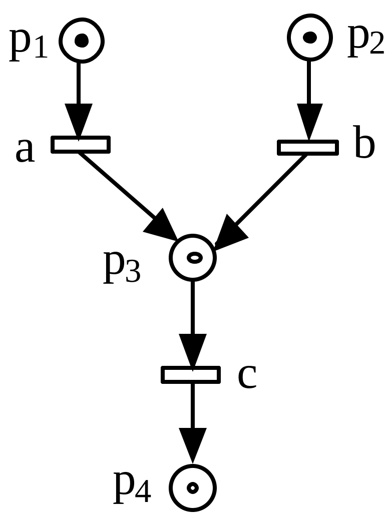
Séquent de logique Linéaire (1)

- **Un séquent (un théorème) :** $A, (A \rightarrow B) \vdash B$
- **Sa preuve (syntaxique) :** $$\dfrac{\dfrac{}{A \vdash A}\,id \qquad \dfrac{}{B \vdash B}\,id}{A, (A \rightarrow B) \vdash B} \rightarrow L$$
- **En logique linéaire, deux règles sont abandonnées**
  - La contraction qui correspond à l'idempotence du « et » et du « ou » $\cancel{A \wedge A \dashv\vdash A}$
  - L'affaiblissement $\cancel{A \wedge B \vdash A}$

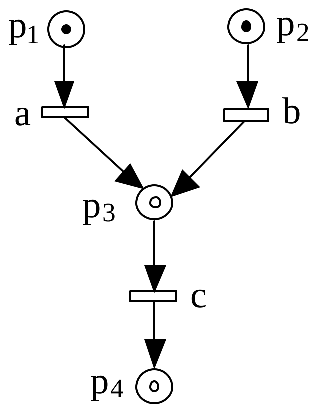
Séquent de logique Linéaire (2)

- **Un scénario : « État initial, actions |- État final »**
- $\boxed{\mathbf{p_1\text{Ä}p_2,\ a,\ b,\ c\ \text{|-}\ p_3\text{Ä}p_4}}$

  $a = p_1 \multimap p_3 \qquad b = p_2 \multimap p_3 \qquad c = p_3 \multimap p_4$
- **Les atomes logiques représentent les jetons**
- **Consommation des propositions utilisées**
- **Pas d'idempotence donc répétition possible**
- $\boxed{\mathbf{p_1\text{Ä}p_2,\ a,\ b,\ c,\ c\ \text{|-}\ p_4\text{Ä}p_4}}$
- **Commutativité mais preuve (causalité)**



Séquent de logique Linéaire (3)



p_3 |- p_3 $\qquad$ p_4 |- p_4

p_3 |- p_3 $\qquad$ p_3, p_4 |- p_3Ä p_4

p_2 |- p_2 $\qquad$ p_3, p_3, p_3-o p_4 |- p_3Ä p_4 $\qquad$ **c**

p_1 |- p_1 $\qquad$ p_3, p_2, p_2-o p_3, p_3-o p_4 |- p_3Ä p_4 $\qquad$ **b**

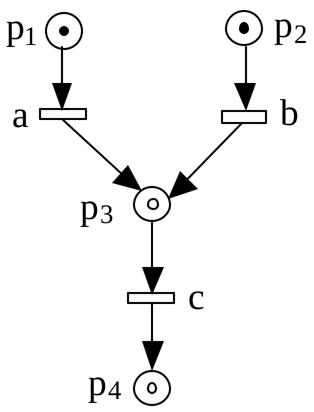
p_1, p_2, p_1-o p_3, p_2-o p_3, p_3-o p_4 |- p_3Ä p_4 $\qquad$ **a**

p_1Ä p_2, p_1-o p_3, p_2-o p_3, p_3-o p_4 |- p_3Ä p_4

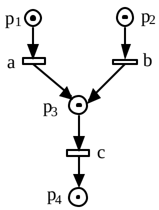
Preuve : a ; b ; c

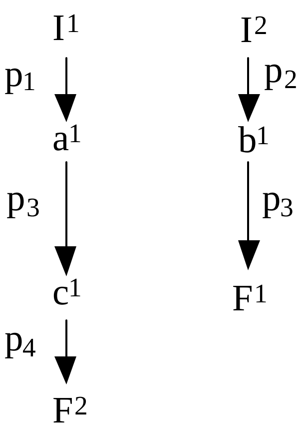
Séquent de logique Linéaire (4)

