

Propriétés de vivacité sous conditions d'équité et sémantique des systèmes d'événements avec la méthode B

Héctor Ruíz Barradas

Laboratoire Logiciels Systèmes Réseaux

Universidad Autónoma Metropolitana Azcapotzalco

22 décembre 2006

Plan

Introduction

Un cadre formel pour la vivacité

Le cas de progrès minimal

Le cas d'équité faible

Le raffinement

Conclusions et travail futur

Introduction

Système d'événements

- Modèle de calcul :

$$\underline{\text{do}} e_1 \parallel e_2 \dots \parallel e_n \underline{\text{od}}$$

- Chaque e_i est une commande gardée :

$$e_i \hat{=} g_i \implies c_i$$

Système d'événements

- Modèle de calcul :

$$\underline{\text{do}} e_1 \parallel e_2 \dots \parallel e_n \underline{\text{od}}$$

- Chaque e_i est une commande gardée :

$$e_i \hat{=} g_i \implies c_i \quad \text{ou} \quad e_i \hat{=} @z.(g_i \implies c_i)$$

Système d'événements

- Modèle de calcul :

$$\underline{\text{do}} e_1 \parallel e_2 \dots \parallel e_n \underline{\text{od}}$$

- Chaque e_i est une commande gardée :

$$e_i \hat{=} g_i \implies c_i \quad \text{ou} \quad e_i \hat{=} @z.(g_i \implies c_i)$$

- Hypothèses d'équité :

Système d'événements

- Modèle de calcul :

$$\underline{\text{do}} \ e_1 \ \parallel \ e_2 \ \dots \ \parallel \ e_n \ \underline{\text{od}}$$

- Chaque e_i est une commande gardée :

$$e_i \hat{=} g_i \implies c_i \quad \text{ou} \quad e_i \hat{=} @z.(g_i \implies c_i)$$

- Hypothèses d'équité :

B événementiel : **progrès minimal**

Système d'événements

- Modèle de calcul :

$$\underline{\text{do}} \ e_1 \ \parallel \ e_2 \ \dots \ \parallel \ e_n \ \underline{\text{od}}$$

- Chaque e_i est une commande gardée :

$$e_i \hat{=} g_i \implies c_i \quad \text{ou} \quad e_i \hat{=} @z.(g_i \implies c_i)$$

- Hypothèses d'équité :

B événementiel :

UNITY :

progrès minimal

équité inconditionnelle

Système d'événements

- Modèle de calcul :

$$\underline{\text{do}} \ e_1 \ \parallel \ e_2 \ \dots \ \parallel \ e_n \ \underline{\text{od}}$$

- Chaque e_i est une commande gardée :

$$e_i \hat{=} g_i \implies c_i \quad \text{ou} \quad e_i \hat{=} @z.(g_i \implies c_i)$$

- Hypothèses d'équité :

B événementiel :	progrès minimal
UNITY :	équité inconditionnelle
TLA, Action Systems :	équité faible

Système d'événements

- Modèle de calcul :

$$\underline{\text{do}} \ e_1 \ \parallel \ e_2 \ \dots \ \parallel \ e_n \ \underline{\text{od}}$$

- Chaque e_i est une commande gardée :

$$e_i \hat{=} g_i \implies c_i \quad \text{ou} \quad e_i \hat{=} @z.(g_i \implies c_i)$$

- Hypothèses d'équité :

B événementiel :	progrès minimal
UNITY :	équité inconditionnelle
TLA, Action Systems :	équité faible, équité forte

Spécification et raffinement

- Approches logiques : **ensemble de formules.**

exemple

- TLA
- UNITY
- Propriétés de sûreté.
- Propriétés de vivacité.
- Système de preuve.
- Approches algorithmiques : notation de programmation.

exemple

- Action Systems.
- B-événementiel.
- Model Checking.
- Notion de raffinement d'actions.
- Calcul des plus petits raffinements.

Spécification et raffinement

- Approches logiques : ensemble de formules.

exemple

- TLA
 - UNITY
- Propriétés de sûreté.
 - Propriétés de vivacité.
 - Système de preuve.
- Approches algorithmiques : notation de programmation.

exemple

- Action Systems.
 - B événementiel.
- Notion d'invariant.
 - Notion de terminaison d'itération.
 - Calcul de plus faible préconditions.

Spécification et raffinement

- Approches logiques : ensemble de formules.

exemple

- TLA
- UNITY
- Propriétés de sûreté.
- Propriétés de vivacité.
- Système de preuve.
- Approches algorithmiques : notation de programmation.

exemple

- Action Systems.
- B événementiel.
- Notion d'invariant.
- Notion de terminaison d'itération.
- Calcul de plus faible préconditions.

Spécification et raffinement

- Approches logiques : ensemble de formules.

exemple

- TLA
- UNITY
- Propriétés de sûreté.
- **Propriétés de vivacité.**
- Système de preuve.
- Approches algorithmiques : notation de programmation.

exemple

- Action Systems.
- B événementiel.
- Notion d'invariant.
- Notion de terminaison d'itération.
- Calcul de plus faible préconditions.

Spécification et raffinement

- Approches logiques : ensemble de formules.

exemple

- TLA
 - UNITY
 - Propriétés de sûreté.
 - Propriétés de vivacité.
 - **Systeme de preuve.**
- Approches algorithmiques : notation de programmation.

exemple

- Action Systems.
- B événementiel.
- Notion d'invariant.
- Notion de terminaison d'itération.
- Calcul de plus faible préconditions.

Spécification et raffinement

- Approches logiques : ensemble de formules.

exemple

- TLA
- UNITY
- Propriétés de sûreté.
- Propriétés de vivacité.
- Système de preuve.
- Approches algorithmiques : **notation de programmation.**

exemple

- Action Systems.
- B événementiel.
- Notion d'invariant.
- Notion de terminaison d'itération.
- Calcul de plus faible préconditions.

Spécification et raffinement

- Approches logiques : ensemble de formules.

exemple

- TLA
- UNITY
- Propriétés de sûreté.
- Propriétés de vivacité.
- Système de preuve.
- Approches algorithmiques : notation de programmation.

exemple

- Action Systems.
- B événementiel.
- Notion d'invariant.
- Notion de terminaison d'itération.
- Calcul de plus faible préconditions.

Spécification et raffinement

- Approches logiques : ensemble de formules.

exemple

- TLA
- UNITY
- Propriétés de sûreté.
- Propriétés de vivacité.
- Système de preuve.
- Approches algorithmiques : notation de programmation.

exemple

- Action Systems.
- B événementiel.
- **Notion d'invariant.**
- Notion de terminaison d'itération.
- Calcul de plus faible préconditions.

Spécification et raffinement

- Approches logiques : ensemble de formules.

exemple

- TLA
 - UNITY
 - Propriétés de sûreté.
 - Propriétés de vivacité.
 - Système de preuve.
- Approches algorithmiques : notation de programmation.

exemple

- Action Systems.
- B événementiel.
- Notion d'invariant.
- **Notion de terminaison d'itération.**
- Calcul de plus faible préconditions.

Spécification et raffinement

- Approches logiques : ensemble de formules.

exemple

- TLA
 - UNITY
 - Propriétés de sûreté.
 - Propriétés de vivacité.
 - Système de preuve.
- Approches algorithmiques : notation de programmation.

exemple

- Action Systems.
- B événementiel.
- Notion d'invariant.
- Notion de terminaison d'itération.
- Calcul de plus faible préconditions.

Proposition

- Deux constatations :
 1. L'approche algorithmique : utilité pratique.
 2. L'approche logique : raisonnement sur les propriétés.
- Une proposition :
 1. Description algorithmique par le B événementiel.
 2. Propriétés de vivacité dans le style de UNITY.

Proposition

- Deux constatations :
 1. L'approche algorithmique : utilité pratique.
 2. L'approche logique : raisonnement sur les propriétés.
- Une proposition :
 1. Description algorithmique par le B événementiel.
 2. Propriétés de vivacité dans le style de UNITY.

Proposition

- Deux constatations :
 1. L'approche algorithmique : utilité pratique.
 2. L'approche logique : raisonnement sur les propriétés.
- Une proposition :
 1. Description algorithmique par le B événementiel.
 2. Propriétés de vivacité dans le style de UNITY.

Proposition

- Deux constatations :
 1. L'approche algorithmique : utilité pratique.
 2. L'approche logique : raisonnement sur les propriétés.
- Une proposition :
 1. Description algorithmique par le B événementiel.
 2. Propriétés de vivacité dans le style de UNITY.

