Dixit

Un éditeur de diagrammes de prédicats

http://www.loria.fr/equipes/mosel/dixit/

Loïc Fejoz

loic.fejoz@loria.fr

Mosel, Loria

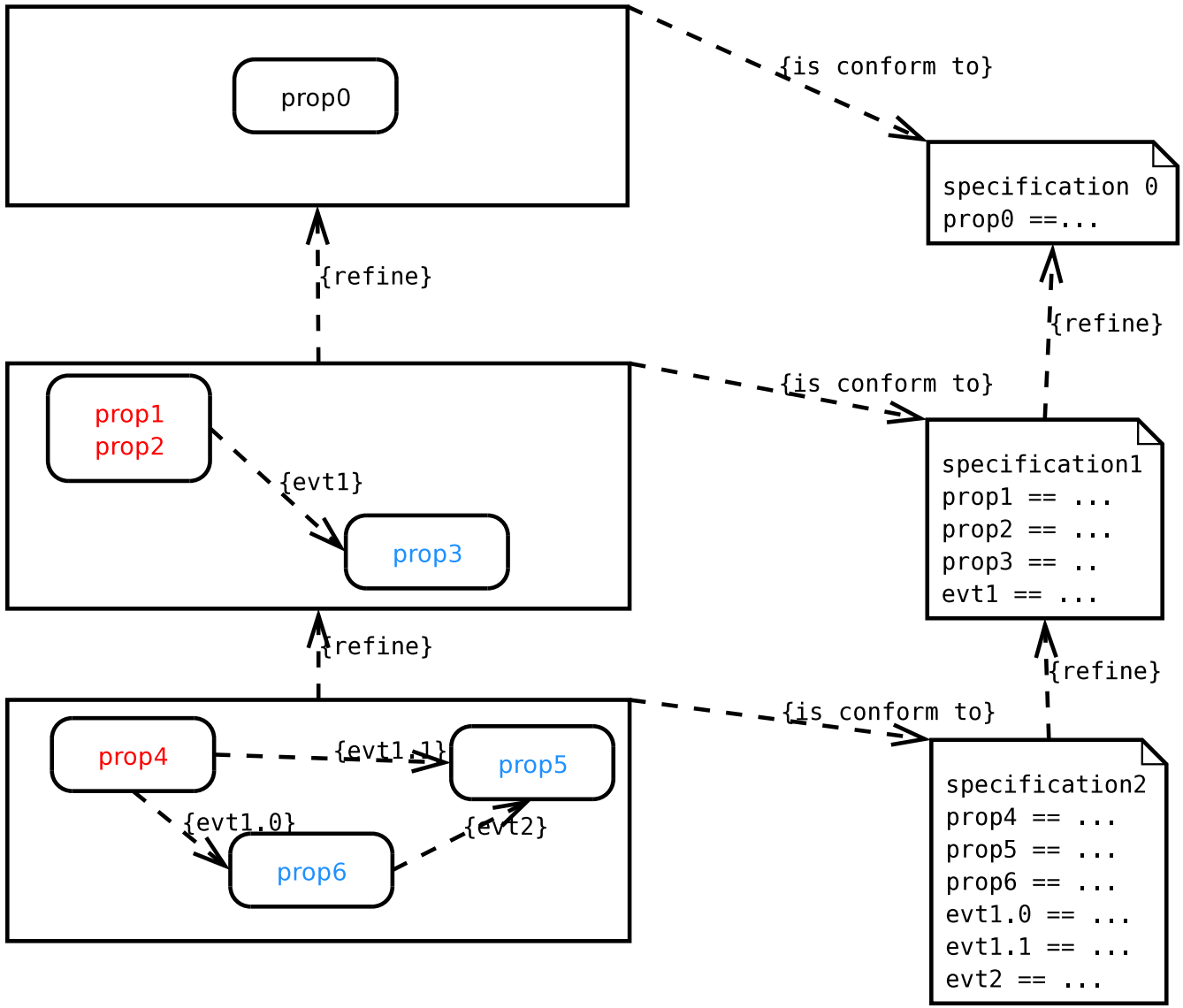
Sommaire

- Présentation de Mosel
- Présentation des diagrammes de prédicats
- Architecture de DIXIT
- Les difficultés dans la programmation

Mosel

- Les Objectifs
  - Développement prouvé de systèmes informatiques ;
  - Intégration de la preuve dans le développement de systèmes informatiques ;
  - Exprimentation du raffinement dans la conception de modèles;
  - Modélisation d'applications comme les systèmes (répartis, mobiles, enfouis).
- Les outils
  - diagrammes de prédicats : DIXIT,
  - balbulette B,
  - model checking UML (HUGO),
  - interface pour TLC.

