

Vérification des Propriétés Quantitatives

une Action Spécifique du RTP SECC

N. Halbwachs (Vérimag, Grenoble)

Ph. Schnoebelen (LSV, Cachan)

<http://www-verimag.imag.fr/AS22/>

“Vérification des propriétés quantitatives”

- Qui ? Quand ? Pourquoi ?
- La problématique de l'Action
- Les résultats de l'Action
- Bilan & perspectives
- Quelle suite à l'Action ?

Qui ? Quand ? Pourquoi ?

Durée : d'octobre 2001 à décembre 2002.

Participants :

LSV (Cachan) : Ph. Schnoebelen, A. Finkel, F. Laroussinie, B. Bérard, L. Fribourg, P. Bouyer, ...

Vérimag (Grenoble) : N. Halbwachs, S. Yovine, S. Tripakis, E. Asarin, P. Raymond, ...

LIAFA (Paris 7) : A. Bouajjani, P. Habermehl, M. Sighireanu, Y. Jurski, ...

IRCCyN (Nantes) : O. Roux, Ch. Mauraas, ...

et aussi : B. Jeannet (IRISA), G. Sutre (LaBRI), ...

Des communautés qui se rejoignent :

- systèmes temporisés \leftrightarrow systèmes à compteurs \leftrightarrow contrôle infini
- model-checking symbolique \leftrightarrow interprétation abstraite \leftrightarrow ...
- propriétés paramétrées \leftrightarrow propriétés numériques \leftrightarrow ...

Budget alloué : 45 kE.

La problématique de l'Action

La montée en puissance du model-checking

Le champ d'application du model-checking
n'a cessé de croître

La montée en puissance du model-checking

Le champ d'application du model-checking
n'a cessé de croître

1985 → : systèmes réactifs

Idées fortes : modèles d'automates + Logique temporelle

La montée en puissance du model-checking

Le champ d'application du model-checking
n'a cessé de croître

1985 → : systèmes réactifs

Idées fortes : modèles d'automates + Logique temporelle

1990 → : systèmes critiques / circuits

Idées fortes : BDD + modèles abstraits

La montée en puissance du model-checking

Le champ d'application du model-checking n'a cessé de croître

1985 → : systèmes réactifs

Idées fortes : modèles d'automates + Logique temporelle

1990 → : systèmes critiques / circuits

Idées fortes : BDD + modèles abstraits

1993 → : systèmes temps réels

Idées fortes : automates temporisés, systèmes hybrides

La montée en puissance du model-checking

Le champ d'application du model-checking n'a cessé de croître

1985 → : systèmes réactifs

Idées fortes : modèles d'automates + Logique temporelle

1990 → : systèmes critiques / circuits

Idées fortes : BDD + modèles abstraits

1993 → : systèmes temps réels

Idées fortes : automates temporisés, systèmes hybrides

2000 → : systèmes embarqués, complexes ou contraints

Idée forte : model-checking symbolique + abstraction automatisée permettent d'attaquer de très nombreux problèmes.

P.ex. : protocoles sécuritifs, systèmes paramétrés, analyses statique pour la compilation, etc.

Et au delà ?

- Les techniques de model-checking continueront à se répandre :
 - nouveaux domaines : web, bases de données, API, compilateurs, ...
 - nouveaux problèmes : systèmes ouverts, ordonnancement, analyse de performance, ...

Et au delà ?

- Les techniques de model-checking continueront à se répandre :
 - nouveaux domaines : web, bases de données, API, compilateurs, ...
 - nouveaux problèmes : systèmes ouverts, ordonnancement, analyse de performance, ...
- Les ingrédients clés :
 - Construction automatique de modèles de type “automate étendu”
 - Représentations symboliques & algorithmes associés

Et au delà ?

- Les techniques de model-checking continueront à se répandre :
 - nouveaux domaines : web, bases de données, API, compilateurs, ...
 - nouveaux problèmes : systèmes ouverts, ordonnancement, analyse de performance, ...
- Les ingrédients clés :
 - Construction automatique de modèles de type “automate étendu”
 - Représentations symboliques & algorithmes associés
- L’obstacle principal :
 - L’explosion combinatoire des états.

Les représentations symboliques

Cas fini :

Binary Decision Diagrams !

Les représentations symboliques

Cas fini :

Binary Decision Diagrams !

Cas infinis :

- Régions / contraintes linéaires
⇒ valuation d'horloges, données temporisées, ...

Les représentations symboliques

Cas fini :

Binary Decision Diagrams !