Un cadre formel pour la vivacité

Notation

- Système d'événements \mathcal{S} composé de :
 - Un vecteur de variables d'état : x .
 - Un invariant $I(x)$.
 - Un ensemble d'événements E .
- L'ensemble d'états du système :

$$u = \{z \mid I(z)\}$$

- Chaque e dans E est un transformateur d'ensembles :

$$e \in \mathbb{P}(u) \rightarrow \mathbb{P}(u)$$

- $t \subseteq u$, $e(t)$ est la plus faible précondition pour établir t :

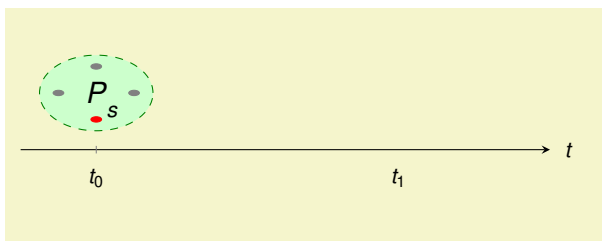
$$e(t) = \{z \mid z \in u \wedge wp(e, x \in t)\}$$

- Le choix d'événements dans E est S :

$$S = \parallel_{e \in E} e$$

Atteignabilité

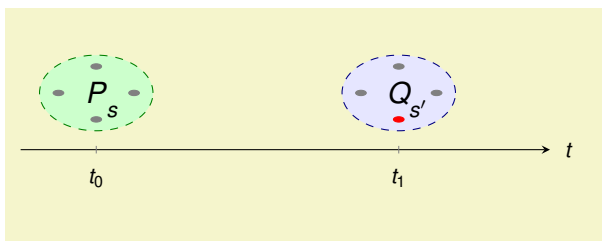
- Notion informelle :



- Relation d'atteignabilité \mathcal{L}_E ($\mathcal{L}_E \in \mathbb{P}(u) \leftrightarrow \mathbb{P}(u)$)
- \mathcal{L}_E est la plus petite relation qui satisfait :
 1. Base : $E \subseteq \mathcal{L}_E$.
 2. Transitivité : $\mathcal{L}_E ; \mathcal{L}_E \subseteq \mathcal{L}_E$.
 3. Disjonction : $I \times \{q\} \subseteq \mathcal{L}_E \Rightarrow \bigcup(I) \mapsto q \in \mathcal{L}_E$)
- Équivalence : $P \sim Q \equiv \text{set}(P) \mapsto \text{set}(P) \in \mathcal{L}_E$

Atteignabilité

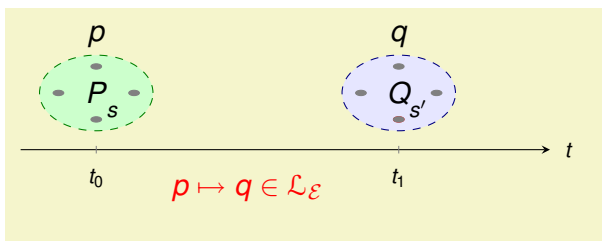
- Notion informelle :



- Relation d'atteignabilité $\mathcal{L}_{\mathcal{E}}$ ($\mathcal{L}_{\mathcal{E}} \in \mathbb{P}(u) \leftrightarrow \mathbb{P}(u)$)
- $\mathcal{L}_{\mathcal{E}}$ est la plus petite relation qui satisfait :
 1. Base : $\mathcal{E} \subseteq \mathcal{L}_{\mathcal{E}}$.
 2. Transitivité : $\mathcal{L}_{\mathcal{E}} ; \mathcal{L}_{\mathcal{E}} \subseteq \mathcal{L}_{\mathcal{E}}$.
 3. Disjonction : $I \times \{q\} \subseteq \mathcal{L}_{\mathcal{E}} \Rightarrow \bigcup(I) \mapsto q \in \mathcal{L}_{\mathcal{E}}$
- Équivalence : $P \sim Q \equiv \text{set}(P) \mapsto \text{set}(P) \in \mathcal{L}_{\mathcal{E}}$

Atteignabilité

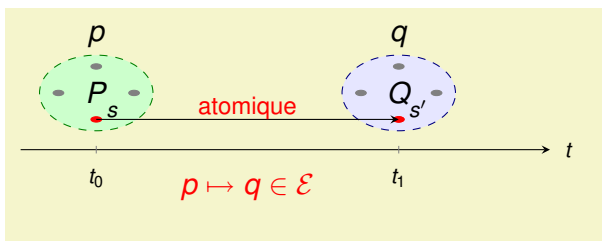
- Notion informelle :



- Relation d'atteignabilité $\mathcal{L}_\mathcal{E}$ ($\mathcal{L}_\mathcal{E} \in \mathbb{P}(u) \leftrightarrow \mathbb{P}(u)$)
- $\mathcal{L}_\mathcal{E}$ est la plus petite relation qui satisfait :
 - Base : $\mathcal{E} \subseteq \mathcal{L}_\mathcal{E}$.
 - Transitivité : $\mathcal{L}_\mathcal{E} ; \mathcal{L}_\mathcal{E} \subseteq \mathcal{L}_\mathcal{E}$.
 - Disjonction : $I \times \{q\} \subseteq \mathcal{L}_\mathcal{E} \Rightarrow \bigcup(I) \mapsto q \in \mathcal{L}_\mathcal{E}$
- Équivalence : $P \sim Q \equiv \text{set}(P) \mapsto \text{set}(P) \in \mathcal{L}_\mathcal{E}$

Atteignabilité

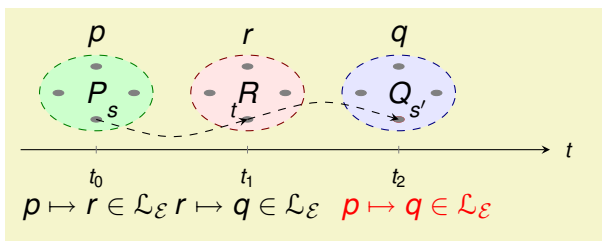
- Notion informelle :



- Relation d'atteignabilité $\mathcal{L}_{\mathcal{E}}$ ($\mathcal{L}_{\mathcal{E}} \in \mathbb{P}(u) \leftrightarrow \mathbb{P}(u)$)
- $\mathcal{L}_{\mathcal{E}}$ est la plus petite relation qui satisfait :
 - Base : $\mathcal{E} \subseteq \mathcal{L}_{\mathcal{E}}$.
 - Transitivité : $\mathcal{L}_{\mathcal{E}} ; \mathcal{L}_{\mathcal{E}} \subseteq \mathcal{L}_{\mathcal{E}}$.
 - Disjonction : $I \times \{q\} \subseteq \mathcal{L}_{\mathcal{E}} \Rightarrow \bigcup(I) \mapsto q \in \mathcal{L}_{\mathcal{E}}$
- Équivalence : $P \sim Q \equiv \text{set}(P) \mapsto \text{set}(P) \in \mathcal{L}_{\mathcal{E}}$

Atteignabilité

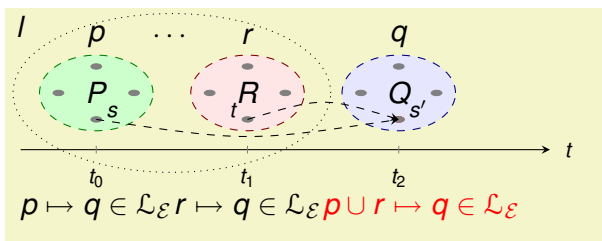
- Notion informelle :



- Relation d'atteignabilité $\mathcal{L}_\mathcal{E}$ ($\mathcal{L}_\mathcal{E} \in \mathbb{P}(u) \leftrightarrow \mathbb{P}(u)$)
- $\mathcal{L}_\mathcal{E}$ est la plus petite relation qui satisfait :
 - Base : $\mathcal{E} \subseteq \mathcal{L}_\mathcal{E}$.
 - Transitivité : $\mathcal{L}_\mathcal{E} ; \mathcal{L}_\mathcal{E} \subseteq \mathcal{L}_\mathcal{E}$.
 - Disjonction : $l \times \{q\} \subseteq \mathcal{L}_\mathcal{E} \Rightarrow \bigcup(l) \mapsto q \in \mathcal{L}_\mathcal{E}$)
- Équivalence : $P \sim Q \equiv \text{set}(P) \mapsto \text{set}(P) \in \mathcal{L}_\mathcal{E}$

Atteignabilité

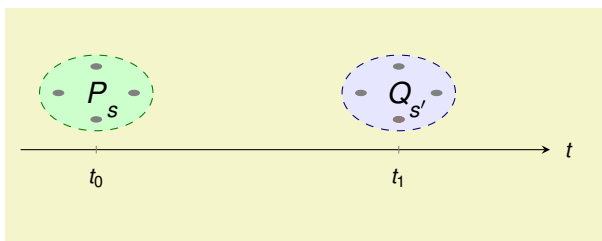
- Notion informelle :



- Relation d'atteignabilité \mathcal{L}_ε ($\mathcal{L}_\varepsilon \in \mathbb{P}(u) \leftrightarrow \mathbb{P}(u)$)
- \mathcal{L}_ε est la plus petite relation qui satisfait :
 1. Base : $\mathcal{E} \subseteq \mathcal{L}_\varepsilon$.
 2. Transitivité : $\mathcal{L}_\varepsilon ; \mathcal{L}_\varepsilon \subseteq \mathcal{L}_\varepsilon$.
 3. Disjonction : $I \times \{q\} \subseteq \mathcal{L}_\varepsilon \Rightarrow \bigcup(I) \mapsto q \in \mathcal{L}_\varepsilon$)
- Équivalence : $P \sim Q \equiv \text{set}(P) \mapsto \text{set}(P) \in \mathcal{L}_\varepsilon$

Atteignabilité

- Notion informelle :



- Relation d'atteignabilité $\mathcal{L}_\mathcal{E}$ ($\mathcal{L}_\mathcal{E} \in \mathbb{P}(u) \leftrightarrow \mathbb{P}(u)$)
- $\mathcal{L}_\mathcal{E}$ est la plus petite relation qui satisfait :
 1. Base : $\mathcal{E} \subseteq \mathcal{L}_\mathcal{E}$.
 2. Transitivité : $\mathcal{L}_\mathcal{E} ; \mathcal{L}_\mathcal{E} \subseteq \mathcal{L}_\mathcal{E}$.
 3. Disjonction : $I \times \{q\} \subseteq \mathcal{L}_\mathcal{E} \Rightarrow \bigcup(I) \mapsto q \in \mathcal{L}_\mathcal{E}$)
- Équivalence : $P \rightsquigarrow Q \equiv \text{set}(P) \mapsto \text{set}(P) \in \mathcal{L}_\mathcal{E}$

Terminaison de l'itération

- Interprétation d'atteignabilité en tant que terminaison :


$\{P\}$

- W un "pas" de l'itération : $W \in \mathbb{P}(u) \rightarrow \mathbb{P}(u)$.
 - $W(q)$: plus faible précondition pour établir q
 - monotone : $p \subseteq q \Rightarrow W(p) \subseteq W(q)$.
 - strict : $W(\emptyset) = \emptyset$.