Les diagrammes de prédicats - Principe



Raffinement de diagrammes - 1

Assume given two predicate diagrams $G^1 = (N^1, I^1, \delta^1, o^1, \zeta^1)$ over $\mathcal{P}^1$ and $\mathcal{A}^1$ and $G^2 = (N^2, I^2, \delta^2, o^2, \zeta^2)$ over $\mathcal{P}^2$ and $\mathcal{A}^2$ where $\mathcal{A}^1 \supseteq \mathcal{A}^2$, as well as a state predicate I. Let x^2 be a tuple of all variables that occur in $\mathcal{P}^2$, but not in $\mathcal{P}^1$, and let $f : N^1 \to N^2$. We say that G^1 *structurally refines* G^2 *up to* I *w.r.t.* f iff all of the following conditions hold:

- $f(I^1) \subseteq I^2$, [STRUCTURAL CHECK]
- $\models n \implies \exists x^2 : I \wedge f(n)$ holds for every node $n \in N^1$. [PROVER]
- For all $n, m \in N^1$ and all $A \in \mathcal{A}^1$ such that $(n, m) \in \delta^1_A$: [STRUCTURAL CHECK]
  1. if $A \in \mathcal{A}^2$ then $(f(n), f(m)) \in \delta^2_A$, and
  2. if $A \in \mathcal{A}^1 \setminus \mathcal{A}^2$ then $(f(n), f(m)) \in \delta^2_=$.

Raffinement de diagrammes - 2

- For all $n, m \in N^1$ and all $A \in \mathcal{A}^1$ such that $(n, m) \in \delta^1_A$: [STRUCTURAL CHECK]
  1. for all $(t_2, \prec_2) \in o^2(f(n), f(m))$ there exists some $(t_1, \prec_1) \in o^1(n, m)$ such that
     - $\models n \wedge m' \wedge I \wedge I' \wedge t'_1 \prec_1 t_1 \implies t'_2 \prec_2 t_2$ and
     - $\models n \wedge n' \wedge I \wedge I' \wedge t'_1 \preceq_1 t_1 \implies t'_2 \preceq_2 t_2$,
  2. if $f(n) = f(m)$ and $(t_2, \prec_2) \in o^2(f(n), m')$ holds for some $m' \in N^2$ then there exists some $(t_1, \prec_1) \in o^1(n, m)$ such that

$$\models n \wedge m' \wedge I \wedge I' \wedge t'_1 \prec_1 t_1 \implies t'_2 \preceq_2 t_2$$

Raffinement de diagrammes - 3

- For every run $\rho^1 = (s_0, n_0, A_0)(s_1, n_1, A_1)\ldots$ of G^1 and every action $A \in \mathcal{A}^2$ such that $\zeta^2(A) = \mathrm{WF}$, either $A_i = A$ or $f(n_i) \notin En^2(A)$ holds for infinitely many $i \in \mathbb{N}$. [MODEL CHECKER]
- For every run $\rho^1 = (s_0, n_0, A_0)(s_1, n_1, A_1)\ldots$ of G^1 and every action $A \in \mathcal{A}^2$ such that $\zeta^2(A) = \mathrm{SF}$, either $A_i = A$ holds for infinitely many $i \in \mathbb{N}$ or $f(n_i) \in En^2(A)$ for only finitely many $i \in \mathbb{N}$. [MODEL CHECKER]

