

Réunion d'avancement ANR HyClock

**Inférence de contraintes sur un formalisme hybride via la
logique de Hoare**

Maxime FOLSCHETTE

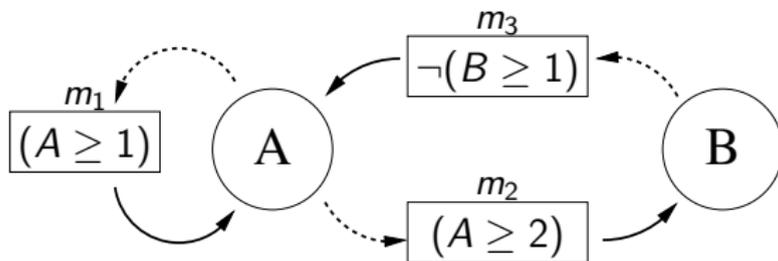
équipe : MeForBio / laboratoire : LS2N (ex-IRCCyN) / Université de Nantes

maxime.folschette@ircyn.ec-nantes.fr

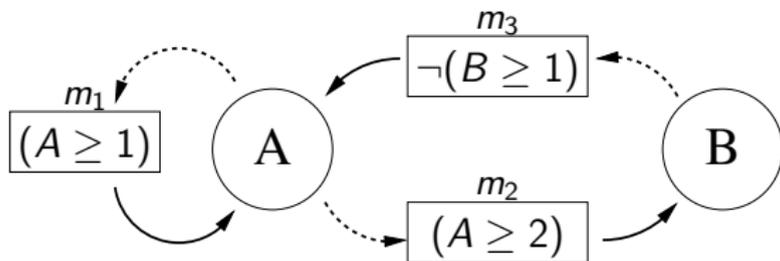
<http://maxime.folschette.name/>

2017/03/21

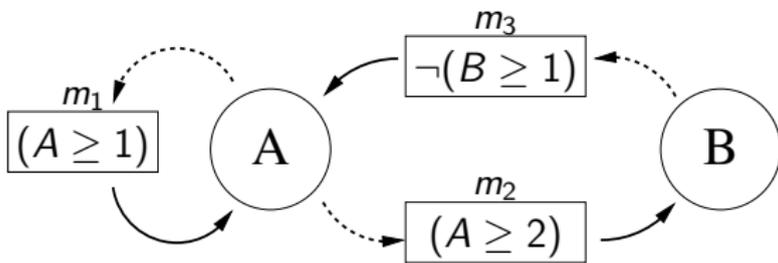
Formalisme de Thomas hybride

[Thomas, *Journal of Theoretical Biology*, 1973][Cornillon et al., *Mod. Complex Bio. Sys. in the Context of Gen.*, 2016] C_A C_B

Formalisme de Thomas hybride

[Thomas, *Journal of Theoretical Biology*, 1973][Cornillon et al., *Mod. Complex Bio. Sys. in the Context of Gen.*, 2016] $C_{A, \emptyset}$ $C_{A, \{m_1\}}$ $C_{A, \{m_3\}}$ $C_{A, \{m_1, m_3\}}$ $C_{B, \emptyset}$ $C_{B, \{m_2\}}$

Formalisme de Thomas hybride

[Thomas, *Journal of Theoretical Biology*, 1973][Cornillon et al., *Mod. Complex Bio. Sys. in the Context of Gen.*, 2016]