Terminaison de l'itération

- Interprétation d'atteignabilité en tant que terminaison :


$\{P\}$ do e_1 [] e_2 [] ... [] e_n od



- W un "pas" de l'itération : $W \in \mathbb{P}(u) \rightarrow \mathbb{P}(u)$.
 - $W(q)$: plus faible précondition pour établir q
 - monotone : $p \subseteq q \Rightarrow W(p) \subseteq W(q)$.
 - strict : $W(\emptyset) = \emptyset$.

Terminaison de l'itération


- Interprétation d'atteignabilité en tant que terminaison :

$$\{P\} \text{ do } e_1 \parallel e_2 \parallel \dots \parallel e_n \text{ od } \{Q\}$$


- W un “pas” de l'itération : $W \in \mathbb{P}(u) \rightarrow \mathbb{P}(u)$.
 - $W(q)$: plus faible précondition pour établir q
 - monotone : $p \subseteq q \Rightarrow W(p) \subseteq W(q)$.
 - strict : $W(\emptyset) = \emptyset$.

Terminaison de l'itération

- Interprétation d'atteignabilité en tant que terminaison :

$$\{P\} \text{ do } \overbrace{e_1 \parallel e_2 \parallel \dots \parallel e_n}^W \text{ od } \{Q\}$$


- W un “pas” de l'itération : $W \in \mathbb{P}(u) \rightarrow \mathbb{P}(u)$.
 - $W(q)$: plus faible précondition pour établir q
 - monotone : $p \subseteq q \Rightarrow W(p) \subseteq W(q)$.
 - strict : $W(\emptyset) = \emptyset$.

La relation de terminaison

- Le corps de l'itération $\mathcal{F}(q)$:

$$\mathcal{F}(q) \hat{=} (\bar{q} \Longrightarrow W)$$

- L'itération :

$$\mathcal{F}(q)^\wedge = (\mathcal{F}(q) ; \mathcal{F}(q)^\wedge) \parallel \text{skip}$$

- L'ensemble de terminaison :

$$\text{pre}(\mathcal{F}(q)^\wedge) = \text{fix}(\mathcal{F}(q))$$

- $\text{fix}(\mathcal{F}(q))$ contient q et les itérations de W terminant en q :

$$\mathcal{F}(q)^\alpha = \bigcup \beta \cdot (\beta < \alpha \mid \mathcal{F}(q)(\mathcal{F}(q)^\beta))$$

- La relation de terminaison \mathcal{T} :

$$\mathcal{T} \hat{=} \{p \mapsto q \mid p \subseteq u \wedge q \subseteq u \wedge p \subseteq \text{fix}(\mathcal{F}(q))\}$$

La relation de terminaison

- Le corps de l'itération $\mathcal{F}(q)$:

$$\mathcal{F}(q) \hat{=} (\bar{q} \Longrightarrow W)$$

- L'itération :

$$\mathcal{F}(q)^\wedge = (\mathcal{F}(q) ; \mathcal{F}(q)^\wedge) \parallel \text{skip}$$

- L'ensemble de terminaison :

$$\text{pre}(\mathcal{F}(q)^\wedge) = \text{fix}(\mathcal{F}(q))$$

- $\text{fix}(\mathcal{F}(q))$ contient q et les itérations de W terminant en q :

$$\mathcal{F}(q)^\alpha = \bigcup \beta \cdot (\beta < \alpha \mid \mathcal{F}(q)(\mathcal{F}(q)^\beta))$$

- La relation de terminaison \mathcal{T} :

$$\mathcal{T} \hat{=} \{p \mapsto q \mid p \subseteq u \wedge q \subseteq u \wedge p \subseteq \text{fix}(\mathcal{F}(q))\}$$

La relation de terminaison

- Le corps de l'itération $\mathcal{F}(q)$:

$$\mathcal{F}(q) \hat{=} (\bar{q} \Longrightarrow W)$$

- L'itération :

$$\mathcal{F}(q)^\wedge = (\mathcal{F}(q) ; \mathcal{F}(q)^\wedge) \parallel \text{skip}$$

- L'ensemble de terminaison :

$$\text{pre}(\mathcal{F}(q)^\wedge) = \text{fix}(\mathcal{F}(q))$$

- $\text{fix}(\mathcal{F}(q))$ contient q et les itérations de W terminant en q :

$$\mathcal{F}(q)^\alpha = \bigcup \beta \cdot (\beta < \alpha \mid \mathcal{F}(q)(\mathcal{F}(q)^\beta))$$

- La relation de terminaison \mathcal{T} :

$$\mathcal{T} \hat{=} \{p \mapsto q \mid p \subseteq u \wedge q \subseteq u \wedge p \subseteq \text{fix}(\mathcal{F}(q))\}$$

La relation de terminaison

- Le corps de l'itération $\mathcal{F}(q)$:

$$\mathcal{F}(q) \hat{=} (\bar{q} \Longrightarrow W)$$

- L'itération :

$$\mathcal{F}(q)^\wedge = (\mathcal{F}(q) ; \mathcal{F}(q)^\wedge) \parallel \text{skip}$$

- L'ensemble de terminaison :

$$\text{pre}(\mathcal{F}(q)^\wedge) = \text{fix}(\mathcal{F}(q))$$

- $\text{fix}(\mathcal{F}(q))$ contient q et les itérations de W terminant en q :

$$\mathcal{F}(q)^\alpha = \bigcup \beta \cdot (\beta < \alpha \mid \mathcal{F}(q)(\mathcal{F}(q)^\beta))$$

- La relation de terminaison \mathcal{T} :

$$\mathcal{T} \hat{=} \{p \mapsto q \mid p \subseteq u \wedge q \subseteq u \wedge p \subseteq \text{fix}(\mathcal{F}(q))\}$$

La relation de terminaison

- Le corps de l'itération $\mathcal{F}(q)$:

$$\mathcal{F}(q) \hat{=} (\bar{q} \Longrightarrow W)$$

- L'itération :

$$\mathcal{F}(q)^\wedge = (\mathcal{F}(q) ; \mathcal{F}(q)^\wedge) \parallel \text{skip}$$

- L'ensemble de terminaison :

$$\text{pre}(\mathcal{F}(q)^\wedge) = \text{fix}(\mathcal{F}(q))$$

- $\text{fix}(\mathcal{F}(q))$ contient q et les itérations de W terminant en q :

$$\mathcal{F}(q)^\alpha = \bigcup \beta \cdot (\beta < \alpha \mid \mathcal{F}(q)(\mathcal{F}(q)^\beta))$$

- La relation de terminaison \mathcal{T} :

$$\mathcal{T} \hat{=} \{ p \mapsto q \mid p \subseteq u \wedge q \subseteq u \wedge p \subseteq \text{fix}(\mathcal{F}(q)) \}$$

Équivalence entre atteignabilité et terminaison

Théorème

- Si W est monotone.
- Si W est strict.
- $p \mapsto q \in \mathcal{E} \Rightarrow p \subseteq q \cup W(q)$
- si $W(q) \mapsto q \in \mathcal{L}_{\mathcal{E}}$ et
- $p \subseteq q \Rightarrow p \mapsto q \in \mathcal{E}$

alors

$$\mathcal{L}_{\mathcal{E}} = \mathcal{T}$$

Preuve

Case $\mathcal{L}_{\mathcal{E}} \subseteq \mathcal{T}$ (Cohérence) :

- Fermeture de $\mathcal{L}_{\mathcal{E}}$.

Case $\mathcal{T} \subseteq \mathcal{L}_{\mathcal{E}}$ (Complétude) :

- Lemme : $\mathcal{F}(q)^{\alpha} \mapsto q \in \mathcal{L}_{\mathcal{E}}$.

Équivalence entre atteignabilité et terminaison

Théorème

- Si W est monotone.
- Si W est strict.
- $p \mapsto q \in \mathcal{E} \Rightarrow p \subseteq q \cup W(q)$
- si $W(q) \mapsto q \in \mathcal{L}_{\mathcal{E}}$ et
- $p \subseteq q \Rightarrow p \mapsto q \in \mathcal{E}$

alors

$$\mathcal{L}_{\mathcal{E}} = \mathcal{T}$$

Preuve

Case $\mathcal{L}_{\mathcal{E}} \subseteq \mathcal{T}$ (Cohérence) :

- Fermeture de $\mathcal{L}_{\mathcal{E}}$.

Case $\mathcal{T} \subseteq \mathcal{L}_{\mathcal{E}}$ (Complétude) :

- Lemme : $\mathcal{F}(q)^{\alpha} \mapsto q \in \mathcal{L}_{\mathcal{E}}$.

Équivalence entre atteignabilité et terminaison

Théorème

- Si W est monotone.
- Si W est strict.
- $p \mapsto q \in \mathcal{E} \Rightarrow p \subseteq q \cup W(q)$
- si $W(q) \mapsto q \in \mathcal{L}_{\mathcal{E}}$ et
- $p \subseteq q \Rightarrow p \mapsto q \in \mathcal{E}$

alors

$$\mathcal{L}_{\mathcal{E}} = \mathcal{T}$$

Preuve

Case $\mathcal{L}_{\mathcal{E}} \subseteq \mathcal{T}$ (Cohérence) :

- Fermeture de $\mathcal{L}_{\mathcal{E}}$.

Case $\mathcal{T} \subseteq \mathcal{L}_{\mathcal{E}}$ (Complétude) :

- Lemme : $\mathcal{F}(q)^{\alpha} \mapsto q \in \mathcal{L}_{\mathcal{E}}$.