- **Il y a un arbre de preuve pour chaque séquence de franchissements possible**
- **4 séquences : (a; b; c) (b; a; c) (a; c; b) (b; c; a)**
- **Double étiquetage pour expliciter les causalités**
- **Règle d'élimination de l'implication transition+nombre**
- **Par atome (soit produit, soit consommé) place+événem.**
- **On obtient le graphe de précédence**



Séquent de logique Linéaire (5)





$$\overline{p_3(b^1) \vdash p_3(F^1)} \qquad \overline{p_4(c^1) \vdash p_4(F^2)}$$

$$\overline{p_3(a^1) \vdash p_3(c^1)} \qquad \dfrac{}{p_3(b^1),\ p_4(c^1) \vdash p_3(F^1) \otimes p_4(F^2)}$$

$$\overline{p_2(I^2) \vdash p_2(b^1)} \qquad \dfrac{}{p_3(a^1),\ p_3(b^1),\ p_3 \multimap p_4 \vdash p_3(F^1) \otimes p_4(F^2)}\ c^1$$

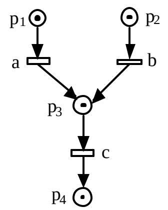
$$\overline{p_1(I^1) \vdash p_1(a^1)} \qquad \dfrac{}{p_3(a^1),\ p_2,\ p_2 \multimap p_3,\ p_3 \multimap p_4 \vdash p_3(F^1) \otimes p_4(F^2)}\ b^1$$

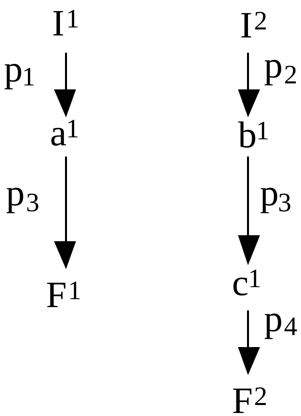
$$\dfrac{}{p_1(I^1),\ p_2(I^2),\ p_1 \multimap p_3,\ p_2 \multimap p_3,\ p_3 \multimap p_4 \vdash p_3(F^1) \otimes p_4(F^2)}\ a^1$$

$$\dfrac{}{p_1(I^1) \otimes p_2(I^2),\ p_1 \multimap p_3,\ p_2 \multimap p_3,\ p_3 \multimap p_4 \vdash p_3(F^1) \otimes p_4(F^2)}$$

Preuve étiq. 1 : a ; b ; c

Séquent de logique Linéaire (6)





$$\overline{p_3(a^1) \vdash p_3(F^1)} \qquad \overline{p_4(c^1) \vdash p_4(F^2)}$$

$$\overline{p_3(b^1) \vdash p_3(c^1)} \qquad \overline{p_3(a^1),\ p_4(c^1) \vdash p_3(F^1) \otimes p_4(F^2)}\ c^1$$

$$\overline{p_2(I^2) \vdash p_2(b^1)} \qquad \overline{p_3(a^1),\ p_3(b^1),\ p_3 \multimap p_4 \vdash p_3(F^1) \otimes p_4(F^2)}\ b^1$$

$$\overline{p_1(I^1) \vdash p_1(a^1)} \qquad \overline{p_3(a^1),\ p_2,\ p_2 \multimap p_3,\ p_3 \multimap p_4 \vdash p_3(F^1) \otimes p_4(F^2)}\ a^1$$

$$\overline{p_1(I^1),\ p_2(I^2),\ p_1 \multimap p_3,\ p_2 \multimap p_3,\ p_3 \multimap p_4 \vdash p_3(F^1) \otimes p_4(F^2)}$$

$$p_1(I^1) \otimes p_2(I^2),\ p_1 \multimap p_3,\ p_2 \multimap p_3,\ p_3 \multimap p_4 \vdash p_3(F^1) \otimes p_4(F^2)$$