$$C_{A, \emptyset, 0}$$

$$C_{A, \{m_1\}, 1}$$

$$C_{A, \{m_1\}, 2}$$

$$C_{A, \{m_3\}, 0}$$

$$C_{A, \{m_1, m_3\}, 1}$$

$$C_{A, \{m_1, m_3\}, 2}$$

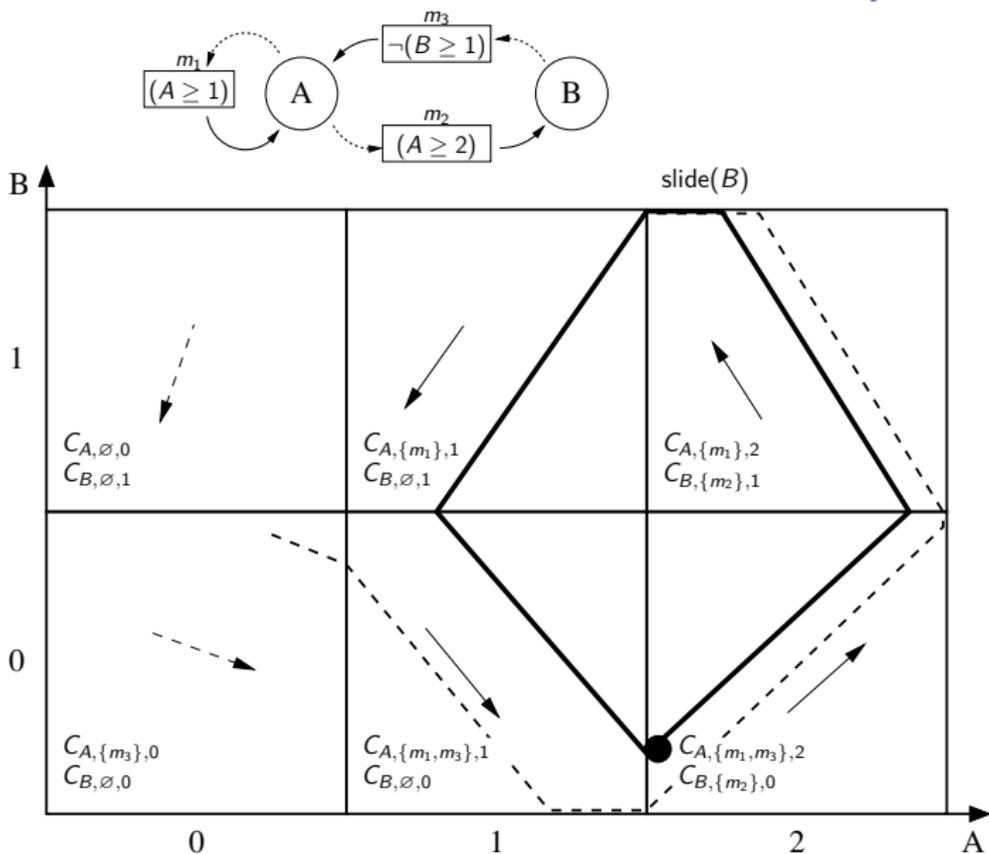
$$C_{B, \emptyset, 0}$$

$$C_{B, \emptyset, 1}$$

$$C_{B, \{m_2\}, 0}$$

$$C_{B, \{m_2\}, 1}$$

Formalisme de Thomas hybride



Logique de Hoare et utilisation dans le cas discret

[Hoare, *Communications of the ACM*, 1969]

[Dijkstra, *Communications of the ACM*, 1975]

[Bernot *et al.*, 2015]

Triplet de Hoare : $\{ Pre \} p \{ Post \}$

- p est un programme impératif
- Pre et $Post$ (pré- et postcondition) sont des propriétés

Signification :

« Si Pre est vraie, alors p peut s'exécuter,
et $Post$ devient vraie après exécution »

Plus faible précondition : Pour p et $Post$ donnés, calculer Pre la plus générale possible vérifiant le triplet

Application au modèle de Thomas (discret) : p représente l'évolution d'un système biologique (discret)

Exemple : $\{ Pre \} a+ ; b+ \{ a = 1 \wedge b = 1 \}$

$$Pre \equiv a = 0 \wedge b = 0 \wedge K_{a,\{a=0,b=0\}} = 1 \wedge K_{b,\{a=1,b=0\}} = 1$$

Logique de Hoare et utilisation dans le cas discret

[Hoare, *Communications of the ACM*, 1969]

[Dijkstra, *Communications of the ACM*, 1975]

[Bernot *et al.*, 2015]

Triplet de Hoare : $\{ Pre \} p \{ Post \}$

- p est un programme impératif
- Pre et $Post$ (pré- et postcondition) sont des propriétés

Signification :

« Si Pre est vraie, alors p peut s'exécuter,
et $Post$ devient vraie après exécution »

Plus faible précondition : Pour p et $Post$ donnés, calculer Pre la plus générale possible vérifiant le triplet

Application au modèle de Thomas (discret) : p représente l'évolution d'un système biologique (discret)

Exemple : $\{ Pre \} a+ ; b+ \{ a = 1 \wedge b = 1 \}$

$$Pre \equiv a = 0 \wedge b = 0 \wedge K_{a,\{a=0,b=0\}} = 1 \wedge K_{b,\{a=1,b=0\}} = 1$$