Instanciación au cas de progrès minimal

Instanciation au cas de progrès minimal

- Conditions pour établir une postcondition :

1. N'importe quel événement doit l'établir
2. Au moins un événement doit être habilité

- Relation de base sous condition de progrès minimal :

$$\mathcal{E}_m \hat{=} \{ p \mapsto q \mid p \subseteq u \wedge q \subseteq u \wedge p \cap \bar{q} \subseteq S(q) \cap \text{grd}(S) \}$$

- Pas d'itération :

$$W_m \hat{=} \text{grd}(S) \mid S$$

Instanciation au cas de progrès minimal

- Conditions pour établir une postcondition :

1. N'importe quel événement doit l'établir
2. Au moins un événement doit être habilité

- Relation de base sous condition de progrès minimal :

$$\mathcal{E}_m \hat{=} \{ p \mapsto q \mid p \subseteq u \wedge q \subseteq u \wedge p \cap \bar{q} \subseteq S(q) \cap \text{grad}(S) \}$$

- Pas d'itération :

$$W_m \hat{=} \text{grad}(S) \mid S$$

Équivalence sous progrès minimal

Les définitions de W_m et \mathcal{E}_m :

- $W_m \hat{=} \text{grd}(S) \mid S,$
- $\mathcal{E}_m \hat{=} \{p \mapsto q \mid p \subseteq u \wedge q \subseteq u \wedge p \cap \bar{q} \subseteq S(q) \cap \text{grd}(S)\}$

répondent aux conditions :

- W_m est monotone et strict,
- $p \subseteq q \Rightarrow p \mapsto q \in \mathcal{E}_m,$
- $p \mapsto q \in \mathcal{E}_m \Rightarrow p \cap \bar{q} \subseteq W_m(q),$
- $W_m(q) \mapsto q \in \mathcal{L}_{\mathcal{E}_m}$

par conséquence, l'égalité $\mathcal{T}_m = \mathcal{L}_{\mathcal{E}_m}$ est vraie.

Les OP pour progrès minimal

- De la définition de \mathcal{E}_w on déduit :

$$p \cap \bar{q} \subseteq S(p \cup q) \cap \text{grd}(S) \Rightarrow p \mapsto q \in \mathcal{E}_w$$

- Sous l'hypothèse $I \Rightarrow [S] I$ on obtient :

	ANTECEDENT	CONSEQUENT
MP0	$I \wedge P \wedge \neg Q \Rightarrow [S] Q$	$P \gg_m Q$
MP1	$I \wedge P \wedge \neg Q \Rightarrow \text{grd}(S)$	

Exemple sous l'hypothèse de progrès minimal

req $\hat{=}$

ANY *p* WHERE

p \in *Idl*

THEN

st(*p*) := *WT*

END ;

ent $\hat{=}$

ANY *p* WHERE

p \in *Wtg* \wedge *pid*(*p*) = *pt*

THEN

st(*p*) := *AC*

END ;

rel $\hat{=}$

ANY *p* WHERE

p \in *Act*

THEN

st(*p*) := *ID* ||

pt := (*pt* + 1) mod card(*PR*)

END ;

req $\hat{=}$

ANY p WHERE

$p \in \text{Idl}$

THEN

$st(p) := WT$

END ;

ent $\hat{=}$

ANY p WHERE

$p \in \text{Wtg} \wedge pid(p) = pt$

THEN

$st(p) := AC$

END ;

ANY p WHERE

$$p \in Wtg \wedge pid(p) = pt$$

THEN

$$st(p) := AC$$

END ;

rel $\hat{=}$

ANY p WHERE

$$p \in Act$$

THEN

$$st(p) := ID \parallel$$

$$pt := (pt + 1) \bmod \text{card}(PR)$$

END ;

Exemple sous l'hypothèse de progrès minimal

req $\hat{=}$

ANY p WHERE

$p \in Idl$

THEN

$st(p) := WT$

END ;

ent $\hat{=}$

ANY p WHERE

$p \in Wtg \wedge pid(p) = pt$

THEN

$st(p) := AC$

END ;

rel $\hat{=}$

ANY p WHERE

$p \in Act$

THEN

$st(p) := ID \parallel$

$pt := (pt + 1) \bmod \text{card}(PR)$

END ;

- $q \in Wtg \rightsquigarrow q \in Act$
- $q \in Wtg \wedge pid(q) = pt \rightsquigarrow q \in Act, \dots$
- $q \in Wtg \wedge pid(q) = pt \ggg_m q \in Act$
- Vérification :
 - MP0 : $I \wedge q \in Wtg \wedge pid(q) = pt \Rightarrow [req \parallel rel \parallel ent] q \in Act$
 - MP1 : $I \wedge q \in Wtg \wedge pid(q) = pt \Rightarrow grd(req) \vee grd(rel) \vee grd(ent)$

Exemple sous l'hypothèse de progrès minimal

req $\hat{=}$

ANY *p* WHERE

p \in *Idl*

THEN

st(*p*) := *WT*

END ;

ent $\hat{=}$

ANY *p* WHERE

p \in *Wtg* \wedge *pid*(*p*) = *pt*

THEN

st(*p*) := *AC*

END ;

rel $\hat{=}$

ANY *p* WHERE

p \in *Act*

THEN

st(*p*) := *ID* ||

pt := (*pt* + 1) mod card(*PR*)

END ;

- $q \in \text{Wtg} \rightsquigarrow q \in \text{Act}$
- $q \in \text{Wtg} \wedge \text{pid}(q) = pt \rightsquigarrow q \in \text{Act}, \dots$
- $q \in \text{Wtg} \wedge \text{pid}(q) = pt \ggg_m q \in \text{Act}$
- Vérification :
 - MP0 : $I \wedge q \in \text{Wtg} \wedge \text{pid}(q) = pt \Rightarrow [\text{req} \parallel \text{rel} \parallel \text{ent}] q \in \text{Act}$
 - MP1 : $I \wedge q \in \text{Wtg} \wedge \text{pid}(q) = pt \Rightarrow \text{grd}(\text{req}) \vee \text{grd}(\text{rel}) \vee \text{grd}(\text{ent})$

Exemple sous l'hypothèse de progrès minimal

req $\hat{=}$

ANY *p* WHERE

p \in *Idl*

THEN

st(*p*) := *WT*

END ;

ent $\hat{=}$

ANY *p* WHERE

p \in *Wtg* \wedge *pid*(*p*) = *pt*

THEN

st(*p*) := *AC*

END ;

rel $\hat{=}$

ANY *p* WHERE

p \in *Act*

THEN

st(*p*) := *ID* ||

pt := (*pt* + 1) mod card(*PR*)

END ;

- $q \in \text{Wtg} \rightsquigarrow q \in \text{Act}$
- $q \in \text{Wtg} \wedge \text{pid}(q) = pt \rightsquigarrow q \in \text{Act}, \dots$
- $q \in \text{Wtg} \wedge \text{pid}(q) = pt \ggg_m q \in \text{Act}$
- Vérification :
 - MP0 : $I \wedge q \in \text{Wtg} \wedge \text{pid}(q) = pt \Rightarrow [\text{req} \parallel \text{rel} \parallel \text{ent}] q \in \text{Act}$
 - MP1 : $I \wedge q \in \text{Wtg} \wedge \text{pid}(q) = pt \Rightarrow \text{grd}(\text{req}) \vee \text{grd}(\text{rel}) \vee \text{grd}(\text{ent})$

Exemple sous l'hypothèse de progrès minimal

req $\hat{=}$

```

ANY p WHERE
  p ∈ Idl
THEN
  st(p) := WT
END ;

```

ent $\hat{=}$

```

ANY p WHERE
  p ∈ Wtg ∧ pid(p) = pt
THEN
  st(p) := AC
END ;

```

rel $\hat{=}$

```

ANY p WHERE
  p ∈ Act
THEN
  st(p) := ID ||
  pt := (pt + 1) mod card(PR)
END ;

```

- $q \in \text{Wtg} \rightsquigarrow q \in \text{Act}$
- $q \in \text{Wtg} \wedge \text{pid}(q) = pt \rightsquigarrow q \in \text{Act}, \dots$
- $q \in \text{Wtg} \wedge \text{pid}(q) = pt \ggg_m q \in \text{Act}$
- Vérification :
 - MP0 : $I \wedge q \in \text{Wtg} \wedge \text{pid}(q) = pt \Rightarrow [\text{req} \parallel \text{rel} \parallel \text{ent}] q \in \text{Act}$
 - MP1 : $I \wedge q \in \text{Wtg} \wedge \text{pid}(q) = pt \Rightarrow \text{grd}(\text{req}) \vee \text{grd}(\text{rel}) \vee \text{grd}(\text{ent})$

Exemple sous l'hypothèse de progrès minimal

req $\hat{=}$

ANY *p* WHERE

p \in *Idl*

THEN

st(*p*) := *WT*

END ;

ent $\hat{=}$

ANY *p* WHERE

p \in *Wtg* \wedge *pid*(*p*) = *pt*

THEN

st(*p*) := *AC*

END ;

rel $\hat{=}$

ANY *p* WHERE

p \in *Act*

THEN

st(*p*) := *ID* ||

pt := (*pt* + 1) mod card(*PR*)

END ;

- $q \in \text{Wtg} \rightsquigarrow q \in \text{Act}$
- $q \in \text{Wtg} \wedge \text{pid}(q) = pt \rightsquigarrow q \in \text{Act}, \dots$
- $q \in \text{Wtg} \wedge \text{pid}(q) = pt \ggg_m q \in \text{Act}$
- Vérification :
 - MP0 : $I \wedge q \in \text{Wtg} \wedge \text{pid}(q) = pt \Rightarrow [\text{req} \parallel \text{rel} \parallel \text{ent}] q \in \text{Act}$
 - MP1 : $I \wedge q \in \text{Wtg} \wedge \text{pid}(q) = pt \Rightarrow \text{grd}(\text{req}) \vee \text{grd}(\text{rel}) \vee \text{grd}(\text{ent})$