Preuve étiq. 2 : a ; b ; c

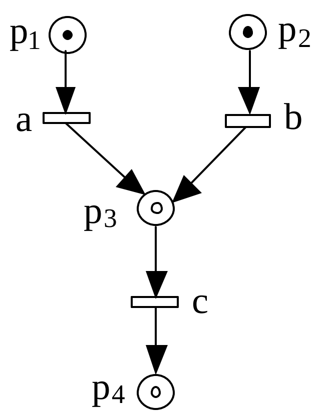
Séquent caractéristique (1)

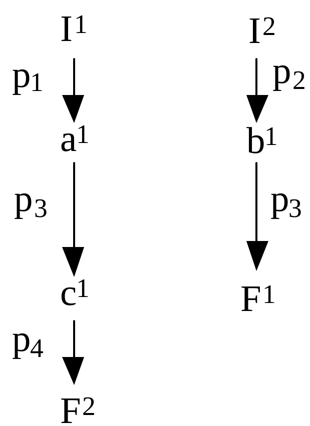
- **1 séquent peut donner *n* arbres de preuves**
- **1 arbre peut donner *m* graphes de précédence par étiquetage**
- **Faire passer l'étiquetage dans l'écriture du séquent**
- **Bijection entre séquent étiqueté et graphe de précédence**
- **On associe aux atomes les événements qui les ont produits**
- **Séquent étiqueté = graphe de précédence = scénario**

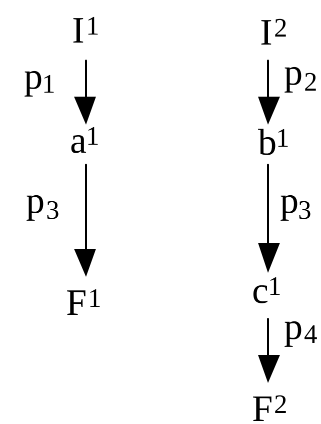
Séquent caractéristique (2)

$$P_1\_I^1 \text{ Ä } p_2\_I^2, \overbrace{p_1\_I^1 \text{ -o } p_3\_a^1}^{a}, \overbrace{p_2\_I^2\text{-o } p_3\_b^1}^{b}, \overbrace{p_3\_a^1\text{-o } p_4\_c^1}^{c} \text{ |- } p_3\_b^1 \text{ Ä } p_4\_c^1$$

$$P_1\_I^1 \text{ Ä } p_2\_I^2, p_1\_I^1 \text{ -o } p_3\_a^1, p_2\_I^2\text{-o } p_3\_b^1, p_3\_b^1\text{-o } p_4\_c^1 \text{ |- } p_3\_a^1 \text{ Ä } p_4\_c^1$$