Conformance - 1

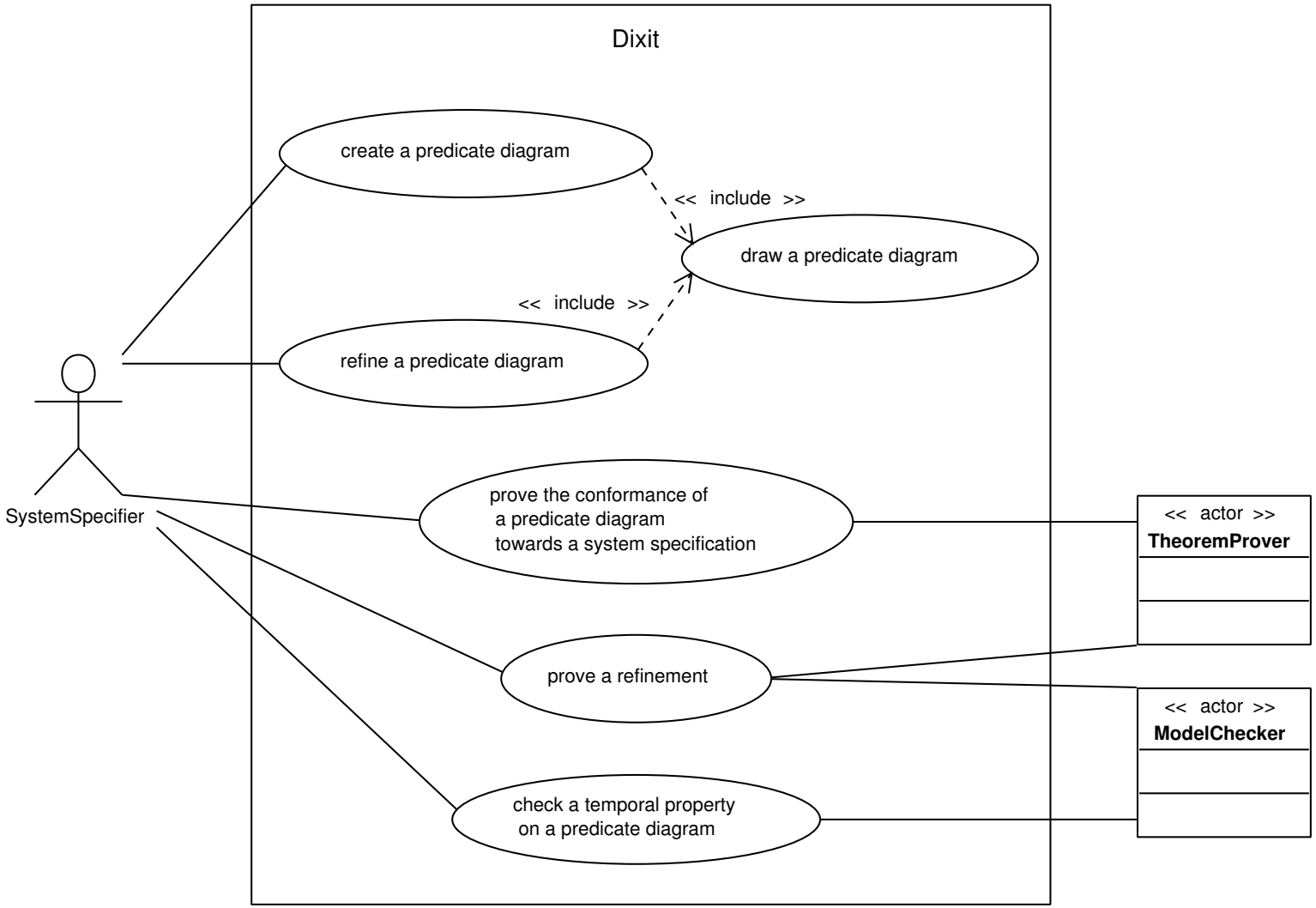
Let $G = (N, I, \delta, o, \zeta)$ be a predicate diagram over $\mathcal{P}$ and $\mathcal{A}$, and $Spec \equiv Init \wedge \Box[Next]_v \wedge L$ be a system specification. If all of the following conditions hold then G conforms to $Spec$.

- $\models Init \implies \bigvee_{n \in I} n$ [PROVER]
- $\models n \wedge [Next]_v \implies n' \vee \bigvee_{\{(A,m):(n,m)\in\delta_A\}} \langle A \rangle_v \wedge m'$ holds for every node $n \in N$. [PROVER]
- For all $n, m \in N$ and all $(t, \prec) \in o(n, m)$: [PROVER]
  1. $\models n \wedge m' \wedge \bigvee_{\{A:(n,m)\in\delta_A\}} \langle A \rangle_v \implies t' \prec t$ and
  2. $\models n \wedge [Next]_v \wedge n' \implies t' \preceq t$.