Instanciation au cas d'équité faible

Atteignabilité sous équité faible

- Conditions pour établir une postcondition :
 1. Un événement utile (*helpful*) doit l'établir
 2. L'événement utile doit être habilité
 3. S préserve la garde ou établit la postcondition.
- Relation de base pour un événement utile G :

$$\mathcal{E}(G) \hat{=} \{ p \mapsto q \mid p \cap \bar{q} \subseteq S(p \cup q) \cap G(q) \cap \text{grad}(G) \}$$

- Relation de base pour l'équité faible :

$$\mathcal{E}_w = \bigcup G \cdot (G \in E \mid \mathcal{E}(G))$$

Atteignabilité sous équité faible

- Conditions pour établir une postcondition :
 1. Un événement utile (*helpful*) doit l'établir
 2. L'événement utile doit être habilité
 3. S préserve la garde ou établit la postcondition.
- Relation de base pour un événement utile G :

$$\mathcal{E}(G) \hat{=} \{ p \mapsto q \mid p \cap \bar{q} \subseteq S(p \cup q) \cap G(q) \cap \text{grad}(G) \}$$

- Relation de base pour l'équité faible :

$$\mathcal{E}_w = \bigcup G \cdot (G \in E \mid \mathcal{E}(G))$$

Atteignabilité sous équité faible

- Conditions pour établir une postcondition :
 1. Un événement utile (*helpful*) doit l'établir
 2. L'événement utile doit être habilité
 3. S préserve la garde ou établit la postcondition.
- Relation de base pour un événement utile G :

$$\mathcal{E}(G) \hat{=} \{ p \mapsto q \mid p \wedge \bar{q} \subseteq S(p \cup q) \wedge G(q) \wedge \text{grad}(G) \}$$

- Relation de base pour l'équité faible :

$$\mathcal{E}_w = \bigcup G \cdot (G \in E \mid \mathcal{E}(G))$$

Terminaison sous équité faible

- L'opérateur *dovetail*

- Exemple : $X = (n := 0 \nabla (X ; n := n + 1))$

- Définition :

$$\mathcal{L}(F \nabla G)(r) = \mathcal{L}(F)(r) \cap \mathcal{L}(G)(r)$$

$$\text{pre}(F \nabla G) = (F(u) \cap G(u)) \cup (\overline{F(\emptyset)} \cap F(u)) \cup (\overline{G(\emptyset)} \cap G(u))$$

- La boucle équitable :

$$Y(q)(G) = \bar{q} \implies ((S ; Y(q)(G)) \nabla (\text{grad}(G) \mid G))$$

- Le pas équitable :

$$W_w = \lambda r \cdot (r \subseteq u \mid \bigcup G \cdot (G \in E \mid Y(r)(G)(r)))$$

Terminaison sous équité faible

- L'opérateur *dovetail*

- Exemple : $X = (n := 0 \nabla (X ; n := n + 1))$

- Définition :

$$\mathcal{L}(F \nabla G)(r) = \mathcal{L}(F)(r) \cap \mathcal{L}(G)(r)$$

$$\text{pre}(F \nabla G) = (F(u) \cap G(u)) \cup (\overline{F(\emptyset)} \cap F(u)) \cup (\overline{G(\emptyset)} \cap G(u))$$

- La boucle équitable :

$$Y(q)(G) = \bar{q} \implies ((S ; Y(q)(G)) \nabla (\text{grad}(G) \mid G))$$

- Le pas équitable :

$$W_w = \lambda r \cdot (r \subseteq u \mid \bigcup G \cdot (G \in E \mid Y(r)(G)(r)))$$

Terminaison sous équité faible

- L'opérateur *dovetail*
 - Exemple : $X = (n := 0 \nabla (X ; n := n + 1))$
 - Définition :

$$\mathcal{L}(F \nabla G)(r) = \mathcal{L}(F)(r) \cap \mathcal{L}(G)(r)$$

$$\text{pre}(F \nabla G) = (F(u) \cap G(u)) \cup (\overline{F(\emptyset)} \cap F(u)) \cup (\overline{G(\emptyset)} \cap G(u))$$

- La boucle équitable :

$$Y(q)(G) = \bar{q} \implies ((S ; Y(q)(G)) \nabla (\text{grad}(G) \mid G))$$

- Le pas équitable :

$$W_w = \lambda r \cdot (r \subseteq u \mid \bigcup G \cdot (G \in E \mid Y(r)(G)(r)))$$

Terminaison sous équité faible

- L'opérateur *dovetail*
 - Exemple : $X = (n := 0 \nabla (X ; n := n + 1))$
 - Définition :

$$\mathcal{L}(F \nabla G)(r) = \mathcal{L}(F)(r) \cap \mathcal{L}(G)(r)$$

$$\text{pre}(F \nabla G) = (F(u) \cap G(u)) \cup (\overline{F(\emptyset)} \cap F(u)) \cup (\overline{G(\emptyset)} \cap G(u))$$

- La boucle équitable :

$$Y(q)(G) = \bar{q} \implies ((S ; Y(q)(G)) \nabla (\text{grad}(G) \mid G))$$

- Le pas équitable :

$$W_w = \lambda r \cdot (r \subseteq u \mid \bigcup G \cdot (G \in E \mid Y(r)(G)(r)))$$

Terminaison sous équité faible

- L'opérateur *dovetail*

- Exemple : $X = (n := 0 \nabla (X ; n := n + 1))$

- Définition :

$$\mathcal{L}(F \nabla G)(r) = \mathcal{L}(F)(r) \cap \mathcal{L}(G)(r)$$

$$\text{pre}(F \nabla G) = (F(u) \cap G(u)) \cup (\overline{F(\emptyset)} \cap F(u)) \cup (\overline{G(\emptyset)} \cap G(u))$$

- La boucle équitable :

$$Y(q)(G) = \bar{q} \implies ((S ; Y(q)(G)) \nabla (\text{grad}(G) \mid G))$$

- Le pas équitable :

$$W_w = \lambda r \cdot (r \subseteq u \mid \bigcup G \cdot (G \in E \mid Y(r)(G)(r)))$$

Équivalence sous équité faible

Les définitions de \mathcal{E}_w et W_w :

- $\mathcal{E}_w = \bigcup G \cdot (G \in E \mid \mathcal{E}(G))$,
- $W_w = \lambda r \cdot (r \subseteq u \mid \bigcup G \cdot (G \in E \mid Y(r)(G)(r)))$

répondent aux conditions :

- W_w est monotone et strict,
- $p \subseteq q \Rightarrow p \mapsto q \in \mathcal{E}_w$,
- $p \mapsto q \in \mathcal{E}_w \Rightarrow p \cap \bar{q} \subseteq W_w(q)$,
- $W_w(q) \mapsto q \in \mathcal{L}_{\mathcal{E}_w}$

par conséquent, l'égalité $\mathcal{T}_w = \mathcal{L}_{\mathcal{E}_w}$ est vraie.

Les OP pour l'équité faible

- Pour certain G , de la définition de \mathcal{E}_w on déduit :

$$p \cap \bar{q} \subseteq S(p \cup q) \cap G(q) \cap \text{grad}(S) \Rightarrow p \mapsto q \in \mathcal{E}_w$$

- Sous l'hypothèse $I \Rightarrow [S] I$ on obtient :

	ANTECEDENT	CONSEQUENT
WF0	$I \wedge P \wedge \neg Q \Rightarrow [S] P \vee Q$	$G \cdot P \gg_w Q$
WF1	$I \wedge P \wedge \neg Q \Rightarrow \text{grad}(G) \wedge [G] Q$	

Exemple sous l'hypothèse d'équité faible

req $\hat{=}$

```

ANY p WHERE
  p ∈ Idl
THEN
  st(p) := WT
END ;

```

ent $\hat{=}$

```

ANY p WHERE
  p ∈ Wtg ∧ pid(p) = pt
THEN
  st(p) := AC
END ;

```

rel $\hat{=}$

```

ANY p WHERE
  p ∈ Act
THEN
  st(p) := ID ||
  pt := (pt + 1) mod card(PR)
END ;

```

- $q \in Wtg \rightsquigarrow q \in Act$
- $q \in Wtg \wedge pid(q) = pt \rightsquigarrow q \in Act, \dots$
- $ent \cdot q \in Wtg \wedge pid(q) = pt \ggg_m q \in Act$
- Vérification :
 - WF0 : $I \wedge q \in Wtg \wedge pid(q) = pt \Rightarrow [req \parallel rel \parallel ent] q \in Act \vee q \in Wtg \wedge pid(q) = pt$
 - WF1 : $I \wedge q \in Wtg \wedge pid(q) = pt \Rightarrow grd(ent) \wedge [ent] q \in Act$

Exemple sous l'hypothèse d'équité faible

req $\hat{=}$

ANY p WHERE

$p \in Idl$

THEN

$st(p) := WT$

END ;

ent $\hat{=}$

ANY p WHERE

$p \in Wtg \wedge pid(p) = pt$

THEN

$st(p) := AC$

END ;

rel $\hat{=}$

ANY p WHERE

$p \in Act$

THEN

$st(p) := ID \parallel$

$pt := (pt + 1) \bmod \text{card}(PR)$

END ;

- $q \in Wtg \rightsquigarrow q \in Act$
- $q \in Wtg \wedge pid(q) = pt \rightsquigarrow q \in Act, \dots$
- $ent \cdot q \in Wtg \wedge pid(q) = pt \ggg_m q \in Act$
- Vérification :
 - WF0 : $I \wedge q \in Wtg \wedge pid(q) = pt \Rightarrow [req \parallel rel \parallel ent] q \in Act \vee q \in Wtg \wedge pid(q) = pt$
 - WF1 : $I \wedge q \in Wtg \wedge pid(q) = pt \Rightarrow grd(ent) \wedge [ent] q \in Act$

