Modélisation formelle d'exigences et logiques temporelles multi-agents

Soutenance de thèse

20 juin 2014

Christophe Chareton

Jury	Régine Laleau	rapporteur
	Nicolas Markey	rapporteur
	Julien Brunel	co-encadrant
	David Chemouil	co-encadrant
	Sophie Pinchinat	examinateur
	Jean-Paul Bodeveix	examinateur
Directrice	Laurence Cholvy	

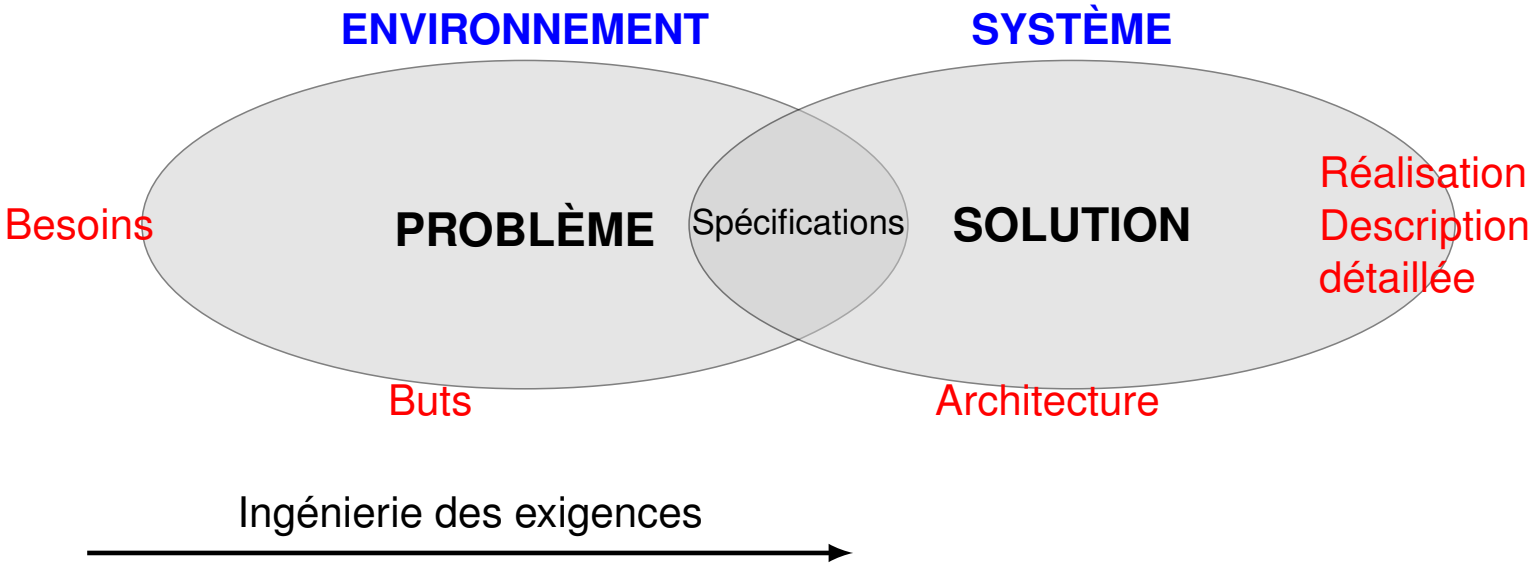
ONERA
THE FRENCH AEROSPACE LAB

ISAE
Institut Supérieur de l'Aéronautique et de l'Espace

Plan

Plan

Ingénierie des exigences



- Objectifs pour l'ingénierie des exigences :
  1. identifier les exigences
  2. dériver des spécifications à partir des exigences fonctionnelles

Principaux concepts utilisés

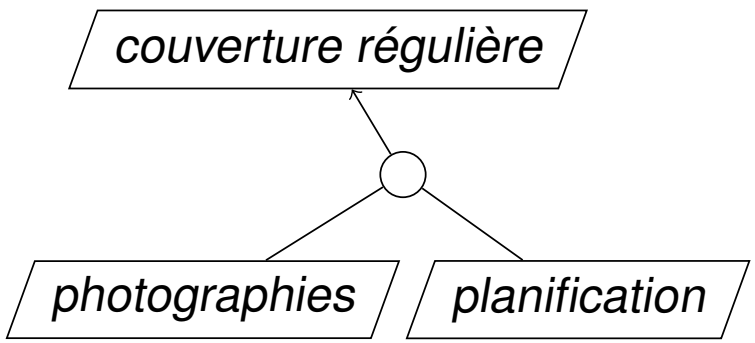
- Nous nous concentrons sur les langages de modélisation
  - buts et opérations (KAOS [vL09, vL03, LvL02])
  - rôles, acteurs et assignation (TROPOS-i^* [CDGM10, CS09, MS06])

Décomposition des buts (KAOS [vL09, vL03, LvL02])

Définition (But)

Un but est un énoncé qui décrit le comportement attendu du système.

Modèle de buts pour la mission satellites



but : formule de LTL

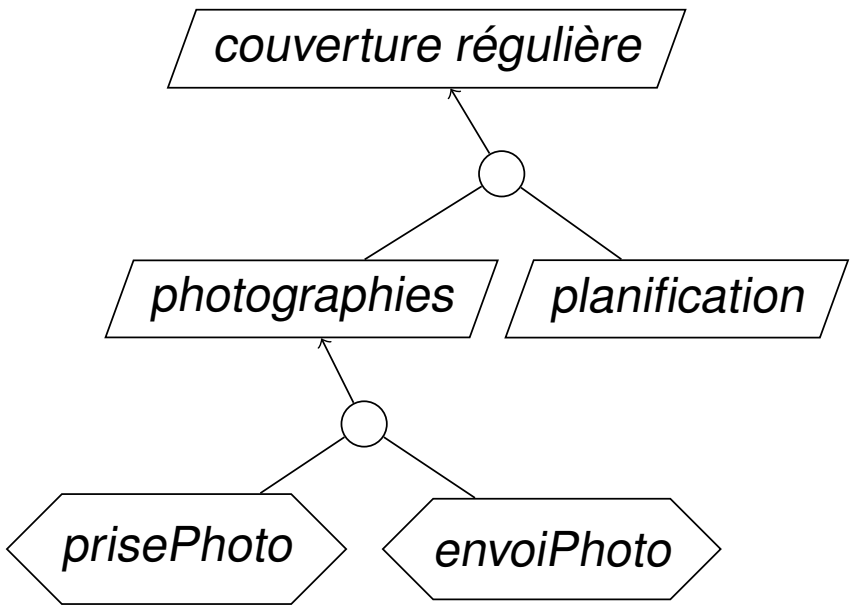
raffine : implication logique

Opérationalisation (KAOS [vL09, vL03, LvL02])

Définition (Opération)

Une opération est une spécification de transitions du système.

Opérations pour le but *prisePhoto*



but : formule de LTL

raffine : implication logique

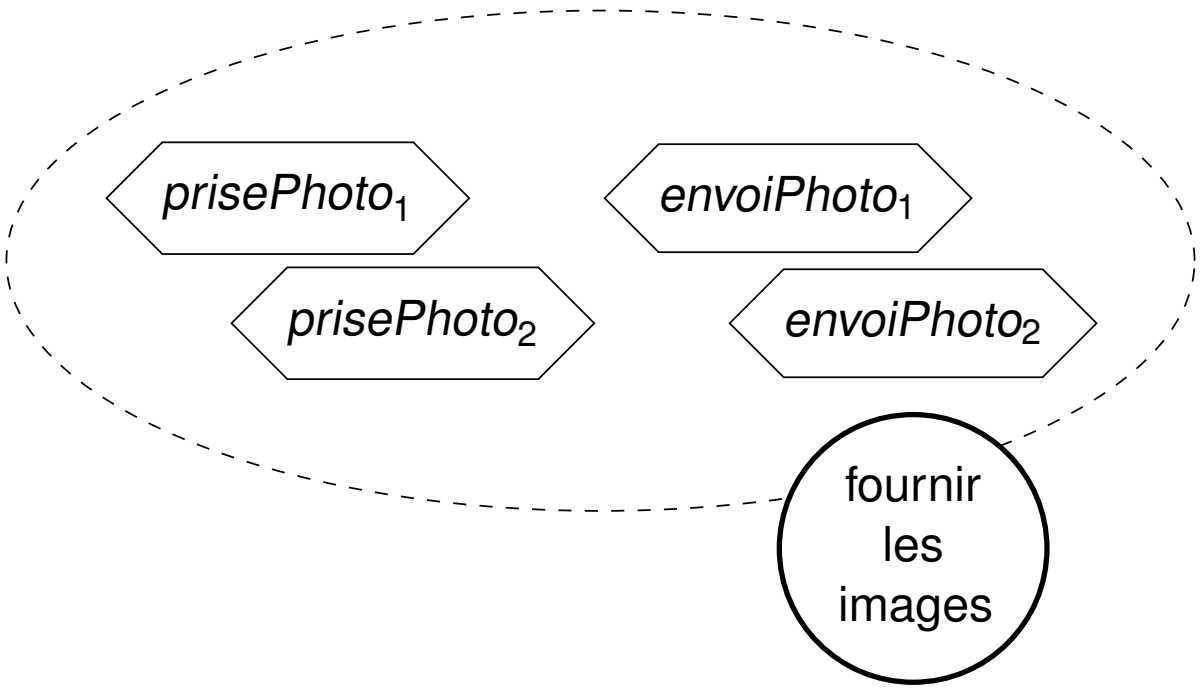
réalise : implication logique

opération : pre, post, traduites en LTL

Rôles (Tropos-i^* [CDGM10, CS09, MS06])

Définition (Rôle)

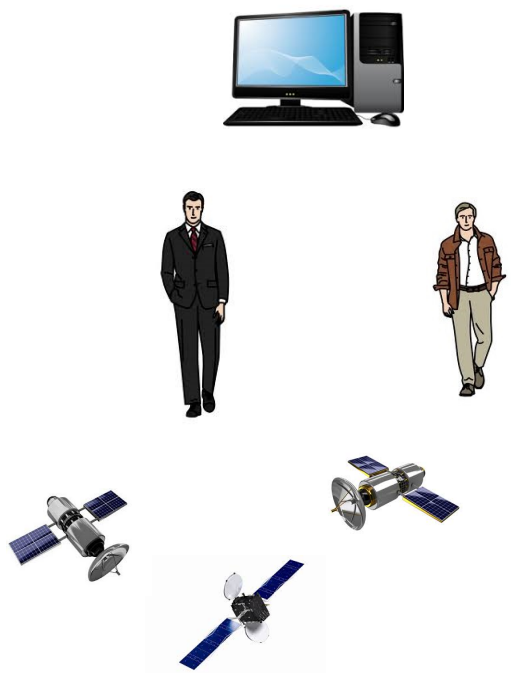
Un rôle est un regroupement d'opérations.