Version hybride de la logique de Hoare

[Behaegel *et al.*, 2016]

Triplet de Hoare :

$$\left\{ \begin{array}{l} D' \\ H' \end{array} \right\} \left(\begin{array}{c} \Delta t \\ \text{assert} \\ v_{\pm} \end{array} \right) \left\{ \begin{array}{l} D \\ H \end{array} \right\}$$

Version hybride de la logique de Hoare

[Behaegel *et al.*, 2016]

$$\text{Triplet de Hoare : } \left\{ \begin{array}{l} D' \\ H' \end{array} \right\} \left(\begin{array}{c} \Delta t \\ \text{assert} \\ v_{\pm} \end{array} \right) \left\{ \begin{array}{l} D \\ H \end{array} \right\}$$

Instruction : $\left(\begin{array}{c} \Delta t \\ \text{assert} \\ v_{\pm} \end{array} \right)$ ← Temps passé dans l'état qualitatif
 ← Connaissances bio (saturation, célérité, ...)
 ← Instruction qualitative ($v+$ ou $v-$)

- $\Delta t \in \mathbb{R}^+$
- **assert** : propriété dont les atomes sont :
 - $\text{slide}^{\pm}(u)$ ← La variable u « glisse » sur un bord (saturation)
 - $\text{noslide}^{\pm}(u)$ ← La variable u ne « glisse » pas
 - $C_u > 0$ ← Contraintes sur les célérités dans l'état courant

Version hybride de la logique de Hoare

[Behaegel *et al.*, 2016]

$$\text{Triplet de Hoare : } \left\{ \begin{array}{l} D' \\ H' \end{array} \right\} \left(\begin{array}{c} \Delta t \\ \text{assert} \\ v_{\pm} \end{array} \right) \left\{ \begin{array}{l} D \\ H \end{array} \right\}$$

Propriétés (pré- et postcondition) : $\left\{ \begin{array}{l} D \\ H \end{array} \right\}$ ← Partie discrète/qualitative
 ← Partie hybride/réelle

D et H sont des propriétés sur :

- $\eta_u \in \mathbb{N}$ ← Les états qualitatifs des variables
- $\pi_u \in [0..1]$ ← Les parties fractionnaires (positions dans l'état hybride)
- $C_{u,\omega,n}$ ← Les célérités
- Δt ← Le temps

Exemples de triplets de Hoare

$$\left\{ \begin{array}{l} D' \equiv (\eta_a = 0) \\ H' \equiv (\pi_a = 0.5) \end{array} \right\} \left(\begin{array}{c} 5 \\ \top \\ a+ \end{array} \right) \left\{ \begin{array}{l} D \equiv (\eta_a = 1) \\ H \equiv (\pi_a = 0) \end{array} \right\}$$

La variable a augmente d'un niveau qualitatif, en partant du milieu ($\pi_a = 0.5$) du niveau 0 et en arrivant en bas ($\pi_a = 0$) du niveau 1, le tout en 5 unités de temps. Aucune information sur les autres variables.

$$\left\{ \begin{array}{l} D' \equiv (\eta_x = 1 \wedge \eta_y = 1) \\ H' \equiv (\text{selon les } C_y) \end{array} \right\} \left(\begin{array}{c} \Delta t_1 \\ C_y \leq 0 \\ x- \end{array} \right); \left(\begin{array}{c} \Delta t_2 \\ \text{slide}^-(x) \\ y- \end{array} \right) \left\{ \begin{array}{l} D \equiv (\eta_x = 0 \wedge \eta_y = 0) \\ H \equiv (\pi_x = 0) \end{array} \right\}$$

La variable x descend d'un niveau qualitatif, pendant que y n'augmente pas ($C_y \leq 0$). Puis la variable y descend d'un niveau qualitatif, après que x a été complètement dégradée ($\text{slide}^-(x)$).