Exemple sous l'hypothèse d'équité faible

req $\hat{=}$

ANY p WHERE

$p \in Idl$

THEN

$st(p) := WT$

END ;

ent $\hat{=}$

ANY p WHERE

$p \in Wtg \wedge pid(p) = pt$

THEN

$st(p) := AC$

END ;

rel $\hat{=}$

ANY p WHERE

$p \in Act$

THEN

$st(p) := ID \parallel$

$pt := (pt + 1) \bmod \text{card}(PR)$

END ;

- $q \in Wtg \rightsquigarrow q \in Act$
- $q \in Wtg \wedge pid(q) = pt \rightsquigarrow q \in Act, \dots$
- $ent \cdot q \in Wtg \wedge pid(q) = pt \ggg_m q \in Act$
- Vérification :
 - $WF0 : I \wedge q \in Wtg \wedge pid(q) = pt \Rightarrow [req \parallel rel \parallel ent] q \in Act \vee q \in Wtg \wedge pid(q) = pt$
 - $WF1 : I \wedge q \in Wtg \wedge pid(q) = pt \Rightarrow grd(ent) \wedge [ent] q \in Act$

Exemple sous l'hypothèse d'équité faible

req $\hat{=}$

ANY p WHERE

$p \in Idl$

THEN

$st(p) := WT$

END ;

ent $\hat{=}$

ANY p WHERE

$p \in Wtg \wedge pid(p) = pt$

THEN

$st(p) := AC$

END ;

rel $\hat{=}$

ANY p WHERE

$p \in Act$

THEN

$st(p) := ID \parallel$

$pt := (pt + 1) \bmod \text{card}(PR)$

END ;

- $q \in Wtg \rightsquigarrow q \in Act$
- $q \in Wtg \wedge pid(q) = pt \rightsquigarrow q \in Act, \dots$
- $ent \cdot q \in Wtg \wedge pid(q) = pt \ggg_m q \in Act$
- Vérification :
 - WF0 : $I \wedge q \in Wtg \wedge pid(q) = pt \Rightarrow [req \parallel rel \parallel ent] q \in Act \vee q \in Wtg \wedge pid(q) = pt$
 - WF1 : $I \wedge q \in Wtg \wedge pid(q) = pt \Rightarrow grd(ent) \wedge [ent] q \in Act$

Exemple sous l'hypothèse d'équité faible

req $\hat{=}$

```

ANY p WHERE
  p ∈ Idl
THEN
  st(p) := WT
END ;

```

ent $\hat{=}$

```

ANY p WHERE
  p ∈ Wtg ∧ pid(p) = pt
THEN
  st(p) := AC
END ;

```

rel $\hat{=}$

```

ANY p WHERE
  p ∈ Act
THEN
  st(p) := ID ||
  pt := (pt + 1) mod card(PR)
END ;

```

- $q \in Wtg \rightsquigarrow q \in Act$
- $q \in Wtg \wedge pid(q) = pt \rightsquigarrow q \in Act, \dots$
- $ent \cdot q \in Wtg \wedge pid(q) = pt \ggg_m q \in Act$
- Vérification :
 - WF0 : $I \wedge q \in Wtg \wedge pid(q) = pt \Rightarrow [req \parallel rel \parallel ent] q \in Act \vee q \in Wtg \wedge pid(q) = pt$
 - WF1 : $I \wedge q \in Wtg \wedge pid(q) = pt \Rightarrow grd(ent) \wedge [ent] q \in Act$

Le raffinement

Notation pour le raffinement

- Le raffinement \mathcal{T} de \mathcal{S} est composé de :
 - Un vecteur de variables d'état : y .
 - Un invariant de collage $J(x, y)$.
 - Un ensemble d'événements $E' : E' = Ec \cup Ne$.
- L'ensemble d'états du raffinement :

$$v = \{y \mid \exists x \cdot (I(x) \wedge J(x, y))\}$$

- La relation de raffinement :

$$r = \{y \mapsto x \mid I(x) \wedge J(x, y)\}$$

- Le choix des événements concrets est T .
- Le choix de nouveaux événements est H .

Préservation de la vivacité

- \mathcal{E}' relation de base dans \mathcal{T} ($\mathcal{E}' \in \mathbb{P}(V) \leftrightarrow \mathbb{P}(V)$).
- Relation d'atteignabilité dans \mathcal{T} : $\mathcal{L}_{\mathcal{E}'}$ ($\mathcal{L}_{\mathcal{E}'} \in \mathbb{P}(V) \leftrightarrow \mathbb{P}(V)$).
- β est un sous-ensemble non vide de \mathcal{E} .
- Propriétés de vivacité générées par β : \mathcal{L}_β

Théorème

Si les propriétés en β sont préservées dans \mathcal{T}

$$\forall (p, q) \cdot (p \mapsto q \in \beta \Rightarrow r^{-1}[p] \mapsto r^{-1}[q] \in \mathcal{L}_{\mathcal{E}'})$$

alors n'importe quelle propriété dans \mathcal{L}_β est préservée dans \mathcal{T}

$$\forall (p, q) \cdot (p \mapsto q \in \mathcal{L}_\beta \Rightarrow r^{-1}[p] \mapsto r^{-1}[q] \in \mathcal{L}_{\mathcal{E}'})$$

Préservation de la vivacité

- \mathcal{E}' relation de base dans \mathcal{T} ($\mathcal{E}' \in \mathbb{P}(V) \leftrightarrow \mathbb{P}(V)$).
- Relation d'atteignabilité dans \mathcal{T} : $\mathcal{L}_{\mathcal{E}'}$ ($\mathcal{L}_{\mathcal{E}'} \in \mathbb{P}(V) \leftrightarrow \mathbb{P}(V)$).
- β est un sous-ensemble non vide de \mathcal{E} .
- Propriétés de vivacité générées par β : \mathcal{L}_{β}

Théorème

Si les propriétés en β sont préservées dans \mathcal{T}

$$\forall (p, q) \cdot (p \mapsto q \in \beta \Rightarrow r^{-1}[p] \mapsto r^{-1}[q] \in \mathcal{L}_{\mathcal{E}'})$$

alors n'importe quelle propriété dans \mathcal{L}_{β} est préservée dans \mathcal{T}

$$\forall (p, q) \cdot (p \mapsto q \in \mathcal{L}_{\beta} \Rightarrow r^{-1}[p] \mapsto r^{-1}[q] \in \mathcal{L}_{\mathcal{E}'})$$

Préservation sous progrès minimal

- Règles pour préserver des propriétés de base :

- (PM1) : $\forall n \cdot (n \in W \Rightarrow w(n) \subseteq H(w'(n)))$

- (PM2) : $r^{-1}[\overline{S(\emptyset)}] \subseteq \overline{(T \parallel H)(\emptyset)}$

où

- $w = \lambda n \cdot (n \in \mathbb{N} \mid \{z \mid z \in v \wedge V(z) = n\})$

- $w' = \lambda n \cdot (n \in \mathbb{N} \mid \{z \mid z \in v \wedge V(z) < n\})$

- Preuve :

$$\frac{p \mapsto q \in \mathcal{E}_m, S \subseteq T, skip \subseteq H, (PM1), (PM2)}{r^{-1}[p] \mapsto r^{-1}[q] \in \mathcal{L}_{\mathcal{E}'}}$$

- Règles pour préserver propriétés de base :

BMP : $I \wedge J \wedge V = n \Rightarrow [H] V < n$

LMP : $I \wedge J \wedge \text{grad}(S) \Rightarrow \text{grad}(T) \vee \text{grad}(H)$

Préservation sous progrès minimal

- Règles pour préserver des propriétés de base :

- (PM1) : $\forall n \cdot (n \in W \Rightarrow w(n) \subseteq H(w'(n)))$

- (PM2) : $r^{-1}[\overline{S(\emptyset)}] \subseteq \overline{(T \parallel H)(\emptyset)}$

où

- $w = \lambda n \cdot (n \in \mathbb{N} \mid \{z \mid z \in v \wedge V(z) = n\})$

- $w' = \lambda n \cdot (n \in \mathbb{N} \mid \{z \mid z \in v \wedge V(z) < n\})$

- Preuve :

$$\frac{p \mapsto q \in \mathcal{E}_m, S \sqsubseteq T, \text{skip} \sqsubseteq H, (PM1), (PM2)}{r^{-1}[p] \mapsto r^{-1}[q] \in \mathcal{L}_{\mathcal{E}'}}$$

- Règles pour préserver propriétés de base :

BMP : $I \wedge J \wedge V = n \Rightarrow [H] V < n$

LMP : $I \wedge J \wedge \text{grad}(S) \Rightarrow \text{grad}(T) \vee \text{grad}(H)$

Préservation sous progrès minimal

- Règles pour préserver des propriétés de base :

- (PM1) : $\forall n \cdot (n \in W \Rightarrow w(n) \subseteq H(w'(n)))$

- (PM2) : $r^{-1}[\overline{S(\emptyset)}] \subseteq \overline{(T \parallel H)(\emptyset)}$

où

- $w = \lambda n \cdot (n \in \mathbb{N} \mid \{z \mid z \in v \wedge V(z) = n\})$

- $w' = \lambda n \cdot (n \in \mathbb{N} \mid \{z \mid z \in v \wedge V(z) < n\})$

- Preuve :

$$\frac{p \mapsto q \in \mathcal{E}_m, S \sqsubseteq T, \text{skip} \sqsubseteq H, (PM1), (PM2)}{r^{-1}[p] \mapsto r^{-1}[q] \in \mathcal{L}_{\mathcal{E}'}}$$

- Règles pour préserver propriétés de base :

BMP : $I \wedge J \wedge V = n \Rightarrow [H] V \prec n$

LMP : $I \wedge J \wedge \text{grd}(S) \Rightarrow \text{grd}(T) \vee \text{grd}(H)$