Conformance - 2

- For every action $A \in \mathcal{A}$ such that $\zeta(A) \neq \mathrm{NF}$:
  1. If $\zeta(A) = \mathrm{WF}$ then $\models Spec \implies \mathrm{WF}_v(A)$. [STRUCTURAL CHECK]
  2. If $\zeta(A) = \mathrm{SF}$ then $\models Spec \implies \mathrm{SF}_v(A)$. [STRUCTURAL CHECK]
  3. $\models n \implies$ ENABLED $\langle A \rangle_v$ holds whenever $n \in En(A)$. [PROVER]
  4. $\models n \wedge \langle A \rangle_v \implies \neg m'$ holds for all $n, m \in N$ such that $(n, m) \notin \delta_A$. [PROVER]

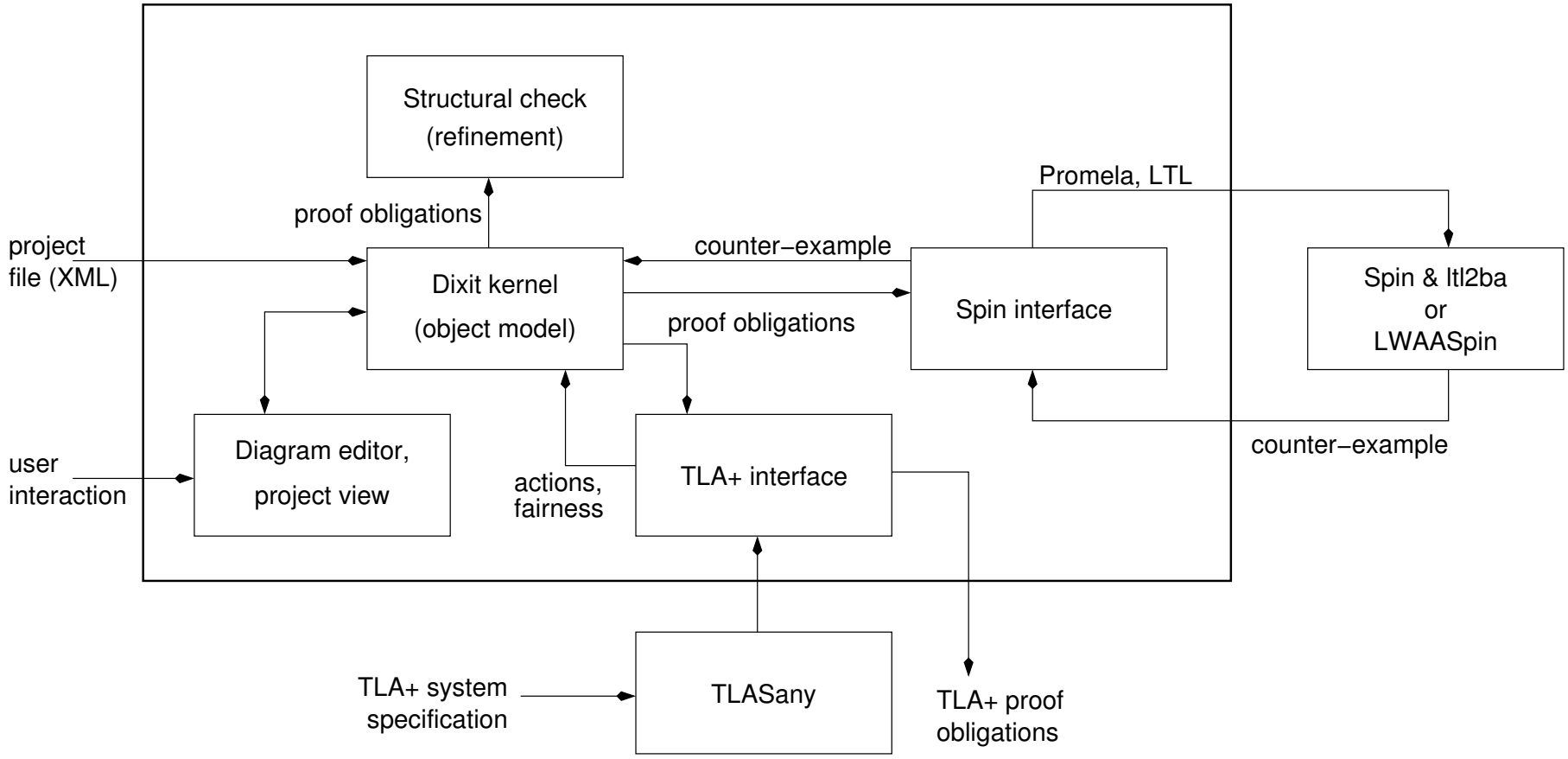
Dixit Use Case



La pratique

Dixit par l'exemple : L'exclusion mutuelle...
Deux agents se partagent une même ressource. Ils ne peuvent l'utiliser en même temps.

Architecture



Les difficultés

- Réutilisation de TLASany ;
- Utilisation de `http://gef.tigris.org/` pour la partie diagramme ;
- Implémentation du modèle MVC (problème avec les threads) ;
- JavaWebStart (File vs. FileContent).

The End

Des questions ?