Exemples de triplets de Hoare

$$\left\{ \begin{array}{l} D' \equiv (\eta_a = 0) \\ H' \equiv (\pi_a = 0.5) \end{array} \right\} \left(\begin{array}{c} 5 \\ \top \\ a+ \end{array} \right) \left\{ \begin{array}{l} D \equiv (\eta_a = 1) \\ H \equiv (\pi_a = 0) \end{array} \right\}$$

La variable a augmente d'un niveau qualitatif, en partant du milieu ($\pi_a = 0.5$) du niveau 0 et en arrivant en bas ($\pi_a = 0$) du niveau 1, le tout en 5 unités de temps. Aucune information sur les autres variables.

$$\left\{ \begin{array}{l} D' \equiv (\eta_x = 1 \wedge \eta_y = 1) \\ H' \equiv \top \text{ (selon les } C_y) \end{array} \right\} \left(\begin{array}{c} \Delta t_1 \\ C_y \leq 0 \\ x- \end{array} \right); \left(\begin{array}{c} \Delta t_2 \\ \text{slide}^-(x) \\ y- \end{array} \right) \left\{ \begin{array}{l} D \equiv (\eta_x = 0 \wedge \eta_y = 0) \\ H \equiv (\pi_x = 0) \end{array} \right\}$$

La variable x descend d'un niveau qualitatif, pendant que y n'augmente pas ($C_y \leq 0$). Puis la variable y descend d'un niveau qualitatif, après que x a été complètement dégradée ($\text{slide}^-(x)$).

Exemples de triplets de Hoare

$$\left\{ \begin{array}{l} D' \equiv (\eta_a = 0) \\ H' \equiv (\pi_a = 0.5) \end{array} \right\} \left(\begin{array}{c} 5 \\ \top \\ a+ \end{array} \right) \left\{ \begin{array}{l} D \equiv (\eta_a = 1) \\ H \equiv (\pi_a = 0) \end{array} \right\}$$

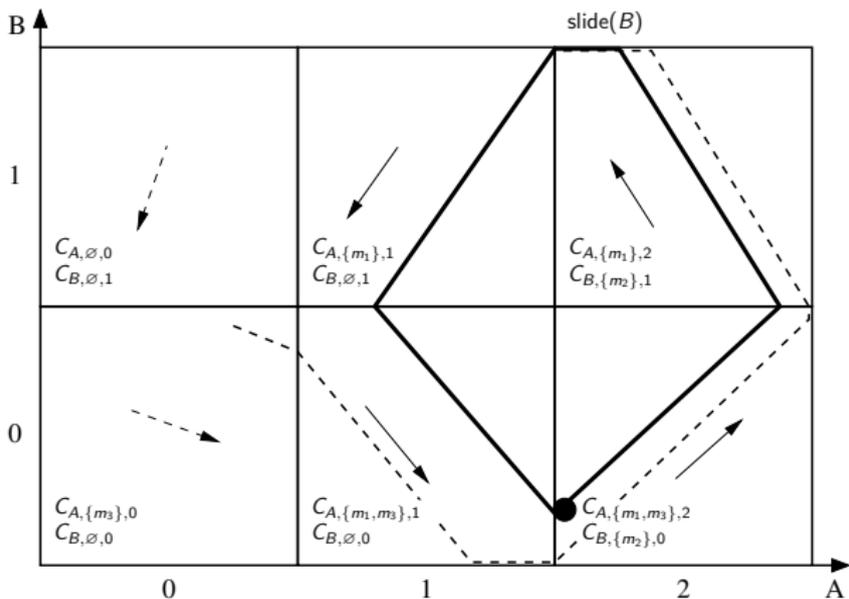
La variable a augmente d'un niveau qualitatif, en partant du milieu ($\pi_a = 0.5$) du niveau 0 et en arrivant en bas ($\pi_a = 0$) du niveau 1, le tout en 5 unités de temps. Aucune information sur les autres variables.

$$\left\{ \begin{array}{l} D' \equiv (\eta_x = 1 \wedge \eta_y = 1) \\ H' \equiv \top \text{ (selon les } C_y) \end{array} \right\} \left(\begin{array}{c} \Delta t_1 \\ C_y \leq 0 \\ x- \end{array} \right); \left(\begin{array}{c} \Delta t_2 \\ \text{slide}^-(x) \\ y- \end{array} \right) \left\{ \begin{array}{l} D \equiv (\eta_x = 0 \wedge \eta_y = 0) \\ H \equiv (\pi_x = 0) \end{array} \right\}$$

La variable x descend d'un niveau qualitatif, pendant que y n'augmente pas ($C_y \leq 0$). Puis la variable y descend d'un niveau qualitatif, après que x a été complètement dégradée ($\text{slide}^-(x)$).