Exemple de préservation sous progrès minimal

req $\hat{=}$

```

ANY p WHERE
  p  $\in$   $st^{-1}[\{ID\}] \wedge ch = \emptyset$ 
THEN
   $st(p) := WT$ 
END ;

```

ent $\hat{=}$

```

ANY p WHERE
  p  $\in$   $st^{-1}[\{WT\}] \cap tk^{-1}[\{true\}]$ 
THEN
   $st(p) := AC$ 
END ;

```

rel $\hat{=}$

```

ANY p WHERE
  p  $\in$   $st^{-1}[\{AC\}]$ 
THEN
   $st(p), ch := ID, ch \leftarrow p$ 
END ;

```

srv $\hat{=}$

```

SELECT
   $ch \neq \emptyset$ 
THEN
   $ch := \emptyset \parallel tk := tk \triangleleft \{ch(1) \mapsto false,$ 
     $pid^{-1}((pid(ch(1)) + 1) \bmod card(PR))$ 
     $\mapsto true\}$ 
END ;

```

req $\hat{=}$

ANY p WHERE

$p \in st^{-1}[\{ID\}] \wedge ch = \emptyset$

THEN

$st(p) := WT$

END ;

ent $\hat{=}$

ANY p WHERE

$p \in st^{-1}[\{WT\}] \cap tk^{-1}[\{true\}]$

THEN

$st(p) := AC$

END ;

rel $\hat{=}$

ANY p WHERE

$p \in st^{-1}[\{AC\}]$

THEN

$st(p), ch := ID, ch \leftarrow p$

END ;

END ;

rel $\hat{=}$

ANY p WHERE

$p \in st^{-1}[\{AC\}]$

THEN

$st(p), ch := ID, ch \leftarrow p$

END ;

srv $\hat{=}$

SELECT

$ch \neq \emptyset$

THEN

$ch := \emptyset \parallel tk := tk \Leftarrow \{ch(1) \mapsto false,$

$pid^{-1}((pid(ch(1)) + 1) \bmod \text{card}(PR))$
 $\mapsto true\}$

END ;

Exemple de préservation sous progrès minimal

```

req ≐
  ANY p WHERE
    p ∈ st-1 [{ID}] ∧ ch = ∅
  THEN
    st(p) := WT
  END ;
ent ≐
  ANY p WHERE
    p ∈ st-1 [{WT}] ∩ tk-1 [{true}]
  THEN
    st(p) := AC
  END ;
rel ≐
  ANY p WHERE
    p ∈ st-1 [{AC}]
  THEN
    st(p), ch := ID, ch ← p
  END ;
srv ≐
  SELECT
    ch ≠ ∅
  THEN
    ch := ∅ ∥ tk := tk ⇐ {ch(1) ↦ false,
      pid-1((pid(ch(1)) + 1) mod card(PR))
      ↦ true}
  END ;

```

- Preuve de BMP :

$$\text{card}(ch) = n \Rightarrow [srv] \text{card}(ch) < n$$

- Preuve de LMP :

$$\begin{aligned}
 \text{grd}(req \parallel ent \parallel rel) \Rightarrow \\
 \text{grd}(req_c) \vee \text{grd}(act_c) \\
 \vee \text{grd}(rel_c) \vee \text{grd}(srv)
 \end{aligned}$$

- $q \in Wtg \rightsquigarrow q \in Act$ est préservée.

Exemple de préservation sous progrès minimal

```

req ≐
  ANY p WHERE
    p ∈ st-1 [{ID}] ∧ ch = ∅
  THEN
    st(p) := WT
  END ;
ent ≐
  ANY p WHERE
    p ∈ st-1 [{WT}] ∩ tk-1 [{true}]
  THEN
    st(p) := AC
  END ;
rel ≐
  ANY p WHERE
    p ∈ st-1 [{AC}]
  THEN
    st(p), ch := ID, ch ← p
  END ;
srv ≐
  SELECT
    ch ≠ ∅
  THEN
    ch := ∅ ∥ tk := tk ⇐ {ch(1) ↦ false,
      pid-1((pid(ch(1)) + 1) mod card(PR))
      ↦ true}
  END ;

```

- Preuve de BMP :

$$\text{card}(ch) = n \Rightarrow [srv] \text{card}(ch) < n$$

- Preuve de LMP :

$$\begin{aligned}
 \text{grd}(req \parallel ent \parallel rel) \Rightarrow \\
 \text{grd}(req_c) \vee \text{grd}(act_c) \\
 \vee \text{grd}(rel_c) \vee \text{grd}(srv)
 \end{aligned}$$

- $q \in Wtg \rightsquigarrow q \in Act$ est préservée.

Exemple de préservation sous progrès minimal

```

req ≐
  ANY p WHERE
    p ∈ st-1[\{ID\}] ∧ ch = ∅
  THEN
    st(p) := WT
  END ;
ent ≐
  ANY p WHERE
    p ∈ st-1[\{WT\}] ∩ tk-1[\{true\}]
  THEN
    st(p) := AC
  END ;
rel ≐
  ANY p WHERE
    p ∈ st-1[\{AC\}]
  THEN
    st(p), ch := ID, ch ← p
  END ;
srv ≐
  SELECT
    ch ≠ ∅
  THEN
    ch := ∅ ∥ tk := tk ⇐ {ch(1) ↦ false,
      pid-1((pid(ch(1)) + 1) mod card(PR))
      ↦ true}
  END ;

```

- Preuve de BMP :

$$\text{card}(ch) = n \Rightarrow [srv] \text{card}(ch) < n$$

- Preuve de LMP :

$$\begin{aligned}
 \text{grd}(req \parallel ent \parallel rel) \Rightarrow \\
 \text{grd}(req_c) \vee \text{grd}(act_c) \\
 \vee \text{grd}(rel_c) \vee \text{grd}(srv)
 \end{aligned}$$

- $q \in Wtg \rightsquigarrow q \in Act$ est préservée.

Exemple de préservation sous progrès minimal

```

req ≐
  ANY p WHERE
    p ∈ st-1 [{ID}] ∧ ch = ∅
  THEN
    st(p) := WT
  END ;
ent ≐
  ANY p WHERE
    p ∈ st-1 [{WT}] ∩ tk-1 [{true}]
  THEN
    st(p) := AC
  END ;
rel ≐
  ANY p WHERE
    p ∈ st-1 [{AC}]
  THEN
    st(p), ch := ID, ch ← p
  END ;
srv ≐
  SELECT
    ch ≠ ∅
  THEN
    ch := ∅ ∥ tk := tk ⇐ {ch(1) ↦ false,
      pid-1((pid(ch(1)) + 1) mod card(PR))
      ↦ true}
  END ;

```

- Preuve de BMP :

$$\text{card}(ch) = n \Rightarrow [srv] \text{card}(ch) < n$$

- Preuve de LMP :

$$\begin{aligned}
 \text{grd}(req \parallel ent \parallel rel) \Rightarrow \\
 \text{grd}(req_c) \vee \text{grd}(act_c) \\
 \vee \text{grd}(rel_c) \vee \text{grd}(srv)
 \end{aligned}$$

- $q \in Wtg \rightsquigarrow q \in Act$ est préservée.

Préservation sous équité faible

- Règles pour préserver $G \cdot x \in p \gg_w x \in q$
 - (PW1) : $r^{-1}[p \cap \bar{q}] \cap \text{grd}(G') \subseteq (F' \parallel H)(\text{grd}(G'))$
 - (PW2) : $r^{-1}[p \cap \bar{q}] \cap \overline{\text{grd}(G')} \mapsto \text{grd}(G') \in \mathcal{L}_{\mathcal{E}'_w}$
- Preuve :

$$\frac{p \mapsto q \in \mathcal{E}(G), S \sqsubseteq T, \text{skip} \sqsubseteq H, (PW1), (PW2)}{r^{-1}[p] \mapsto r^{-1}[q] \in \mathcal{L}_{\mathcal{E}'_w}}$$

- Règles sous la forme de prédicats :

$$\text{SAP} : I \wedge J \wedge P \wedge \neg Q \wedge \text{grd}(G') \Rightarrow [F' \parallel H] \text{grd}(G')$$

$$\text{LIP} : I \wedge J \wedge P \wedge \neg Q \wedge \neg \text{grd}(G') \rightsquigarrow \text{grd}(G')$$

Préservation sous équité faible

- Règles pour préserver $G \cdot x \in p \gg_w x \in q$
 - (PW1) : $r^{-1}[p \cap \bar{q}] \cap \text{grd}(G') \subseteq (F' \parallel H)(\text{grd}(G'))$
 - (PW2) : $r^{-1}[p \cap \bar{q}] \cap \overline{\text{grd}(G')} \mapsto \text{grd}(G') \in \mathcal{L}_{\mathcal{E}'_w}$
- Preuve :

$$\frac{p \mapsto q \in \mathcal{E}(G), S \sqsubseteq T, \text{skip} \sqsubseteq H, (PW1), (PW2)}{r^{-1}[p] \mapsto r^{-1}[q] \in \mathcal{L}_{\mathcal{E}'_w}}$$

- Règles sous la forme de prédicats :

$$\text{SAP} : I \wedge J \wedge P \wedge \neg Q \wedge \text{grd}(G') \Rightarrow [F' \parallel H] \text{grd}(G')$$

$$\text{LIP} : I \wedge J \wedge P \wedge \neg Q \wedge \neg \text{grd}(G') \rightsquigarrow \text{grd}(G')$$

Préservation sous équité faible

- Règles pour préserver $G \cdot x \in p \gg_w x \in q$
 - (PW1) : $r^{-1}[p \cap \bar{q}] \cap \text{grd}(G') \subseteq (F' \parallel H)(\text{grd}(G'))$
 - (PW2) : $r^{-1}[p \cap \bar{q}] \cap \overline{\text{grd}(G')} \mapsto \text{grd}(G') \in \mathcal{L}_{\mathcal{E}'_w}$