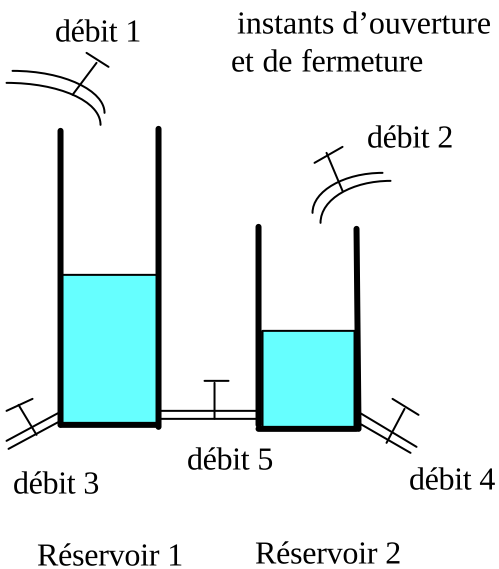


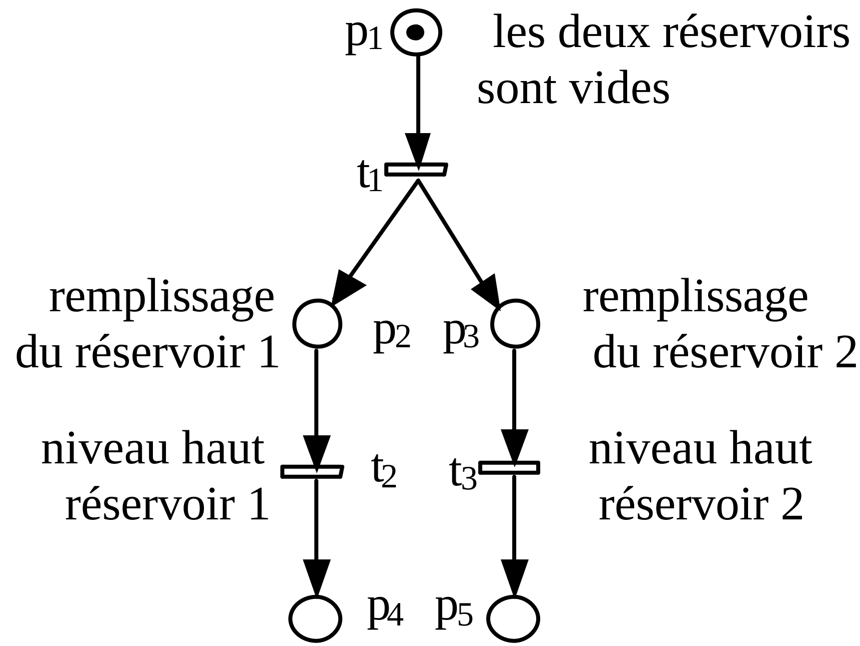




Preuve (1)

- **Montrer que le niveau haut du réservoir 2 est atteint avant le niveau haut du réservoir 1**

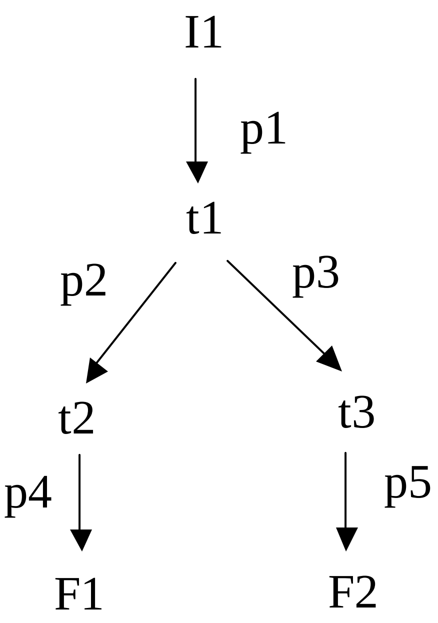


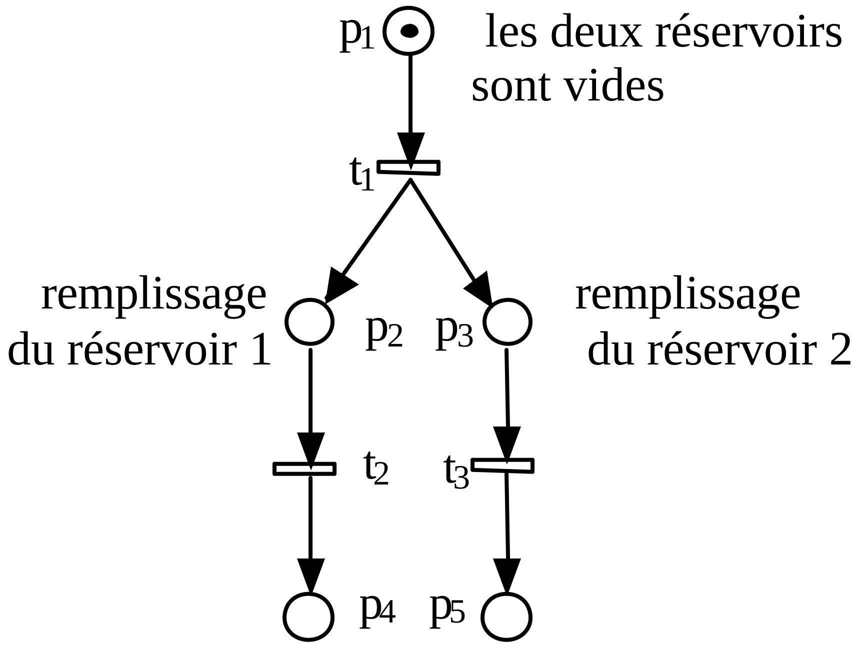


Marquage (p3 p4) inaccessible

Preuve (2)