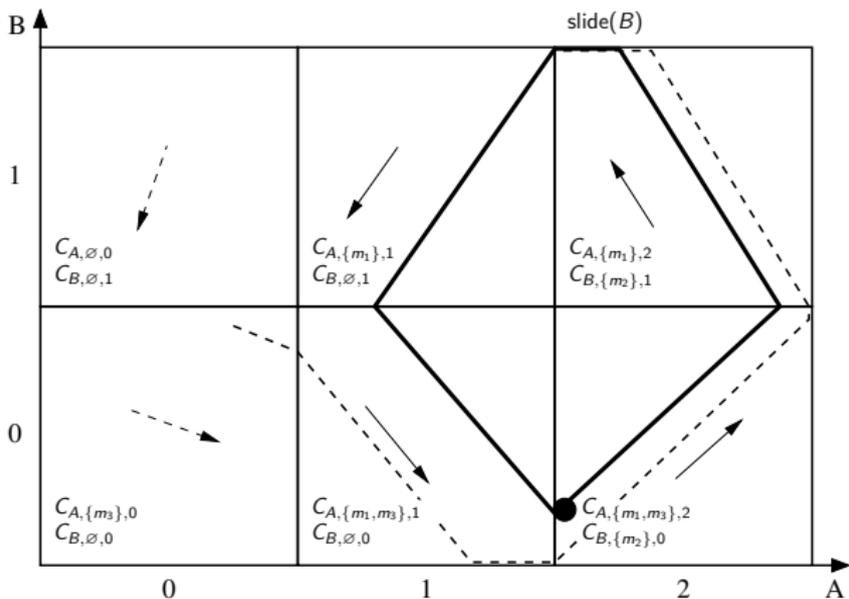
Inférence de paramètres par la logique de Hoare

$$\left\{ \begin{array}{l} D' \equiv D \\ H' \equiv ? \end{array} \right\} \left(\begin{array}{c} T_4 \\ \top \\ B+ \end{array} \right); \left(\begin{array}{c} T_3 \\ \text{slide}^+(B) \\ A- \end{array} \right); \left(\begin{array}{c} T_2 \\ \top \\ B- \end{array} \right); \left(\begin{array}{c} T_1 \\ \top \\ A+ \end{array} \right) \left\{ \begin{array}{l} D \equiv (\eta_A = 2 \wedge \eta_B = 0) \\ H \equiv \top \end{array} \right\}$$



Inférence de paramètres par la logique de Hoare

$$\left\{ \begin{array}{l} D' \equiv D \\ H' \equiv ? \end{array} \right\} \left(\begin{array}{c} T_4 \\ \top \\ B+ \end{array} \right); \left(\begin{array}{c} T_3 \\ \text{slide}^+(B) \\ A- \end{array} \right); \left(\begin{array}{c} T_2 \\ \top \\ B- \end{array} \right); \left(\begin{array}{c} T_1 \\ \top \\ A+ \end{array} \right) \left\{ \begin{array}{l} D \equiv (\eta_A = 2 \wedge \eta_B = 0) \\ H \equiv \top \end{array} \right\}$$



Plus faible précondition

Plus faible précondition : WP

Cas d'une instruction simple :

$$\left\{ \begin{array}{l} D' \\ H' \end{array} \right\} \left(\begin{array}{c} \Delta t \\ \text{assert} \\ v \pm \end{array} \right) \left\{ \begin{array}{l} D \\ H \end{array} \right\}$$

- $D' \equiv D[\eta_v \setminus \eta_v \pm 1]$ (remplacements)
- $H' \equiv H \wedge \Phi_v^\pm(\Delta t) \wedge \mathcal{F}_v(\Delta t) \wedge \neg \mathcal{W}_v^\pm \wedge \mathcal{A}(\Delta t, \text{assert}) \wedge \mathcal{J}_v$

Cas d'une séquence : $\{ Pre \} p_1 ; p_2 \{ Post \}$

- $\mathbf{WP}(p_1; p_2, Post) \equiv \mathbf{WP}(p_1, \mathbf{WP}(p_2, Post))$

Calcul du la plus faible précondition

$$H' \equiv H \wedge \Phi_v^+(\Delta t) \wedge \mathcal{F}_v(\Delta t) \wedge \neg \mathcal{W}_v^+ \wedge \mathcal{A}(\Delta t, \text{assert}) \wedge \mathcal{J}_v$$