Acteurs (Tropos-i^* [CDGM10, CS09, MS06])

Définition (Acteur)

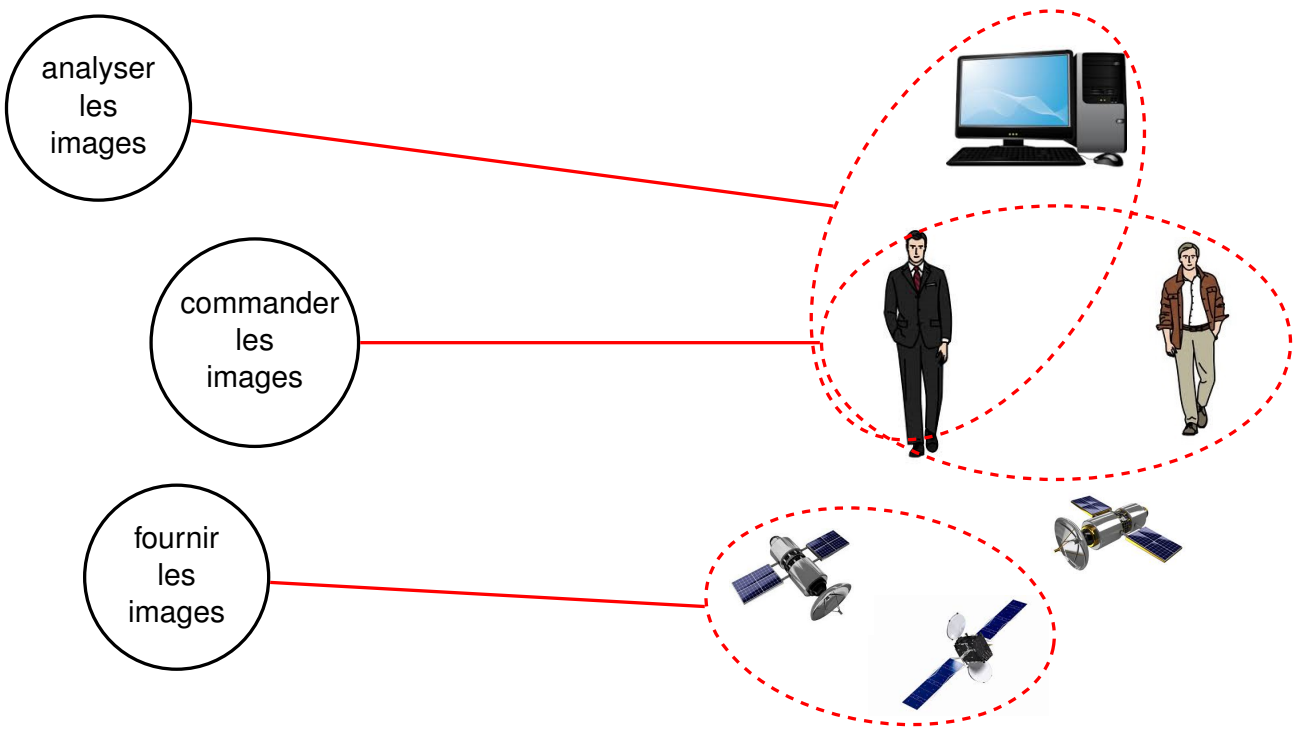
Un acteur est une entité qui agit au sein du système. Il est décrit par des capacités d'actions.



Assignation

Définition (Assignation)

Une assignation est une affectation de chacun des rôles à une coalition (un ensemble) d'acteurs.



Problème de l'assignation : les rôles sont-ils assignés à des coalitions d'acteurs capables de les remplir ?

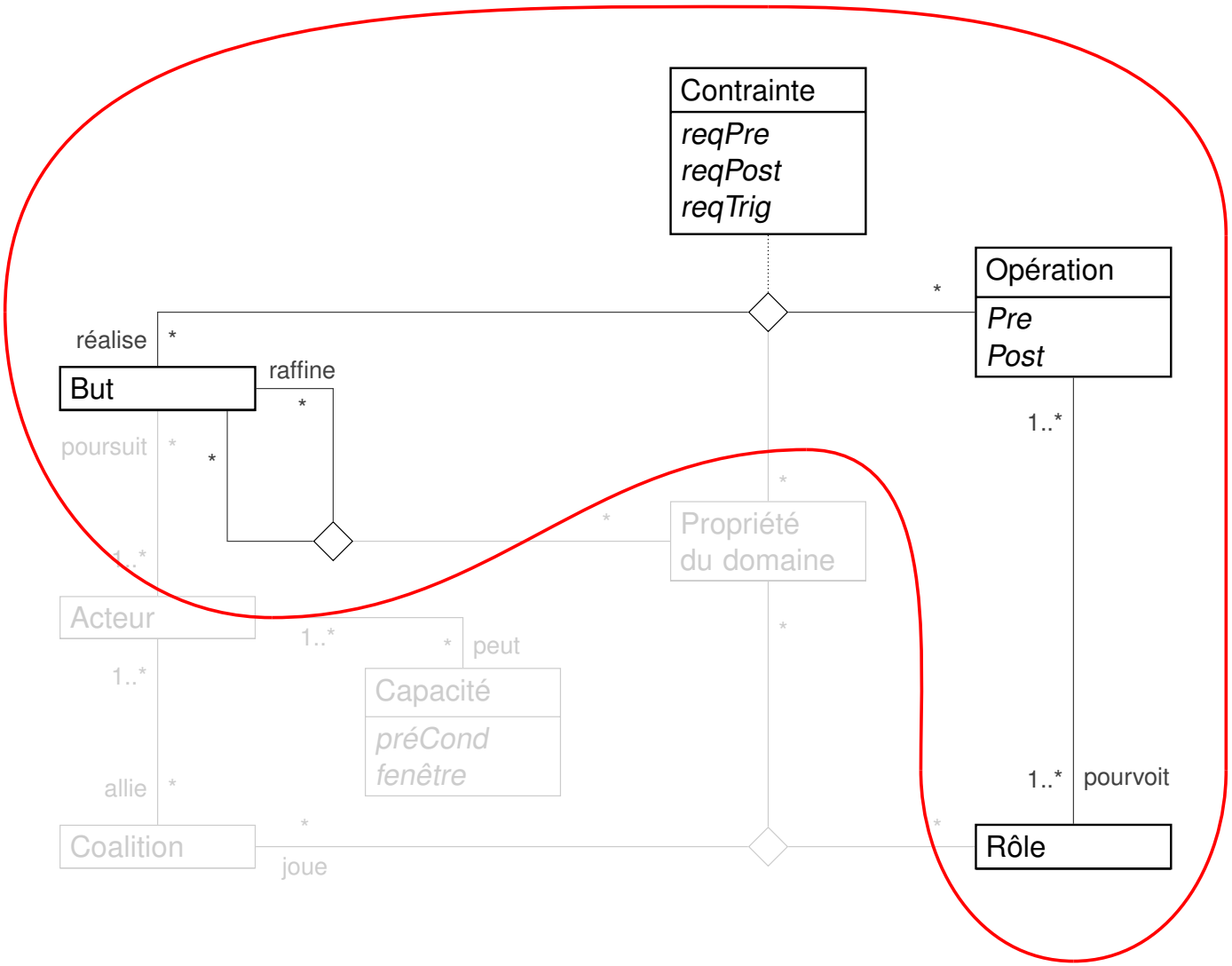
Contribution

- Un langage de modélisation (Khi [Cha 11, Cha 12]) qui réunit :
  - la description des buts dynamiques et des opérations
  - la relation d'assignation entre les rôles issus des spécifications et les acteurs
- Une logique temporelle multi-agents (USL [Cha 13, Cha 14])
- Une méthode pour :
  - traduire toute instance de Khi en un modèle et un ensemble de formules de USL
  - réduire le problème de l'assignation à une question de *model-checking* pour USL

Plan

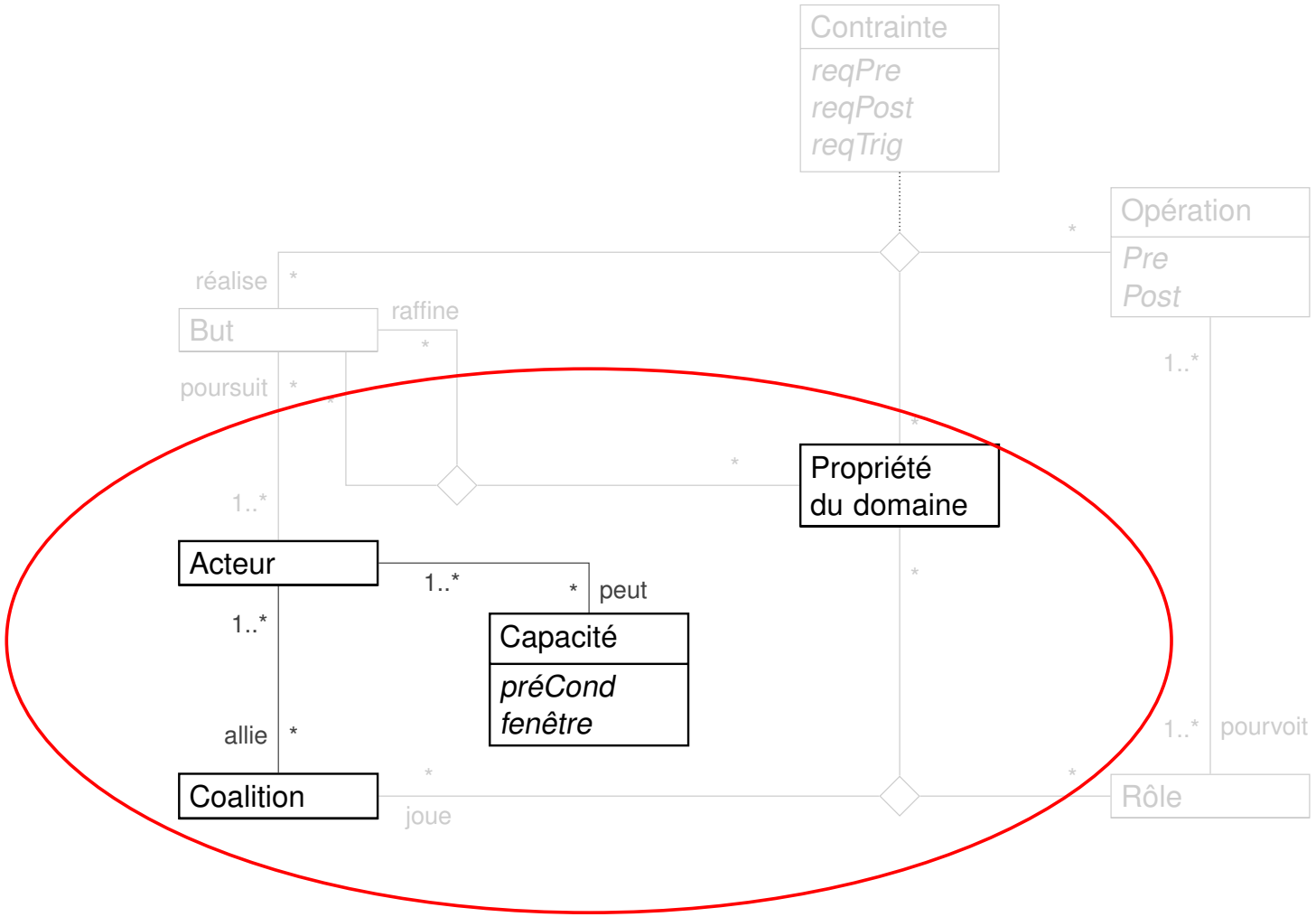
Metamodèle (1/2)