- **Extraire les relation de causalité exprimées par le séquent de logique Linéaire**

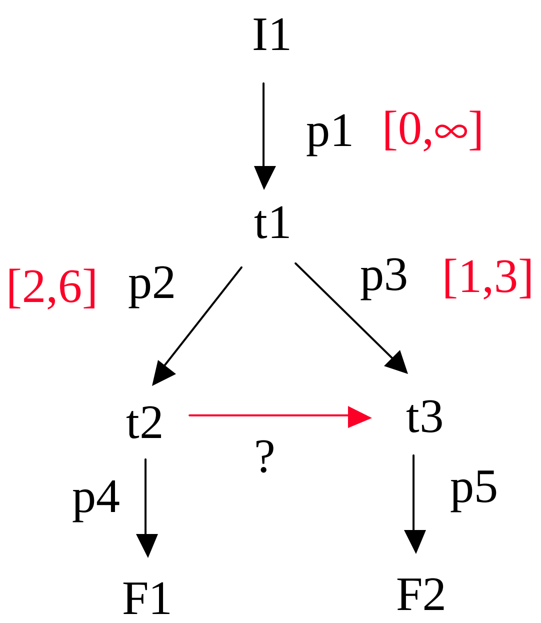


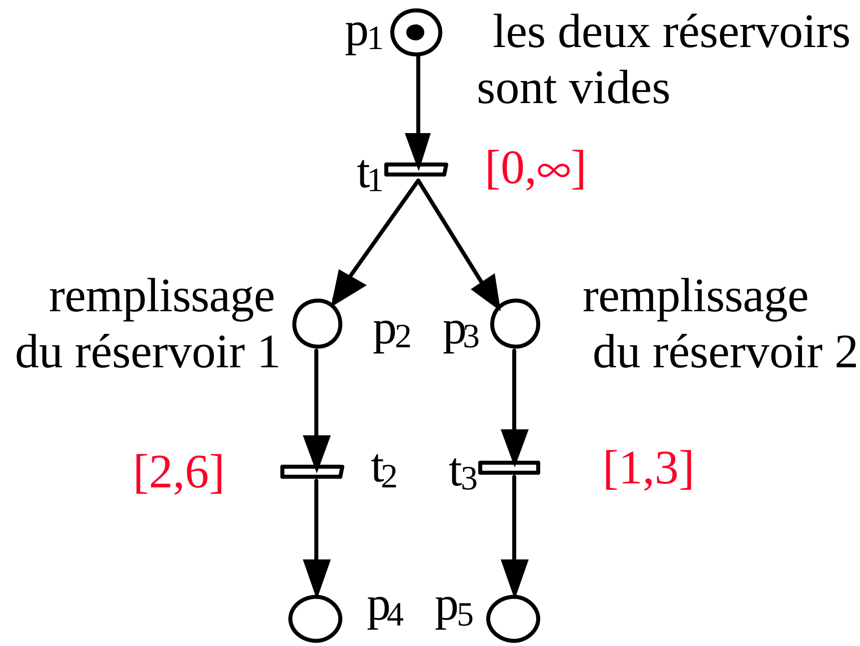


$$p_1(I_1), \underbrace{p_1 \multimap p_2 \otimes p_3}_{t1}, \underbrace{p_2 \multimap p_4}_{t2}, \underbrace{p_3 \multimap p_5}_{t3} \vdash p_4(F_1) \otimes p_5(F_2)$$

Preuve (3)