Calcul de la plus faible précondition

$$H' \equiv H \wedge \Phi_v^+(\Delta t) \wedge \mathcal{F}_v(\Delta t) \wedge \neg \mathcal{W}_v^+ \wedge \mathcal{A}(\Delta t, \text{assert}) \wedge \mathcal{J}_v$$

Hypothèses sur le changement d'état qualitatif de v :

$$\Phi_v^+(\Delta t) \equiv \underbrace{(\pi_v = 1)}_{\text{1}} \wedge \bigwedge_{\substack{\omega \in R^-(v) \\ n \in \llbracket 0.. \max_v \rrbracket}} \left(\underbrace{\Phi_v^\omega}_{\text{a}} \wedge \underbrace{(\eta_v = n)}_{\text{b}} \right) \Rightarrow \underbrace{(C_{v,\omega,n} > 0)}_{\text{2}} \wedge \underbrace{(\pi'_v = \pi_v - C_{v,\omega,n} \cdot \Delta t)}_{\text{3}}$$

- a** Les ressources de v dans l'état courant sont ω
- b** Le niveau qualitatif de v dans l'état courant est n
- 1** La variable v doit terminer sur le bord correspondant à son changement d'état qualitatif
- 2** La célérité dans l'état courant pousse v vers ce bord
- 3** La variable v met un temps Δt pour atteindre ce bord

Calcul de la plus faible précondition

$$H' \equiv H \wedge \Phi_v^+(\Delta t) \wedge \mathcal{F}_v(\Delta t) \wedge \neg \mathcal{W}_v^+ \wedge \mathcal{A}(\Delta t, \text{assert}) \wedge \mathcal{J}_v$$

La variable v ne rencontre pas de mur : $\neg \mathcal{W}_v^+ \equiv \neg IW_v^+ \wedge \neg EW_v^+$

Mur externe :

$$EW_v^+ \equiv \underbrace{(\eta_v = \max_v)}_{\text{1}} \wedge \bigwedge_{\omega \in R^-(v)} \left(\Phi_v^\omega \Rightarrow \underbrace{C_{v,\omega,\max_v} > 0}_{\text{2}} \right)$$

- a** Les valeurs qualitatives de v vont de 0 à \max_v
- 1** La variable v est au maximum de ses valeurs qualitatives...
- 2** ...Et sa célérité la pousse vers le haut de l'état qualitatif

Calcul de la plus faible précondition

$$H' \equiv H \wedge \Phi_v^+(\Delta t) \wedge \mathcal{F}_v(\Delta t) \wedge \neg \mathcal{W}_v^+ \wedge \mathcal{A}(\Delta t, \text{assert}) \wedge \mathcal{J}_v$$

La variable v ne rencontre pas de mur : $\neg \mathcal{W}_v^+ \equiv \neg IW_v^+ \wedge \neg EW_v^+$

Mur interne :

$$IW_v^+ \equiv \underbrace{(\eta_v < \max_v)}_{\text{1}} \wedge \bigwedge_{\substack{\omega, \omega' \subset R^-(v) \\ n \in [0.. \max_v]}} \left(\underbrace{((\eta_v = n) \wedge (m = n + 1))}_{\text{a}} \wedge \underbrace{\Phi_v^\omega \wedge \Phi_{v+}^{\omega'}}_{\text{b}} \right) \Rightarrow \underbrace{C_{v, \omega, n} > 0 \wedge C_{v, \omega', m} < 0}_{\text{2}}$$

- 1** La variable v n'est pas dans son niveau qualitatif maximum
- a** Le niveau courant de v est n ; son niveau supérieur est m
- b** Les ressources de v sont ω dans l'état courant et deviennent ω' si on incrémente v
- 2** Les célérités poussent v vers un bord qu'elle ne peut pas franchir

Calcul de la plus faible précondition

$$H' \equiv H \wedge \Phi_v^+(\Delta t) \wedge \mathcal{F}_v(\Delta t) \wedge \neg \mathcal{W}_v^+ \wedge \mathcal{A}(\Delta t, \text{assert}) \wedge \mathcal{J}_v$$