Les exigences :

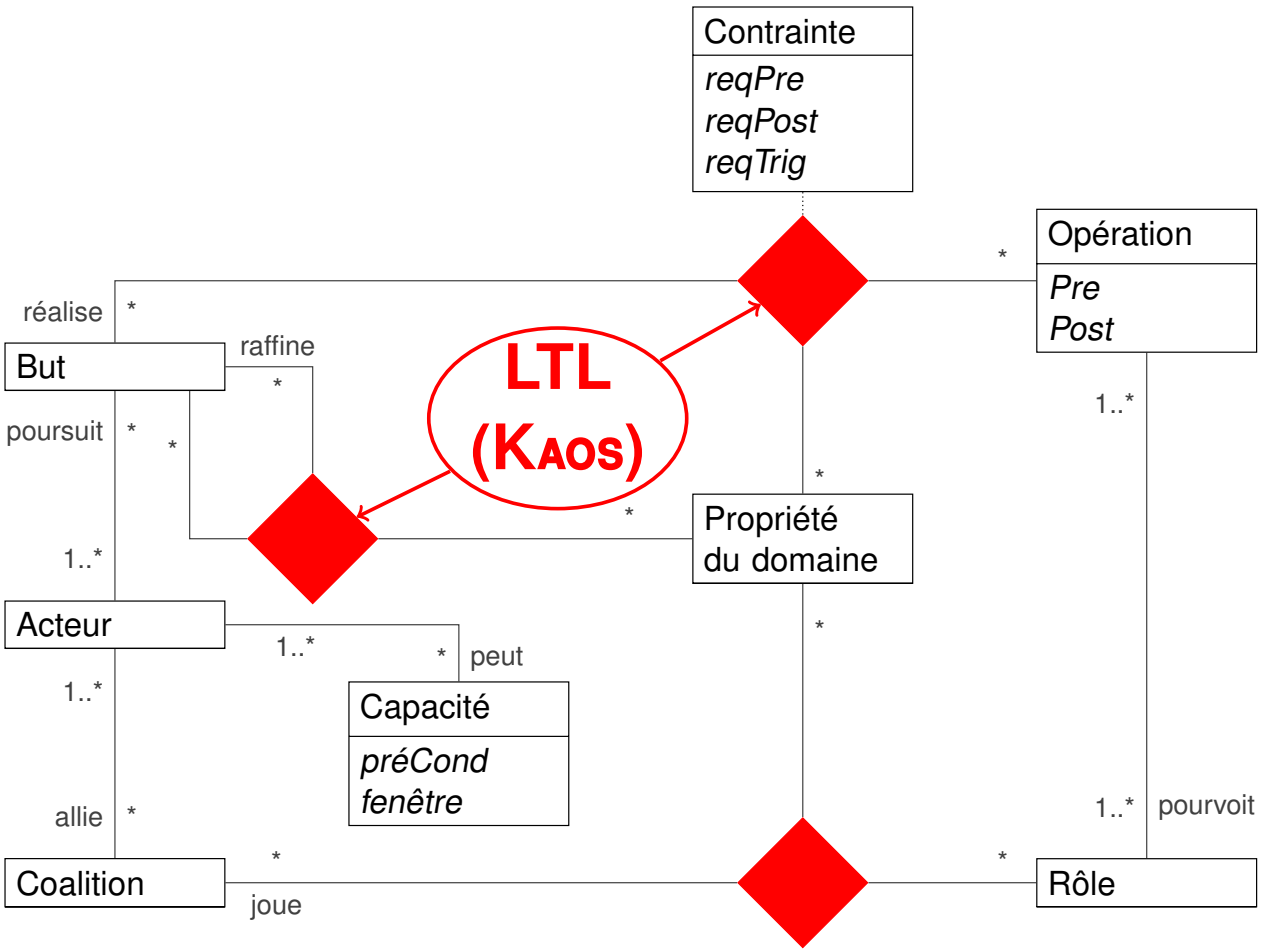


Metamodèle (2/2)

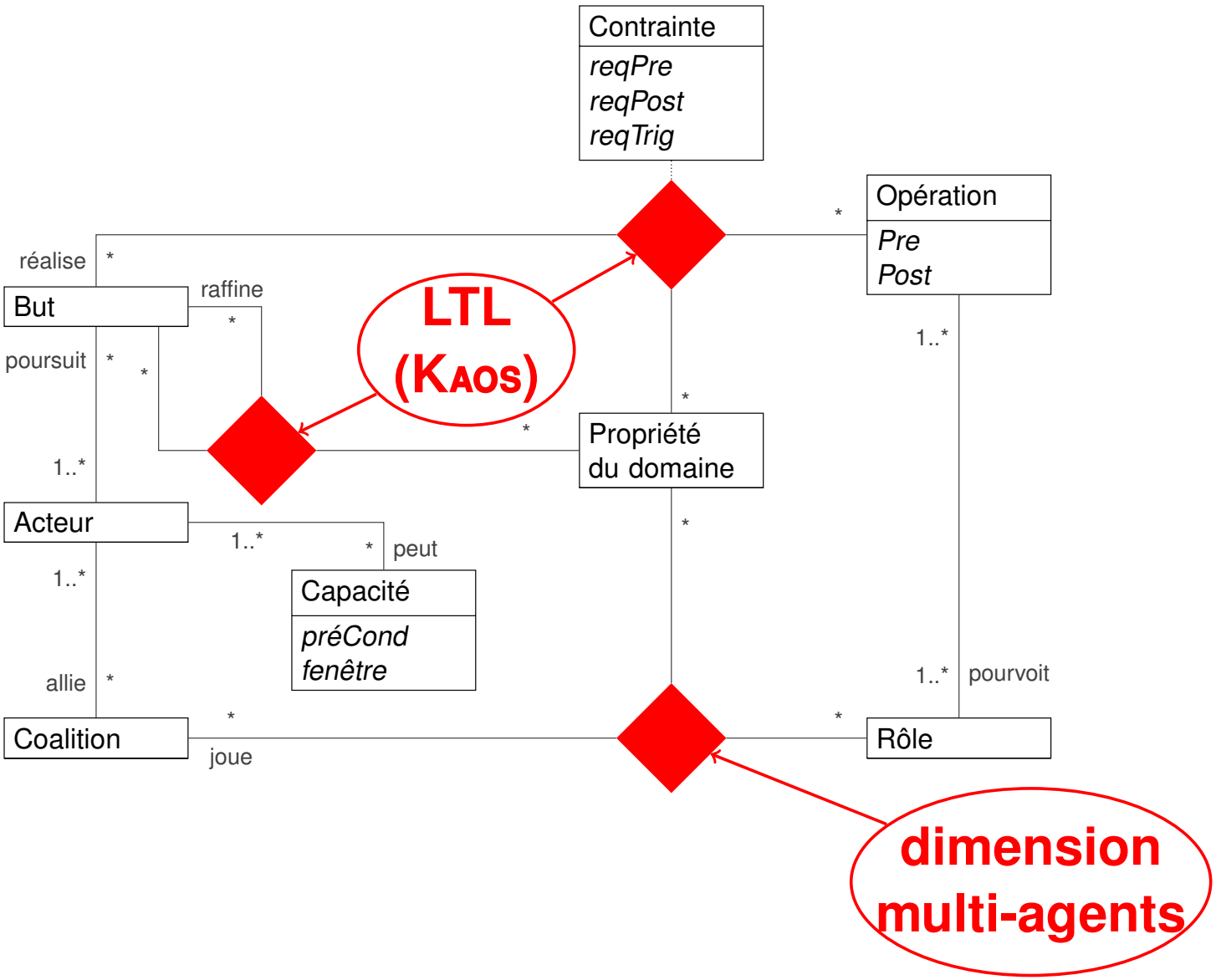
Les moyens :



Vérifications : le raffinement et la réalisation



Vérifications : l'assignation



Correction de l'assignation

- Définition d'un certain nombre de *critères* pour la correction de l'assignation
  - Ex (correction locale) : chaque rôle est assigné à une coalition capable de le remplir
- Objectif : formaliser et vérifier la satisfaction de ces critères
- Besoin d'une logique temporelle multi-agents

Plan

Modèles pour interpréter USL : les CGSs [AHK97]

Modèles utilisés pour interpréter les logiques temporelles multi-agents : ATL [AHK97], ATL_{sc} [DCL11, BDCLLM09], SL [MMPV11, MMV10], ...

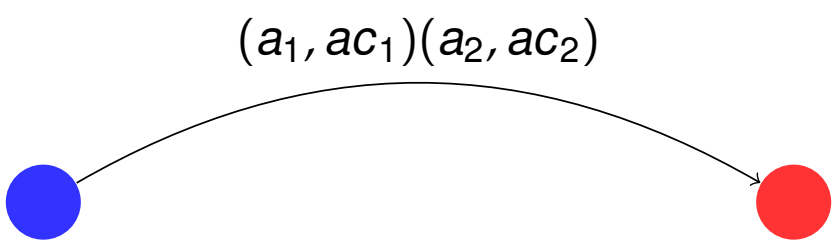
Définition (CGSs (Concurrent Game Structures))

un ensemble d'états labellisés — $\{$  ,  $\}$

un ensemble d'agents — $\{a_1, a_2\}$

un ensemble d'actions — $\{ac_1, ac_2\}$

une fonction de transition — *Couleur inchangée ssi même action jouée*

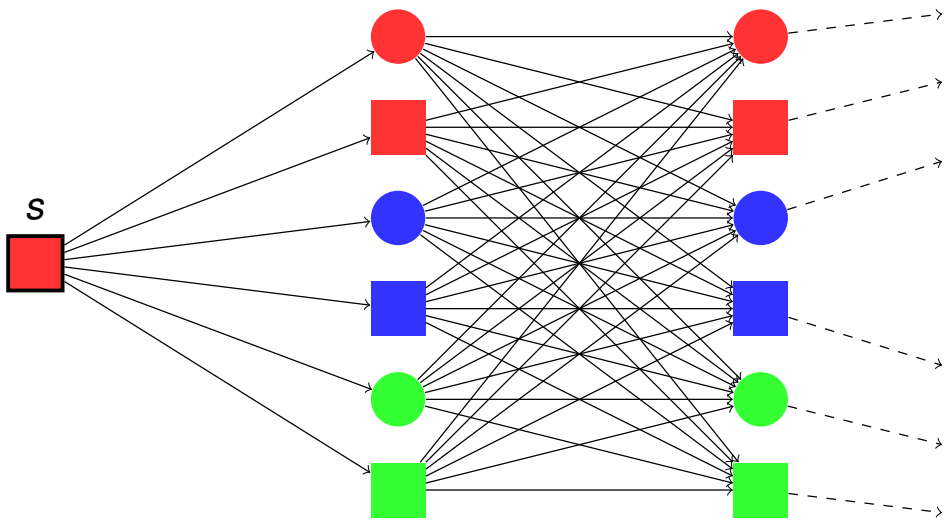


Multi-stratégies

Définition (Multi-stratégie)

Une multi-stratégie est une fonction qui indique les actions potentielles pour un agent en fonction des états visités.