- **Passer au graphe de contraintes temporelles**

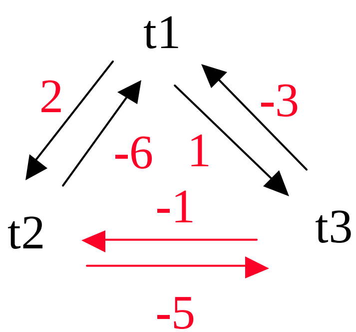




Marquage (p3 p4) inaccessible : t2 précède t3 impossible

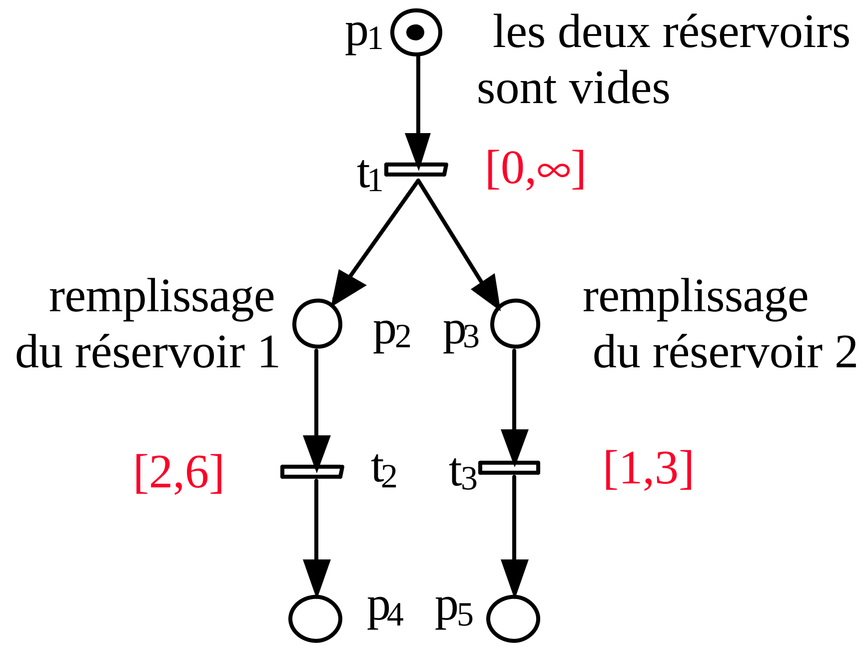
Preuve (4)