Aucune variable ne change d'état qualitatif avant v :

$$\mathcal{F}_v(\Delta t) \equiv \bigwedge_{u \in V \setminus \{v\}} \textcircled{a} \left(\bigwedge_{\substack{\omega \in R^-(u) \\ n \in \llbracket 0..b_u \rrbracket}} \underbrace{\left((\eta_u = n) \wedge \Phi_u^\omega \wedge C_{u,\omega,n} > 0 \wedge \pi'_{u,i} > \pi_{u,i} - C_{u,\omega,n} \cdot \Delta t \right)}_{\textcircled{1}} \Rightarrow \underbrace{\mathcal{W}_u^+}_{\textcircled{2}} \right) \wedge \left(\bigwedge_{\substack{\omega \in R^-(u) \\ n \in \llbracket 0..b_u \rrbracket}} \underbrace{\left((\eta_u = n) \wedge \Phi_u^\omega \wedge C_{u,\omega,n} < 0 \wedge \pi'_{u,i} < \pi_{u,i} - C_{u,\omega,n} \cdot \Delta t \right)}_{\textcircled{1}} \Rightarrow \underbrace{\mathcal{W}_u^-}_{\textcircled{2}} \right) .$$

a Pour toute variable u autre que v ...

1 Si u touche un bord avant v ,

2 Alors u rencontre un mur qui l'empêche de passer

Calcul de la plus faible précondition

$$H' \equiv H \wedge \Phi_v^+(\Delta t) \wedge \mathcal{F}_v(\Delta t) \wedge \neg \mathcal{W}_v^+ \wedge \mathcal{A}(\Delta t, \text{assert}) \wedge \mathcal{J}_v$$

Prise en compte des assertions : $\mathcal{A}(\Delta t, \text{assert})$

- Les C_u sont transformés en $C_{u,\omega,n}$ en fonction de l'état courant
- Les $\text{slide}^+(u)$ décrivent un glissement donné par $\mathcal{S}^+(\Delta t)$:

$$\mathcal{S}^+(\Delta t) \equiv \underbrace{\pi_u = 1}_{\text{1}} \wedge \underbrace{(C_{u,\omega,n} > 0 \Rightarrow \pi'_u > \pi_u - C_{u,\omega,n} \cdot \Delta t)}_{\text{2}}$$

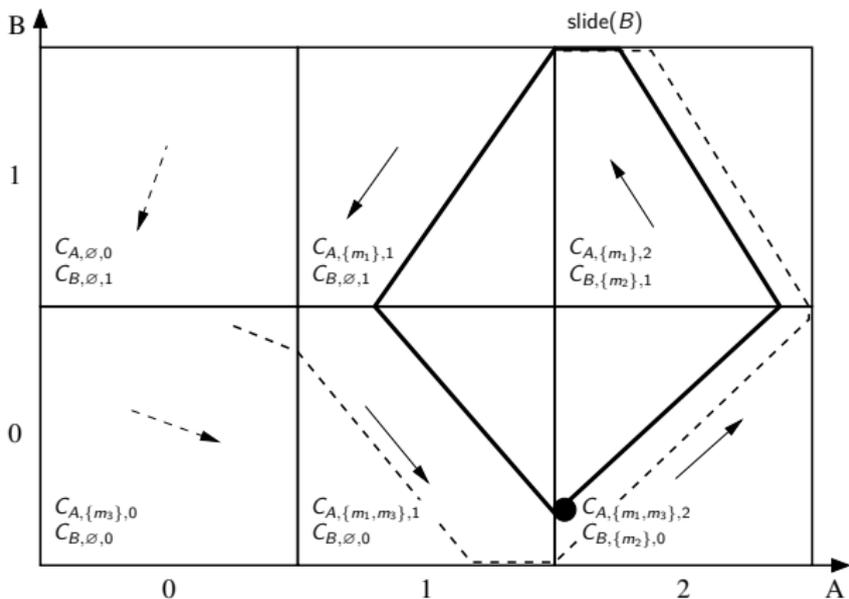
- 1 u finit par toucher le haut de l'état qualitatif du fait du glissement
- 2 Si la célérité de u est non-nulle, alors on obtient cette inégalité

Jointure entre deux états qualitatifs : \mathcal{J}_v

- Toutes les variables gardent leur partie fractionnaire
- Sauf v qui se retrouve sur le bord opposé