Originalité : le non-déterminisme



La CGS $\mathcal{G}_1$

L'agent *couleur* décide pour la couleur, l'agent *forme* décide pour la forme

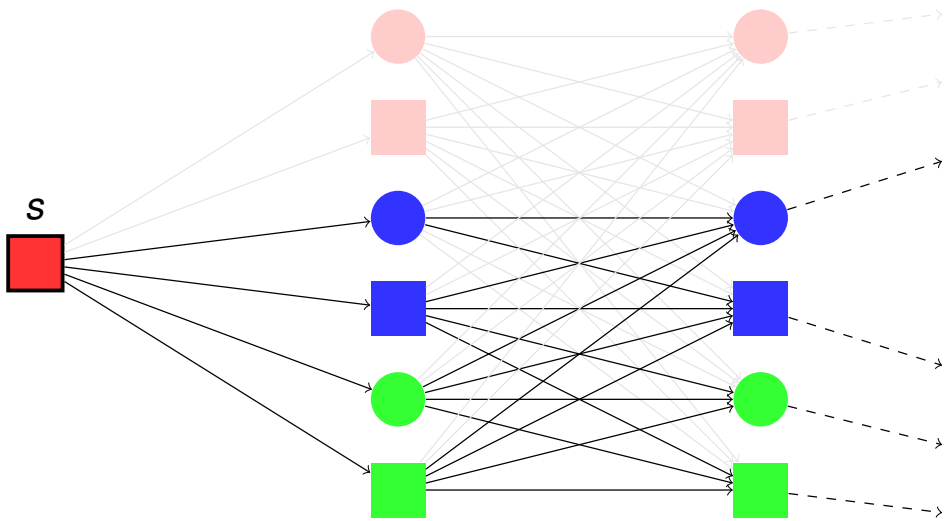
Multi-stratégies

Définition (Multi-stratégie)

Une multi-stratégie est une fonction qui indique les actions potentielles pour un agent en fonction des états visités.

Originalité : le non-déterminisme

- Exemple : *couleur* joue toujours *bleu* ou *vert*



La CGS $\mathcal{G}_1$

L'agent *couleur* décide pour la couleur, l'agent *forme* décide pour la forme

USL : syntaxe

Exprimer, grâce aux multi-stratégies, les capacités d'agents à satisfaire des propriétés temporelles

Définition (Formules d'USL)

L'ensemble des formules d'USL est généré par la grammaire suivante :

- *Formules d'états :*

Il existe une multi-stratégie x t.q...

si les agents dans A jouent x alors ...

$$\varphi := p \mid \neg\varphi \mid \varphi \wedge \varphi \mid \langle\langle x \rangle\rangle \varphi \mid (A \triangleright x)\psi \mid (A \not\triangleright x)\psi$$

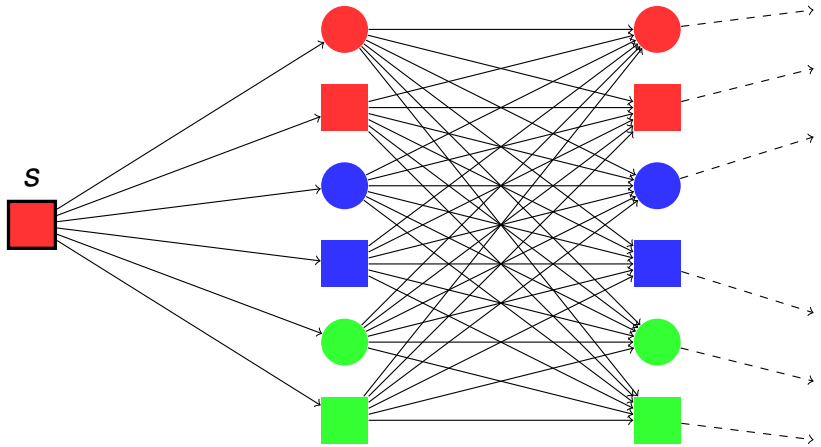
si les agents dans A ne jouent plus x alors ...

- *Formules de chemins :*

$$\psi := \varphi \mid \neg\psi \mid \psi \wedge \psi \mid \mathsf{X}\,\psi \mid \psi\,\mathsf{U}\,\psi$$

Sémantique : le quantificateur $\langle\langle x \rangle\rangle$

Il existe une multi-stratégie

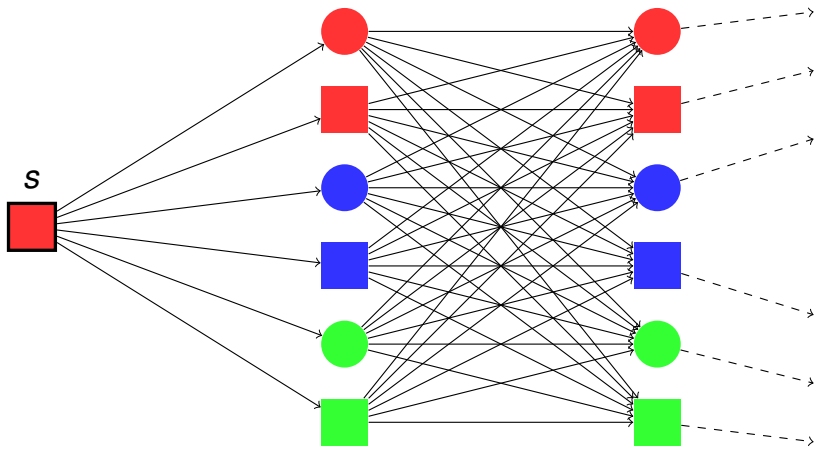


La CGS $\mathcal{G}_1$

$\mathcal{G}_1, s \models_{\mathsf{USL}} \langle\langle x \rangle\rangle \varphi$

Sémantique : le quantificateur $\langle\langle x \rangle\rangle$

Il existe une multi-stratégie



La CGS $\mathcal{G}_1$

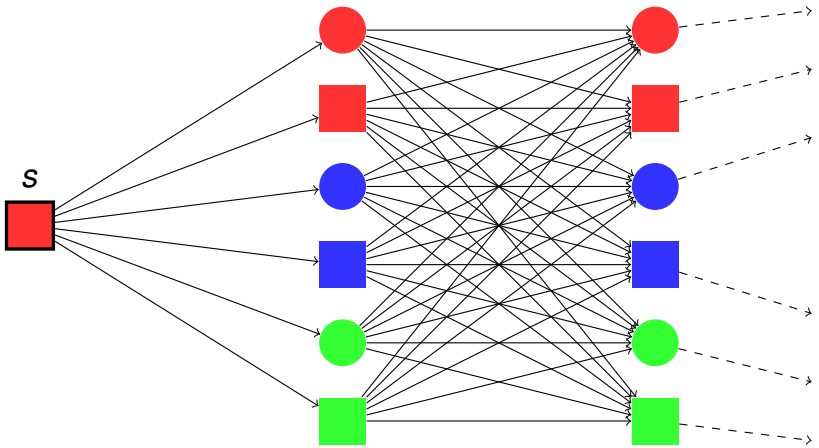
$\mathcal{G}_1, s \models_{\text{USL}} \langle\langle x \rangle\rangle \varphi$ ssi il existe une multi-stratégie σ t.q.

$$\mathcal{G}_1, \langle (x \mapsto \sigma) \rangle, s \models_{\text{USL}} \varphi$$

Sémantique : le lieur $(A \triangleright x)$

Exemple : évaluer $(couleur \triangleright x)$ sachant que

- x est la multi-stratégie *toujoursBleu*

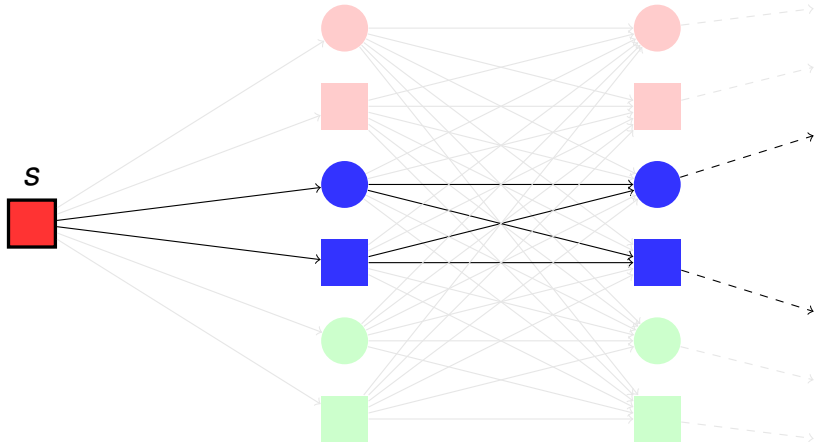


La CGS $\mathcal{G}_1$

Sémantique : le lieur $(A \triangleright x)$

Exemple : évaluer $(\mathit{couleur} \triangleright x)$ sachant que

- x est la multi-stratégie *toujoursBleu*



La CGS $\mathcal{G}_1$

$\mathcal{G}_1, \langle (x \mapsto \mathit{toujoursBleu}) \rangle, s \models_{\mathrm{USL}} (\mathit{couleur} \triangleright x)\psi$