- **Propagation de contrainte (arc consistence)**



$-5 \leq t3 - t2 \leq 1$

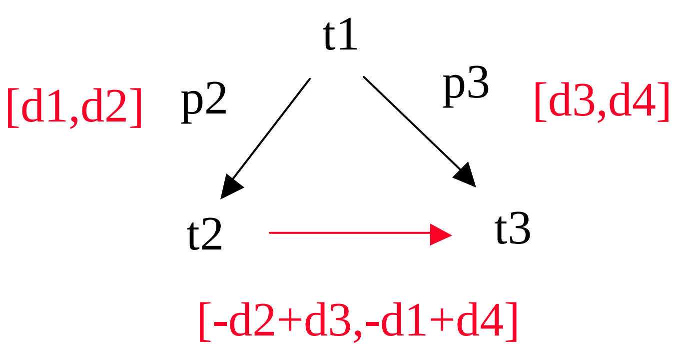
Echec car incertitude trop grande

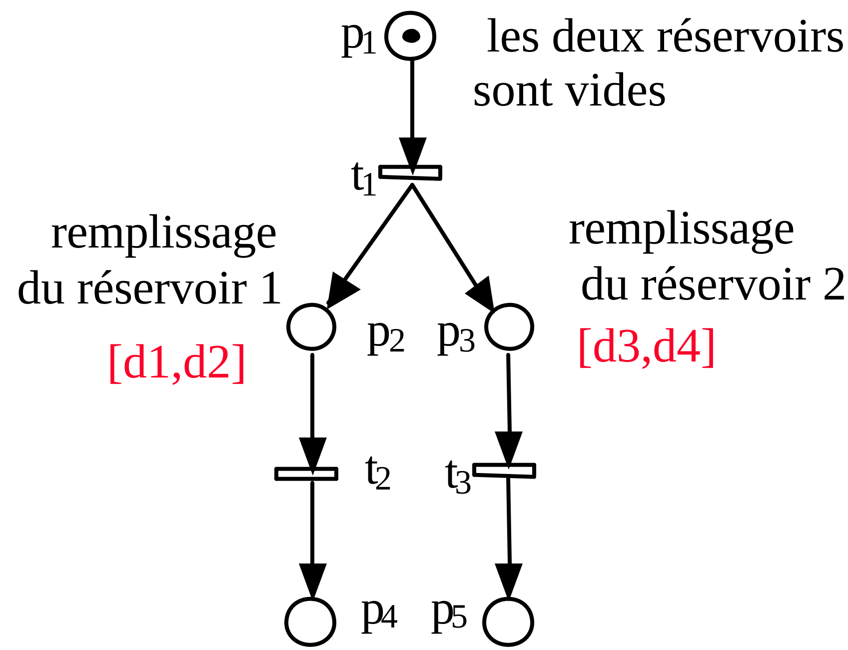


Marquage (p3 p4) inaccessible

Preuve (5)

- **Revenir sur les activités sous-jacentes aux causalités**
- **Travailler en symbolique**



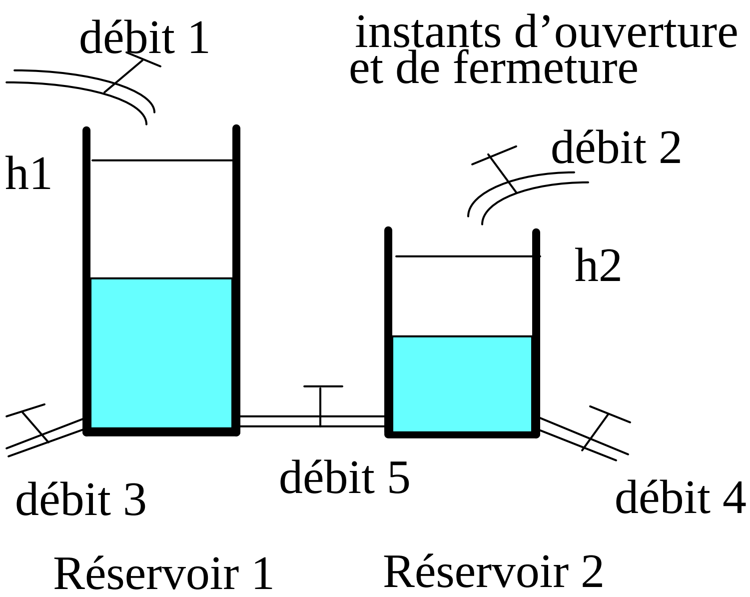


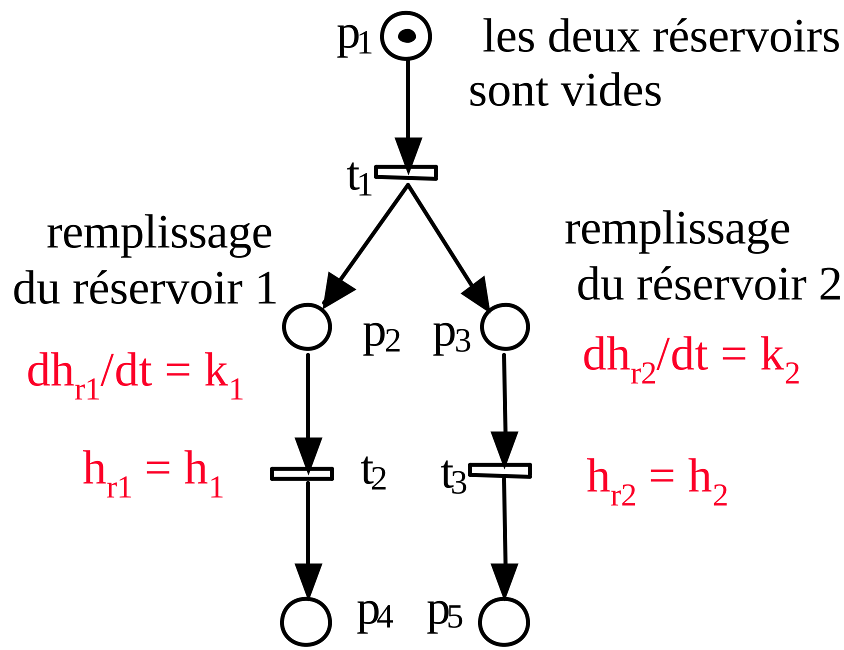
-d1 + d4 < 0 est la condition limite permettant la preuve par abstraction temporelle