Inférence de paramètres par la logique de Hoare

$$\left\{ \begin{array}{l} D' \equiv D \\ H' \equiv ? \end{array} \right\} \left(\begin{array}{c} T_4 \\ \top \\ B+ \end{array} \right); \left(\begin{array}{c} T_3 \\ \text{slide}^+(B) \\ A- \end{array} \right); \left(\begin{array}{c} T_2 \\ \top \\ B- \end{array} \right); \left(\begin{array}{c} T_1 \\ \top \\ A+ \end{array} \right) \left\{ \begin{array}{l} D \equiv (\eta_A = 2 \wedge \eta_B = 0) \\ H \equiv \top \end{array} \right\}$$



Résultat de l'inférence

$$\begin{aligned}
H_F \equiv & \left(\neg(C_{B,\emptyset,0} > 0) \vee \neg(1 > \pi_B^{0'} - C_{B,\emptyset,0} \cdot T_1) \right) \\
& \wedge (C_{A,\{m_1,m_3\},1} > 0) \wedge (\pi_A^{1'} = 1 - C_{A,\{m_1,m_3\},1} \cdot T_1) \\
& \wedge \left(\neg(C_{A,\{m_1\},1} > 0) \vee \neg(1 > \pi_A^{1'} - C_{A,\{m_1\},1} \cdot T_2) \right) \\
& \wedge \left((C_{A,\emptyset,0} > 0) \vee \neg(C_{A,\{m_1\},1} < 0) \vee \neg(1 < \pi_A^{1'} - C_{A,\{m_1\},1} \cdot T_2) \right) \\
& \wedge (C_{B,\emptyset,1} < 0) \wedge (1 = 0 - C_{B,\emptyset,1} \cdot T_2) \\
& \wedge \left(\neg(C_{B,\{m_2\},1} < 0) \vee \neg(0 < 1 - C_{B,\{m_2\},1} \cdot T_3) \right) \\
& \wedge (C_{A,\{m_1\},2} < 0 \wedge (\pi_A^{3'} = 0 - C_{A,\{m_1\},2} \cdot T_3)) \\
& \wedge \left(\neg(C_{B,\{m_2\},1} > 0) \vee (0 > 1 - C_{B,\{m_2\},1} \cdot T_3) \right) \\
& \wedge \left(\neg(C_{A,\{m_1,m_3\},2} < 0) \vee \neg(0 < \pi_A^{3'} - C_{A,\{m_1,m_3\},2} \cdot T_4) \right) \\
& \wedge (C_{B,\{m_2\},0} > 0) \wedge (\pi_B^{0'} = 1 - C_{B,\{m_2\},0} \cdot T_4) .
\end{aligned}$$

Travail basé sur :

- Une version hybride du modèle de Thomas
- Une version hybride de la logique de Hoare
- La logique des prédicats (plus faible précondition) de Dijkstra

Travail réalisé :

→ Fournit des contraintes sur :

- les célérités (paramètres)
- les états au cours de l'exécution (parties fractionnaires)
- en fonction du temps de chaque étape

→ Implémentation réalisée

Limites actuelles :

- Résultat complexe et long à interpréter ⇒ Optimisations + solveur !
- Preuves de correction/complétude ⇒ En cours !
- Le programme laisse peu de place à l'incertitude
⇒ Autoriser des embranchements (\forall, \exists) ?

Bibliographie

- René Thomas. [Boolean formalization of genetic control circuits](#). *Journal of Theoretical Biology* 42 (3), 1973.
- Émilien Cornillon, Jean-Paul Comet, Gilles Bernot, Gilles Énée. [Hybrid gene network: a new formalism and a software environment](#). *Modelling Complex Biological Systems in the Context of Genomics*. 2016.
- Charles A. R. Hoare. [An axiomatic basis for computer programming](#). *Communications of the ACM* 12 (10), 1969.
- Edsger W. Dijkstra. [Guarded commands, nondeterminacy and formal derivation of programs](#). *Communications of the ACM* 18, 1975.
- Gilles Bernot, Jean-Paul Comet, Zohra Khalis, Adrien Richard, Olivier Roux. [A genetically modified Hoare logic](#). Rapport de recherche, *arXiv: 1506.05887*, 2015.
- Jonathan Behaegel, Jean-Paul Comet, Maxime Folschette. [A Hybridisation of the Genetically Modified Hoare Logic](#). Rapport de recherche, *arXiv: 1610.06715*, 2016