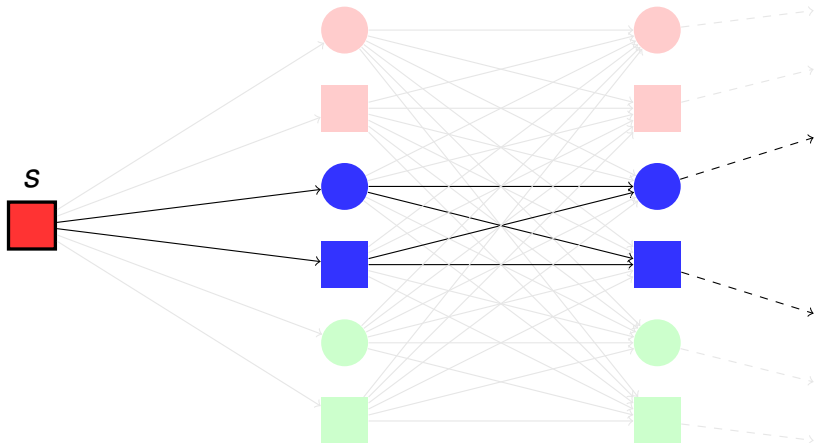
ssi pour toute $\lambda \in \mathit{out}(\langle\langle \mathit{couleur}, \mathit{toujoursBleu} \rangle\rangle, s)$

$\mathcal{G}_1, \langle\langle \mathit{couleur}, \mathit{toujoursBleu} \rangle\rangle, \lambda \models_{\mathrm{USL}} \psi$

Sémantique : le lieur, enrichissement du contexte

Exemple : évaluer ($forme \triangleright y$) sachant que

- y est la multi-stratégie *toujoursCarré*
- *couleur* joue *toujoursBleu*

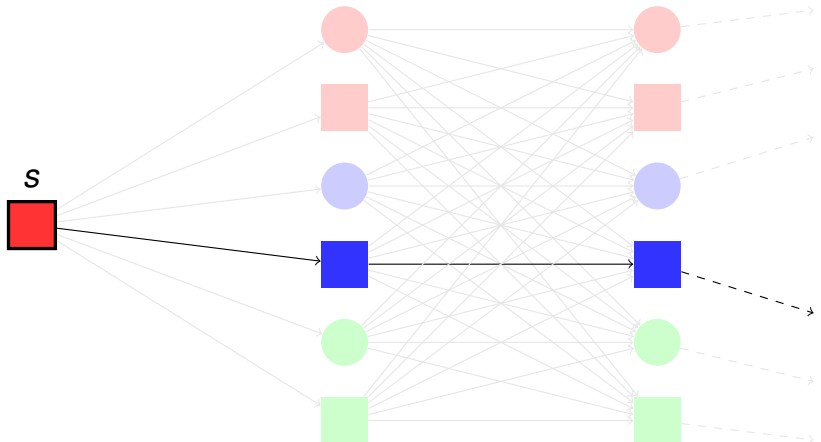


La CGS $\mathcal{G}_1$

Sémantique : le lieur, enrichissement du contexte

Exemple : évaluer $(\mathit{forme} \triangleright y)$ sachant que

- y est la multi-stratégie *toujoursCarré*
- *couleur* joue *toujoursBleu*



La CGS $\mathcal{G}_1$

$\mathcal{G}_1, \langle (y \mapsto \mathit{toujoursCarré}), \langle \mathit{couleur}, \mathit{toujoursBleu} \rangle \rangle, s \models_{\mathrm{USL}} (\mathit{forme} \triangleright y)\psi$

ssi pour toute $\lambda \in \mathit{out}(\langle \langle \mathit{couleur}, \mathit{toujoursBleu} \rangle \langle \mathit{forme}, \mathit{toujoursCarré} \rangle \rangle, s)$

$\mathcal{G}_1, \langle \langle \mathit{couleur}, \mathit{toujoursBleu} \rangle \langle \mathit{forme}, \mathit{toujoursCarré} \rangle \rangle, \lambda \models_{\mathrm{USL}} \psi$

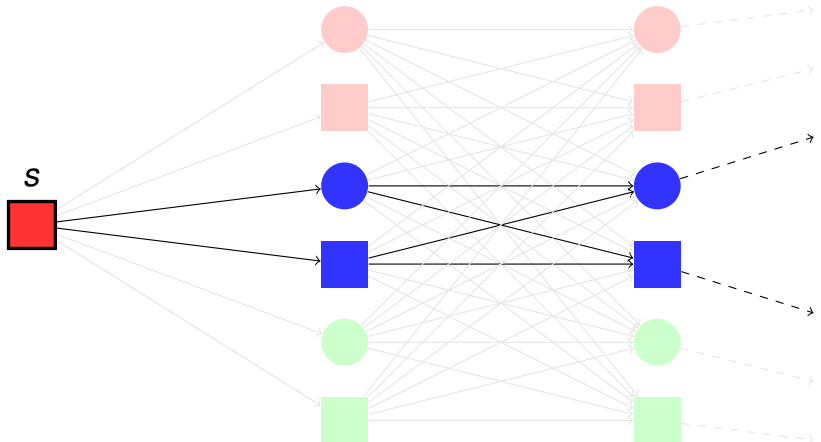
Contextes de stratégies et liaison

- Utilisation des contextes de stratégies : ATL_{sc}, SL
  - Évaluer les formules dans des environnements où plusieurs agents jouent en même temps différentes stratégies
  - Un opérateur de liaison enrichit le contexte . . .
    - Exemple : si *a* joue *x* dans un contexte où *b* joue *y* alors *a* joue *x* et *b* joue *y*
  - . . . sauf s'il concerne un agent déjà lié dans ce contexte
    - Exemple : si *a* joue *x* dans un contexte où *a* joue *y* alors *a* joue *x*
- USL : généraliser le mécanisme d'enrichissement du contexte
  - Le non-déterminisme des **multi-stratégies** permet de les raffiner : un agent peut jouer en même temps selon plusieurs multi-stratégies
    - Exemple : si *a* joue *x* dans un contexte où *a* joue *y* alors *a* joue à la fois *x* et *y*

Sémantique : le lieur, raffinement de multi-stratégie

Exemple : évaluer $(a \triangleright y)$ sachant que

- y est la multi-stratégie *toujoursCarré*
- a joue **déjà** *toujoursBleu*

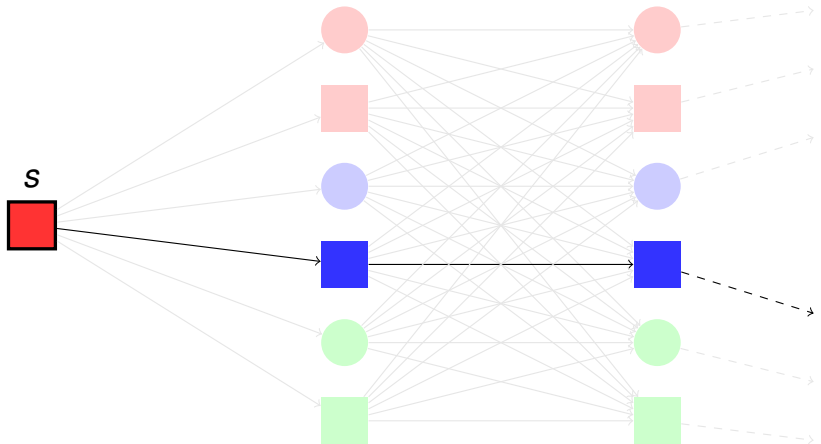


La CGS $\mathcal{G}_2$: un seul agent, a, décide à la fois pour la couleur et pour la forme

Sémantique : le lieur, raffinement de multi-stratégie

Exemple : évaluer $(a \triangleright y)$ sachant que

- y est la multi-stratégie *toujoursCarré*
- a joue **déjà** *toujoursBleu*



La CGS $\mathcal{G}_2$: un seul agent, a, décide à la fois pour la couleur et pour la forme

$\mathcal{G}_2, \langle (y \mapsto \mathit{toujoursCarré}), \langle a, \mathit{toujoursBleu}\rangle\rangle, s \models_{\mathrm{USL}} (a \triangleright y)\psi$

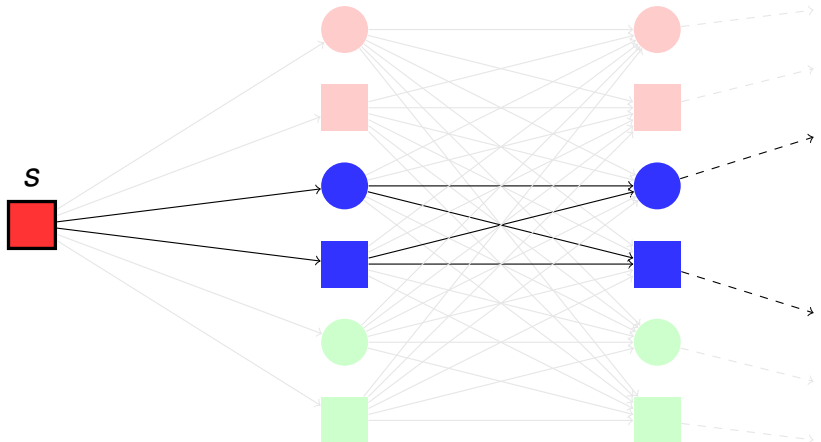
ssi pour toute $\lambda \in \mathit{out}(\langle\langle a, \mathit{toujoursBleu}\rangle\langle a, \mathit{toujoursCarré}\rangle\rangle, s)$

$\mathcal{G}_2, \langle\langle a, \mathit{toujoursBleu}\rangle\langle a, \mathit{toujoursCarré}\rangle\rangle, \lambda \models_{\mathrm{USL}} \psi$