- Preuve :

$$\frac{p \mapsto q \in \mathcal{E}(G), S \sqsubseteq T, \text{skip} \sqsubseteq H, (PW1), (PW2)}{r^{-1}[p] \mapsto r^{-1}[q] \in \mathcal{L}_{\mathcal{E}'_w}}$$

- Règles sous la forme de prédicats :

$$\text{SAP} : I \wedge J \wedge P \wedge \neg Q \wedge \text{grd}(G') \Rightarrow [F' \parallel H] \text{grd}(G')$$

$$\text{LIP} : I \wedge J \wedge P \wedge \neg Q \wedge \neg \text{grd}(G') \rightsquigarrow \text{grd}(G')$$

Exemple de préservation sous équité faible

req $\hat{=}$

```

ANY p WHERE
  p  $\in$   $st^{-1}[\{ID\}] \wedge ch = \emptyset$ 
THEN
  st(p) := WT
END ;

```

ent $\hat{=}$

```

ANY p WHERE
  p  $\in$   $st^{-1}[\{WT\}] \cap tk^{-1}[\{true\}]$ 
THEN
  st(p) := AC
END ;

```

rel $\hat{=}$

```

ANY p WHERE
  p  $\in$   $st^{-1}[\{AC\}]$ 
THEN
  st(p), ch := ID, ch  $\leftarrow$  p
END ;

```

srv $\hat{=}$

```

SELECT
  ch  $\neq$   $\emptyset$ 
THEN
  ch :=  $\emptyset$  || tk := tk  $\Leftarrow$  {ch(1)  $\mapsto$  false,
    pid-1((pid(ch(1)) + 1) mod card(PR))
     $\mapsto$  true}
END ;

```

Exemple de préservation sous équité faible

req $\hat{=}$

```
ANY p WHERE
  p  $\in$   $st^{-1}[\{ID\}] \wedge ch = \emptyset$ 
THEN
   $st(p) := WT$ 
END ;
```

ent $\hat{=}$

```
ANY p WHERE
  p  $\in$   $st^{-1}[\{WT\}] \cap tk^{-1}[\{true\}]$ 
THEN
   $st(p) := AC$ 
END ;
```

rel $\hat{=}$

```
ANY p WHERE
  p  $\in$   $st^{-1}[\{AC\}]$ 
THEN
   $st(p), ch := ID, ch \leftarrow p$ 
END ;
```

srv $\hat{=}$

```
SELECT
   $ch \neq \emptyset$ 
THEN
   $ch := \emptyset \parallel tk := tk \Leftarrow \{ch(1) \mapsto false,$   

 $pid^{-1}((pid(ch(1)) + 1) \bmod \text{card}(PR))$   

 $\mapsto true\}$ 
END ;
```

- Le système abstrait satisfait :

$$ent \cdot q \in Wtg \wedge pid(q) = pt \gg_w q \in Act$$

- La préservation est garanti par :

$$q \in Wtg \wedge pid(q) = pt \wedge grd(ent) \Rightarrow [req \parallel rel \parallel srv] grd(ent)$$

$$q \in Wtg \wedge pid(q) = pt \wedge \neg grd(ent) \rightsquigarrow grd(ent)$$

Exemple de préservation sous équité faible

req $\hat{=}$

```
ANY p WHERE
  p ∈ st-1 [{ID}] ∧ ch = ∅
THEN
  st(p) := WT
END ;
```

ent $\hat{=}$

```
ANY p WHERE
  p ∈ st-1 [{WT}] ∩ tk-1 [{true}]
THEN
  st(p) := AC
END ;
```

rel $\hat{=}$

```
ANY p WHERE
  p ∈ st-1 [{AC}]
THEN
  st(p), ch := ID, ch ← p
END ;
```

srv $\hat{=}$

```
SELECT
  ch ≠ ∅
THEN
  ch := ∅ || tk := tk ⇐ {ch(1) ↦ false,
  pid-1 ((pid(ch(1)) + 1) mod card(PR))
  ↦ true}
END ;
```

- Le système abstrait satisfait :

$$ent \cdot q \in Wtg \wedge pid(q) = pt \gg_w q \in Act$$

- La préservation est garanti par :

$$q \in Wtg \wedge pid(q) = pt \wedge grd(ent) \Rightarrow [req \parallel rel \parallel srv] grd(ent)$$

$$q \in Wtg \wedge pid(q) = pt \wedge \neg grd(ent) \rightsquigarrow grd(ent)$$

Exemple de préservation sous équité faible

req $\hat{=}$

```

ANY p WHERE
  p  $\in$   $st^{-1}[\{ID\}] \wedge ch = \emptyset$ 
THEN
  st(p) := WT
END ;

```

ent $\hat{=}$

```

ANY p WHERE
  p  $\in$   $st^{-1}[\{WT\}] \cap tk^{-1}[\{true\}]$ 
THEN
  st(p) := AC
END ;

```

rel $\hat{=}$

```

ANY p WHERE
  p  $\in$   $st^{-1}[\{AC\}]$ 
THEN
  st(p), ch := ID, ch  $\leftarrow$  p
END ;

```

srv $\hat{=}$

```

SELECT
  ch  $\neq$   $\emptyset$ 
THEN
  ch :=  $\emptyset \parallel tk := tk \Leftarrow \{ch(1) \mapsto false,$ 
    pid $^{-1}((pid(ch(1)) + 1) \bmod \text{card}(PR))$ 
     $\mapsto true\}$ 
END ;

```

- Le système abstrait satisfait :

$$ent \cdot q \in Wtg \wedge pid(q) = pt \gg_w q \in Act$$

- La préservation est garanti par :

$$q \in Wtg \wedge pid(q) = pt \wedge grd(ent) \Rightarrow [req \parallel rel \parallel srv] grd(ent)$$

$$q \in Wtg \wedge pid(q) = pt \wedge \neg grd(ent) \rightsquigarrow grd(ent)$$

Conclusions et travail future

Conclusions

- Une approche à la spécification, preuve et raffinement de propriétés de vivacité.
- L'approche est justifiée dans un cadre formel.
- L'approche est illustrée par des exemples.
- Le document contient :
 - Sémantique avec le plus fort invariant.
 - Comparaison avec le style de preuves de B.
 - Une règle pour vérifier le passage de WF à MP.
- Vérification de preuves :
 - Invariants et propriétés de base.
 - Certains preuves au niveau meta.

Conclusions

- Une approche à la spécification, preuve et raffinement de propriétés de vivacité.
- L'approche est justifiée dans un cadre formel.
- L'approche est illustrée par des exemples.
- Le document contient :
 - Sémantique avec le plus fort invariant.
 - Comparaison avec le style de preuves de B.
 - Une règle pour vérifier le passage de WF à MP.
- Vérification de preuves :
 - Invariants et propriétés de base.
 - Certains preuves au niveau meta.

Conclusions

- Une approche à la spécification, preuve et raffinement de propriétés de vivacité.
- L'approche est justifiée dans un cadre formel.
- L'approche est illustrée par des exemples.
- Le document contient :
 - Sémantique avec le plus fort invariant.
 - Comparaison avec le style de preuves de B.
 - Une règle pour vérifier le passage de WF à MP.
- Vérification de preuves :
 - Invariants et propriétés de base.
 - Certains preuves au niveau meta.

Conclusions

- Une approche à la spécification, preuve et raffinement de propriétés de vivacité.
- L'approche est justifiée dans un cadre formel.
- L'approche est illustrée par des exemples.
- Le document contient :
 - Sémantique avec le plus fort invariant.
 - Comparaison avec le style de preuves de B.
 - Une règle pour vérifier le passage de WF à MP.
- Vérification de preuves :
 - Invariants et propriétés de base.
 - Certains preuves au niveau meta.

Conclusions

- Une approche à la spécification, preuve et raffinement de propriétés de vivacité.
- L'approche est justifiée dans un cadre formel.
- L'approche est illustrée par des exemples.
- Le document contient :
 - Sémantique avec le plus fort invariant.
 - Comparaison avec le style de preuves de B.
 - Une règle pour vérifier le passage de WF à MP.
- Vérification de preuves :
 - Invariants et propriétés de base.
 - Certains preuves au niveau meta.

Publications



H. Ruíz-Barradas and D. Bert.

Proof Obligations for Specification and Refinement of Liveness Properties under Weak Fairness.

Technical Report 1071-I LSR 20, LSR-IMAG, Grenoble, 2005.



H. Ruíz-Barradas and D. Bert.

A Fixpoint Semantics of Event Systems with and without Fairness Assumptions.

Technical Report 1081-I LSR 21, LSR-IMAG, Grenoble, 2005.



H. Ruíz-Barradas and D. Bert.

Specification and Proof of Liveness Properties under Fairness Assumptions in B Event Systems.

In Integrated Formal Methods, Third International Conference IFM 2002, LNCS 2335, pages 360–379.
Springer-Verlag, May 2002.

Publications (cont.)



Héctor Ruíz-Barradas and Didier Bert.

A Fixpoint Semantics of Event Systems with and without Fairness Assumptions.

In Fifth International Conference on Integrated Formal Methods IFM 2005, LNCS 3771. Springer-Verlag, 2005.



H. Ruíz-Barradas and D. Bert.

Propriétés dynamiques avec hypothèses d'équité en B événementiel.

Technique et science informatique, RSTI, série TSI, 25(1) :73–102, 2006.



D. Bert and H. Ruíz-Barradas.

Développement et preuve de vivacité de l'algorithme distribué de Ricart-Agrawala.

In Actes de la Conférence AFADL'06 : Approches Formelles dans l'Assistance au Développement de Logiciels, pages 161–178. ENST, Paris, France, 2006.

Travail futur

- Inclusion de l'équité forte.
- Améliorer l'étude du passage de WF à MP.
- Etude sur la distribution.