Marquage (p3 p4) inaccessible

Preuve (6)

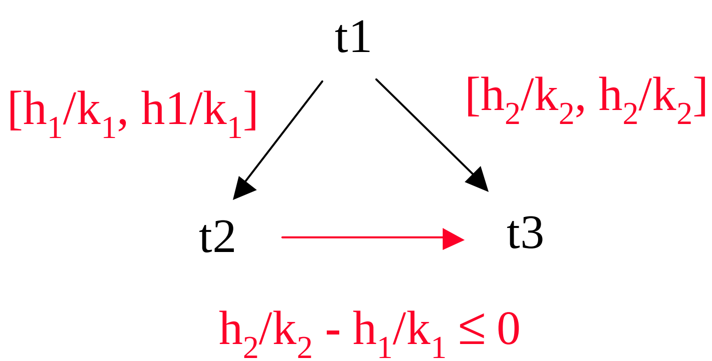
- **Dynamique des activités (débit5=0)**
- **Equa. diff. associées aux places**

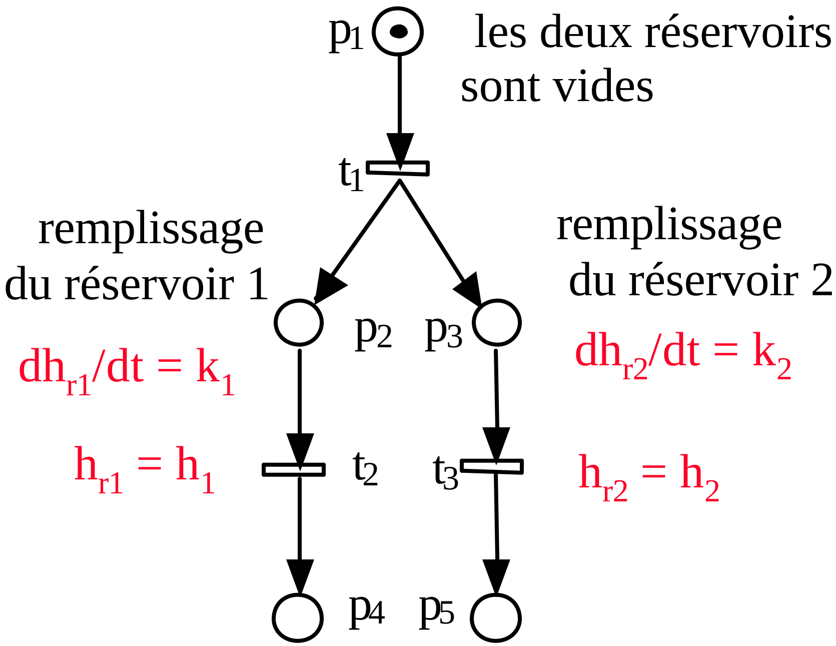




Preuve (7)

- **Dynamique des activités sous-jacentes aux causalités**
- **Travailler en symbolique**





Si par exemple $k_1 = k_2$ mais très variable on sera bien meilleur que l'approximation temporelle

Marquage (p3 p4) inaccessible

Conclusion (1)

- Pour aborder les systèmes hybrides, une dose d’approche de type « preuve » est souvent nécessaire
- L’analyse sous contraintes permet une prise en compte « progressive » des contraintes (« relaxation » de certaines contraintes) - modularité
- La logique linéaire permet d’extraire les contraintes de précédence « logiques » (causalité) entre les événements et elle s’insère bien dans une telle démarche

Conclusion (2)

La maîtrise des systèmes temporisés est un pas essentiel

- **Le temps « universel » est ce qui relie la dynamique continue (équa. diff.) et la dynamique discrète (ordre partiel entre évé.)**
- **On fait souvent des abstractions temporelles pour l'hybride**
- **Un ensemble d'horloges prenant leurs valeurs dans le temps universel # un temps unique**
  - égalité de variables ou égalité de valeurs