Sémantique : le lieur, engagement contradictoire

Exemple : évaluer $(a \triangleright y)$ sachant que

- y est la multi-stratégie *toujoursRouge*
- a joue **déjà** *toujoursBleu*

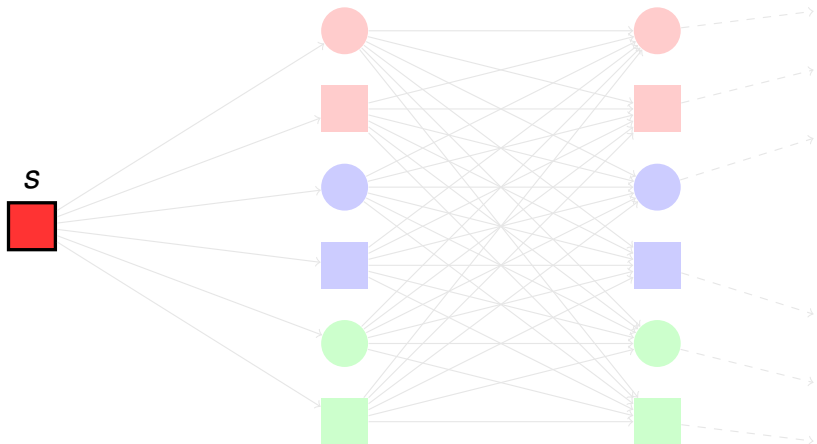


La CGS $\mathcal{G}_2$

Sémantique : le lieur, engagement contradictoire

Exemple : évaluer $(a \triangleright y)$ sachant que

- y est la multi-stratégie *toujoursRouge*
- a joue **déjà** *toujoursBleu*



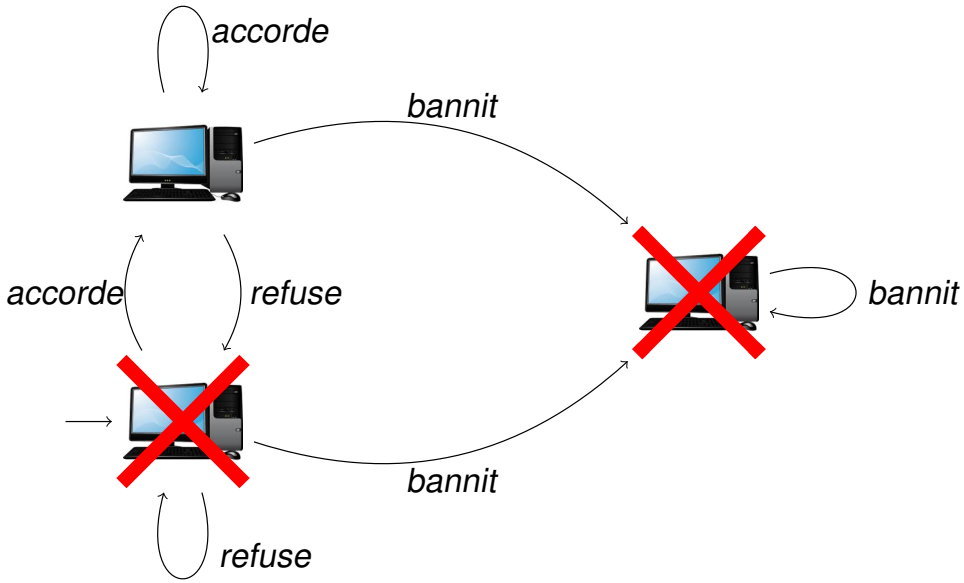
La CGS $\mathcal{G}_2$

$\mathcal{G}_2, \langle (y \mapsto \mathit{toujoursRouge}), \langle a, \mathit{toujoursBleu}\rangle\rangle, s \models_{\mathrm{USL}} (a \triangleright y)\psi$

ssi pour toute $\lambda \in \mathit{out}(\langle\langle a, \mathit{toujoursBleu}\rangle\langle a, \mathit{toujoursRouge}\rangle\rangle, s)$

$\mathcal{G}_2, \langle\langle a, \mathit{toujoursBleu}\rangle\langle a, \mathit{toujoursRouge}\rangle\rangle, \lambda \models_{\mathrm{USL}} \psi$

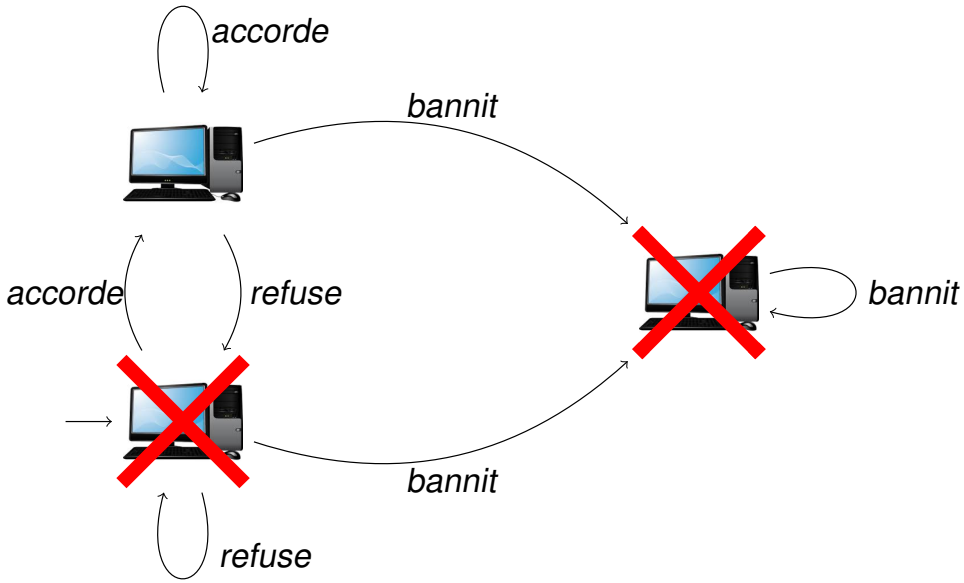
Propriétés exprimables : contrôle pérenne



La CGS $\mathcal{G}_3$: le *serveur* contrôle la connexion du seul client représenté

- La capacité d'un agent à satisfaire et à falsifier une propriété à tout moment.
- *Même si elle est utilisée, cette capacité reste active.*

Propriétés exprimables : contrôle pérenne

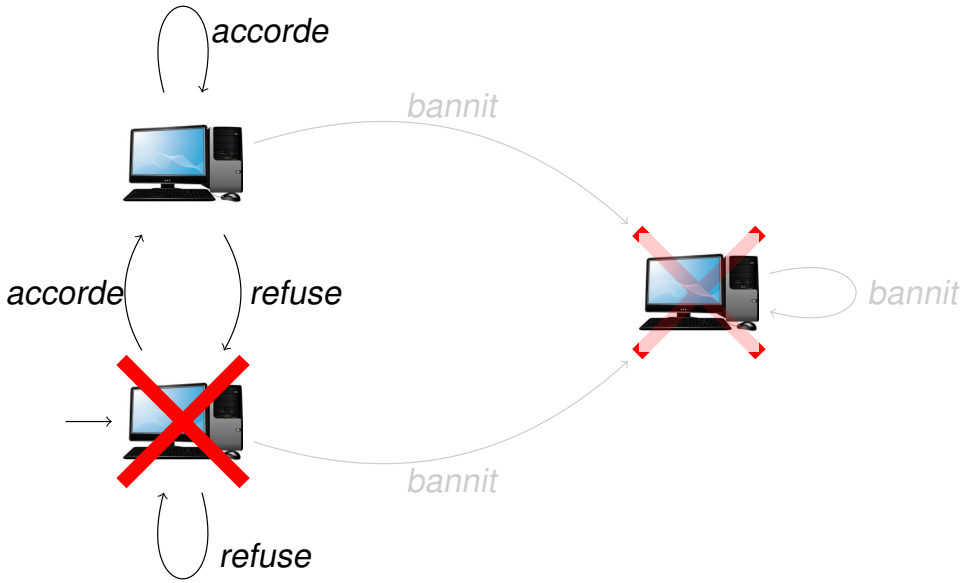


La CGS $\mathcal{G}_3$: le *serveur* contrôle la connexion du seul client représenté

$$\mathcal{G}_3, s \models_{\mathrm{USL}} \langle\!\langle x \rangle\!\rangle (\mathit{serveur} \triangleright x)$$

$$\Box \Big(\langle\!\langle y \rangle\!\rangle (\mathit{serveur} \triangleright y) \, \mathrm{X} \, \text{💻} \; \wedge \langle\!\langle z \rangle\!\rangle (\mathit{serveur} \triangleright z) \, \mathrm{X} \, \text{🚫} \Big)$$

Propriétés exprimables : contrôle pérenne



La CGS $\mathcal{G}_3$: le *serveur* contrôle la connexion du seul client représenté

- multi-stratégie *aor* : toujours jouer *accorde* ou *refuse*

$\mathcal{G}_3, \langle\langle (serveur, aor) \rangle\rangle, s \models_{\mathrm{USL}}$

$$\Box\Big(\langle\langle y \rangle\rangle (serveur \triangleright y)\, \mathrm{X}\, \text{  } \wedge \langle\langle z \rangle\rangle (serveur \triangleright z)\, \mathrm{X}\, \text{  }\Big)$$

pour toute ψ, $\Box\psi := \neg(\top\, \mathrm{U}\, \neg\psi)$

Autres propriétés

- Exécutions finies/infinies
- Ordre partiel sur les multi-stratégies par inclusion
- Stratégies au sens classique (déterministes)
- Dépendance, dépendance forte ...

Propriétés méta-théoriques

Théorème (Pouvoir expressif des logiques de stratégies)

$$ATL \prec ATL_{sc} \prec SL \prec USL$$

Démonstration.

- Plongement de SL dans USL
- Utilisation d'une formule qui *distingue* les actions ayant le même effet

Théorème (Model-checking)

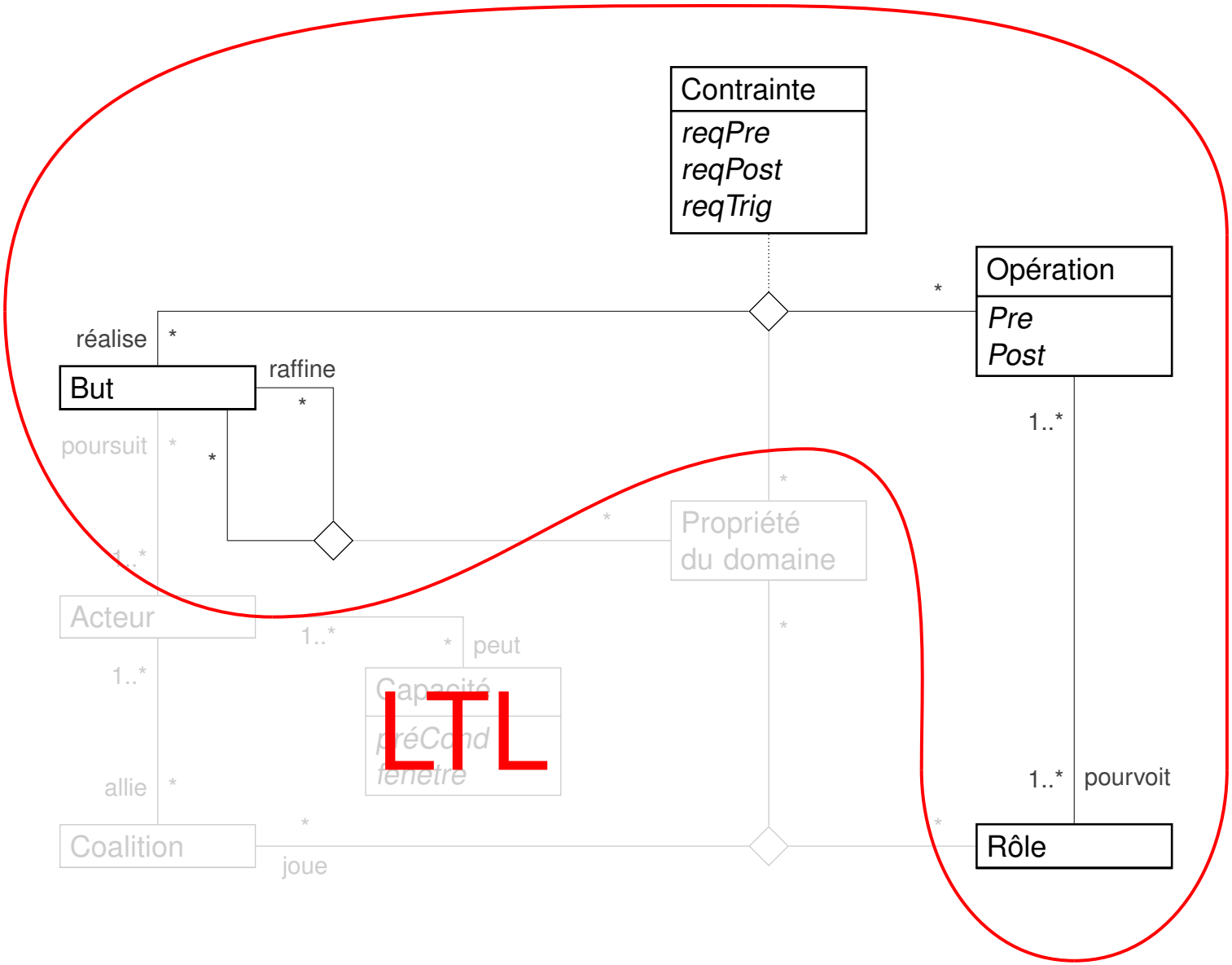
Le problème de model-checking pour USL est décidable en temps NonElémentaire *(comme pour SL).*

Démonstration.

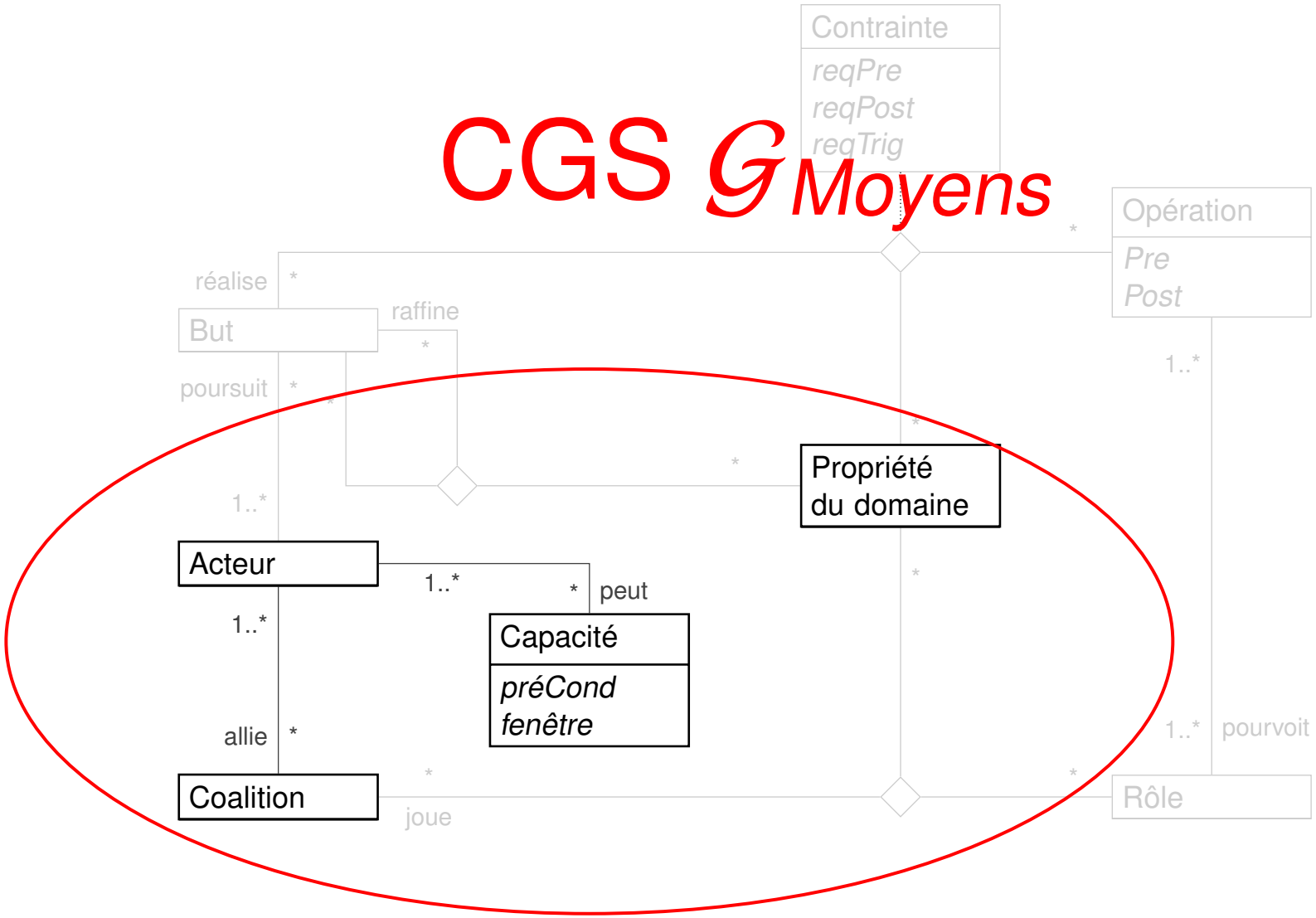
Similaire à celles pour SL, QCTL [LM13] , QDμ [Pin07] . . . : en utilisant des *automates d'arbres alternants*

Plan

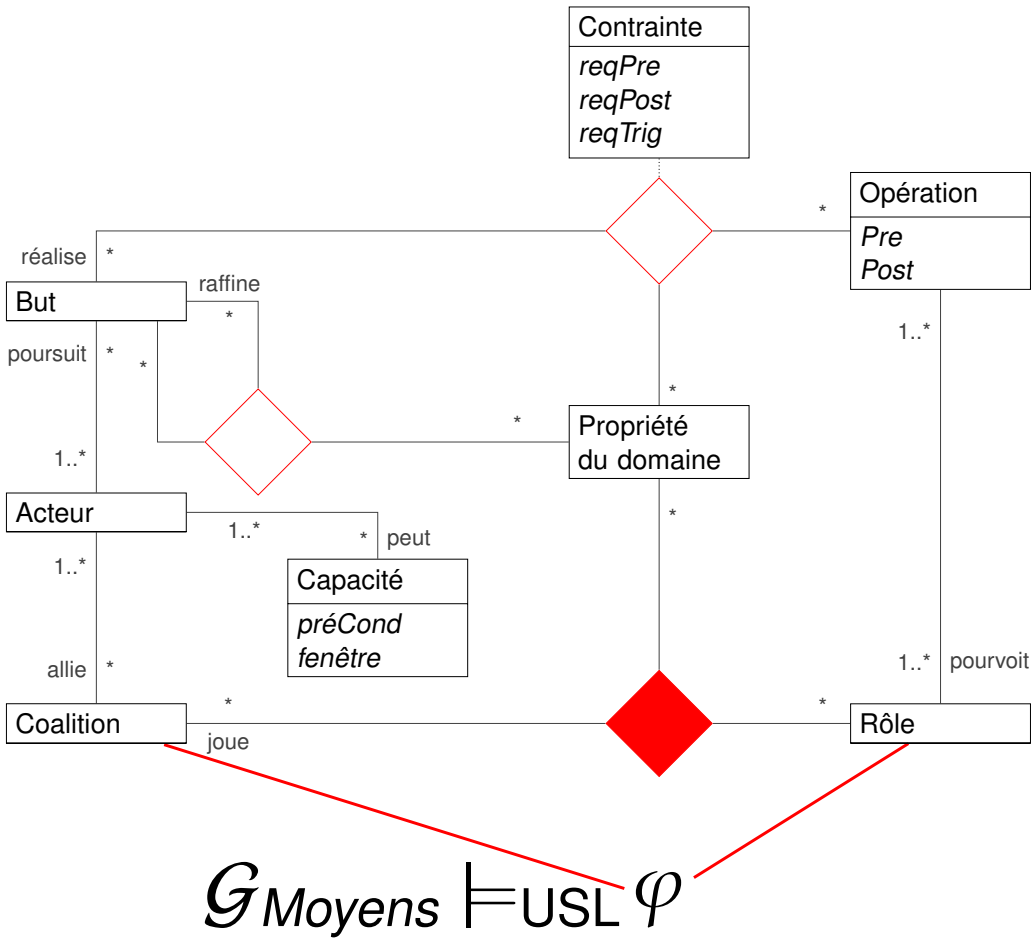
KHI et USL : les exigences



KHI et USL : les moyens



KHI et USL

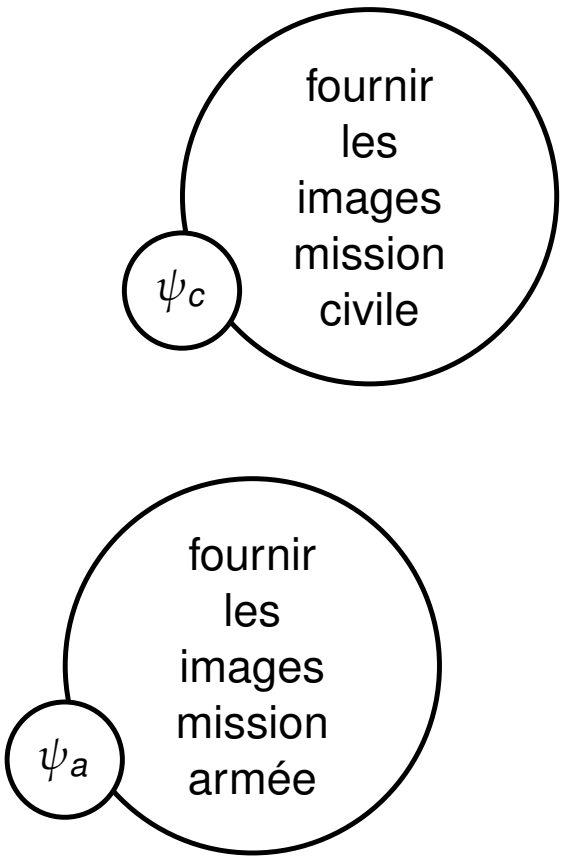


Version de USL pour KHI :

- Forme particulière des formules de LTL pour les rôles : multi-stratégies sans mémoire (model-checking PSPACE complet, comme LTL)
- Modélisation d'*actions contradictoires* : *CGSs étendues* (fonction de transition partielle)

Le problème de l'assignation

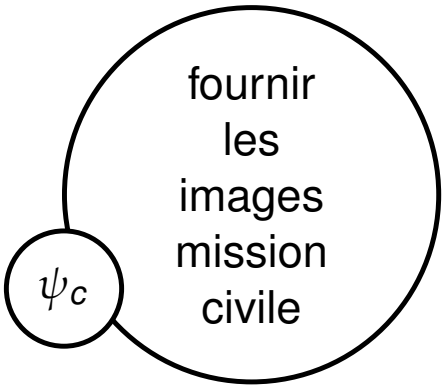
- Un ensemble de rôles donné par l'étude des buts

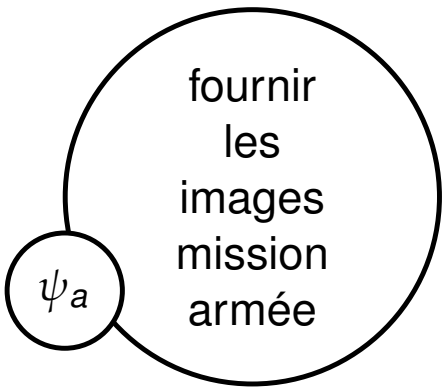


Deux rôles pour fournir des images

Le problème de l'assignation

- Un ensemble de rôles donné par l'étude des buts
- Un ensemble d'acteurs disponibles

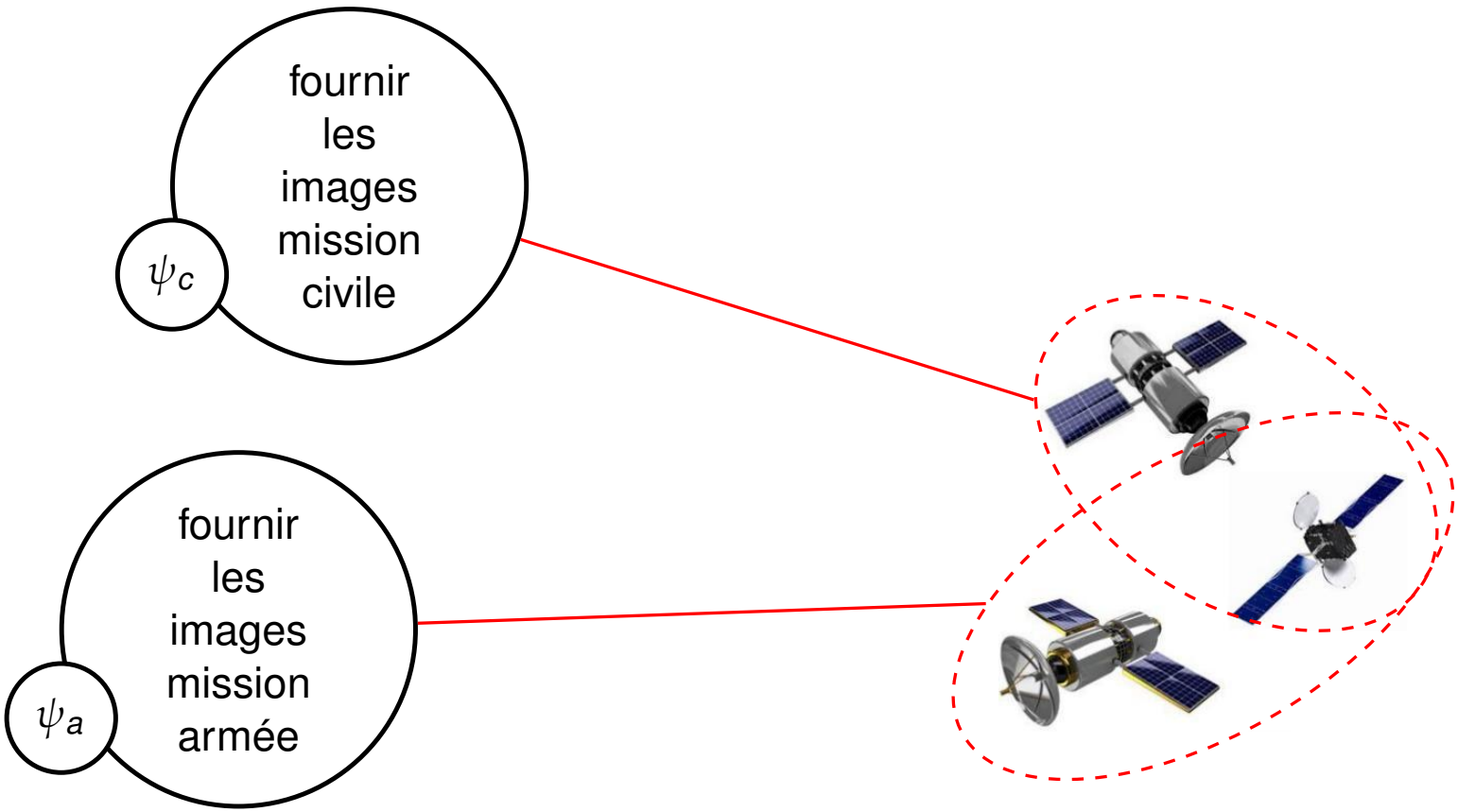




Trois satellites disponibles

Le problème de l'assignation

- Un ensemble de rôles donné par l'étude des buts
- Un ensemble d'acteurs disponibles
- Une assignation des rôles aux coalitions d'acteurs



Critères de correction pour l'assignation

- Correction locale

$$\mathcal{G} \vdash_{\mathsf{USL}} \left(\langle\!\langle \vec{x} \rangle\!\rangle(\ \ \triangleright\ \vec{x})\psi_c\right) \wedge \left(\langle\!\langle \vec{y} \rangle\!\rangle(\ \ \triangleright\ \vec{y})\psi_a\right)$$

$[\![x]\!]\varphi := \neg\langle\!\langle x \rangle\!\rangle\neg\varphi$ $\qquad$ $\langle\!\langle \vec{x} \rangle\!\rangle := \langle\!\langle x_1 \rangle\!\rangle\langle\!\langle x_2 \rangle\!\rangle$

Critères de correction pour l'assignation

- Correction locale

$$\mathcal{G} \vdash_{\mathsf{USL}} \left(\langle\!\langle \vec{x} \rangle\!\rangle(\ \ \triangleright\ \vec{x})\psi_c\right) \wedge \left(\langle\!\langle \vec{y} \rangle\!\rangle(\ \ \triangleright\ \vec{y})\psi_a\right)$$

- Correction globale

$$\mathcal{G} \vdash_{\mathsf{USL}} \langle\!\langle \vec{x} \rangle\!\rangle\left((\ \ \triangleright\ \vec{x})\psi_c \wedge (\ \ \triangleright\ \vec{x})\psi_a\right)$$

$[\![x]\!]\varphi := \neg\langle\!\langle x \rangle\!\rangle\neg\varphi$ $\qquad$ $\langle\!\langle \vec{x} \rangle\!\rangle := \langle\!\langle x_1 \rangle\!\rangle\langle\!\langle x_2 \rangle\!\rangle$

Critères de correction pour l'assignation

- Correction locale

$$\mathcal{G} \vdash_{\mathsf{USL}} \left(\langle\!\langle \vec{x} \rangle\!\rangle(\ \triangleright\ \vec{x})\psi_c\right) \wedge \left(\langle\!\langle \vec{y} \rangle\!\rangle(\ \triangleright\ \vec{y})\psi_a\right)$$

- Correction globale

$$\mathcal{G} \vdash_{\mathsf{USL}} \langle\!\langle \vec{x} \rangle\!\rangle\left((\ \triangleright\ \vec{x})\psi_c \wedge (\ \triangleright\ \vec{x})\psi_a\right)$$

- Collaboration

$$\mathcal{G} \vdash_{\mathsf{USL}} \langle\!\langle \vec{x} \rangle\!\rangle(\ \triangleright\ \vec{x})\left(\psi_c \wedge \langle\!\langle \vec{y} \rangle\!\rangle(\ \triangleright\ \vec{y})\psi_a\right)$$

$[\![x]\!]\varphi := \neg\langle\!\langle x \rangle\!\rangle\neg\varphi$ $\qquad$ $\langle\!\langle \vec{x} \rangle\!\rangle := \langle\!\langle x_1 \rangle\!\rangle\langle\!\langle x_2 \rangle\!\rangle$

Critères de correction pour l'assignation

- Correction locale

$$\mathcal{G} \vdash_{\mathrm{USL}} \left(\langle\!\langle \vec{x} \rangle\!\rangle(\ \triangleright\ \vec{x})\psi_c\right) \wedge \left(\langle\!\langle \vec{y} \rangle\!\rangle(\ \triangleright\ \vec{y})\psi_a\right)$$

- Correction globale

$$\mathcal{G} \vdash_{\mathrm{USL}} \langle\!\langle \vec{x} \rangle\!\rangle\left((\ \triangleright\ \vec{x})\psi_c \wedge (\ \triangleright\ \vec{x})\psi_a\right)$$

- Collaboration

$$\mathcal{G} \vdash_{\mathrm{USL}} \langle\!\langle \vec{x} \rangle\!\rangle(\ \triangleright\ \vec{x})\left(\psi_c \wedge \langle\!\langle \vec{y} \rangle\!\rangle(\ \triangleright\ \vec{y})\psi_a\right)$$

- Contribution

$$\mathcal{G} \vdash_{\mathrm{USL}} [\![\vec{x}]\!]\left((\ \triangleright\ \vec{x})\psi_c \rightarrow \langle\!\langle \vec{y} \rangle\!\rangle(\ \triangleright\ \vec{y})\psi_a\right)$$

$[\![x]\!]\varphi := \neg\langle\!\langle x \rangle\!\rangle\neg\varphi$ $\qquad$ $\langle\!\langle \vec{x} \rangle\!\rangle := \langle\!\langle x_1 \rangle\!\rangle\langle\!\langle x_2 \rangle\!\rangle$

Plan

Bilan

- Un langage de modélisation (Khi [Cha 11, Cha 12]) qui réunit :
  - la description des buts dynamiques et des opérations
  - la relation d'assignation entre les rôles issus des spécifications et les acteurs
- Une logique temporelle multi-agents (USL [Cha 13, Cha 14])
  - formalise les raffinements de multi-stratégies
  - formalise l'incohérence de contextes
  - étend le pouvoir expressif des formalismes du domaine sans accroître la complexité
  - définition et étude de variantes pour la sémantique (actions contradictoires, multi-stratégies sans mémoire, composition de multi-stratégies sans arrêt de l'exécution)
- Une formalisation des instances de Khi en USL : formalisation du problème de l'assignation et résolution en espace polynomial
- Une étude de cas non triviale des missions d'observations par satellite. Elle illustre l'ensemble de l'étude.

Perspectives

- Pour Khi :
  - affiner les critères exprimables et vérifiables
  - généraliser les relations entre les rôles dans la collaboration et la contribution
  - étendre la modélisation et la formalisation en USL : sécurité . . .
- Logique :
  - recherche de fragments d'USL avec des meilleurs résultats de complexité
  - poursuite de l'étude du pouvoir expressif d'USL
  - analyser d'autres modes de composition entre les multi-stratégies

Merci de votre attention