Cas infinis :

- Régions / contraintes linéaires
⇒ valuation d'horloges, données temporisées, ...
- Ensembles semilinéaires / Formules de Presburger / contraintes arithmétiques
⇒ valeurs de compteurs, indices de tableaux, ...

Les représentations symboliques

Cas fini :

Binary Decision Diagrams !

Cas infinis :

- Régions / contraintes linéaires
⇒ valuation d'horloges, données temporisées, ...
- Ensembles semilinéaires / Formules de Presburger / contraintes arithmétiques
⇒ valeurs de compteurs, indices de tableaux, ...
- Langages réguliers / Automates
⇒ contenus de files, contrôle des programmes récursifs
- ...

Les propriétés quantitatives

Un bon terrain de rencontre !

- non booléen \approx quantitatif (numérique, etc.)

Les propriétés quantitatives

Un bon terrain de rencontre !

- non booléen \approx quantitatif (numérique, etc.)
- **Modèles quantitatifs :**
systèmes temporisés, hybrides, ...
- **Spécifications quantitatives :**
temps d'exécution, disponibilité, paramètres, ...
- **Techniques quantitatives :**
randomisation, ...

Les propriétés quantitatives

Un bon terrain de rencontre !

- non booléen \approx quantitatif (numérique, etc.)
- **Modèles quantitatifs :**
systèmes temporisés, hybrides, ...
Spécifications quantitatives :
temps d'exécution, disponibilité, paramètres, ...
Techniques quantitatives :
randomisation, ...
- \neq systèmes infinis ?
 - ne se focalise pas sur les modèles ou les domaines d'application
 - approche plus orientée vers les algorithmes
 - l'objectif est d'unifier, de transférer des idées, des techniques, ...

Les questions fondamentales

- Quelles représentations symboliques généralistes subsisteront ? (& quels algorithmes)

Équivalent futur des BDDs ?

Les questions fondamentales

- Quelles représentations symboliques généralistes subsisteront ? (& quels algorithmes)

Équivalent futur des BDDs ?

- Quels modèles ? (& pour quelles applications, avec quelles techniques)

Frontières contrôle / données ?

Les questions fondamentales

- Quelles représentations symboliques généralistes subsisteront ? (& quels algorithmes)

Équivalent futur des BDDs ?

- Quels modèles ? (& pour quelles applications, avec quelles techniques)

Frontières contrôle / données ?

- Quelles techniques généralistes de vérification ?
- Comment combiner des méthodes ?

Résultats de l'Action

Représentations symboliques

Représentations hétérogènes :

- Booléens & contraintes linéaires (Mauras, Garriou, Jeannet)
- Automates & contraintes linéaires (Bouajjani, Habermehl *et al.*)
- DBM paramétrées + NDD (Bouajjani *et al.*)

Représentations symboliques

Représentations hétérogènes :

- Booléens & contraintes linéaires (Mauras, Garriou, Jeannet)
- Automates & contraintes linéaires (Bouajjani, Habermehl *et al.*)
- DBM paramétrées + NDD (Bouajjani *et al.*)

Représentations généralistes :

- Ensembles semilinéaires pour l'abstraction de la synchronisation (programmes multithreads) (Bouajjani, Touili)
- Beaux préordres (Finkel, Schnoebelen, etc.)
- Compteurs pour paramètres (protocole TTPC, *broadcast protocols*) (Finkel, Bouajjani, etc.)

Représentations symboliques

Représentations hétérogènes :

- Booléens & contraintes linéaires (Mauras, Garriou, Jeannet)
- Automates & contraintes linéaires (Bouajjani, Habermehl *et al.*)
- DBM paramétrées + NDD (Bouajjani *et al.*)

Représentations généralistes :

- Ensembles semilinéaires pour l'abstraction de la synchronisation (programmes multithreads) (Bouajjani, Touili)
- Beaux préordres (Finkel, Schnoebelen, etc.)
- Compteurs pour paramètres (protocole TTPC, *broadcast protocols*) (Finkel, Bouajjani, etc.)

Algorithmique :

- Polyèdres (Halbwachs)
- Semilinéaires & Presburger (Finkel)

Algorithmes de vérification

- Traduction de spécifications “*duration calculus*” en automates à compteurs symboliques (Halbwachs *et al.*)
- Chaînage-avant et vérification symbolique des automates temporisés (Bouyer)
- Fonctions affines par morceaux pour l’accessibilité et le calcul du portrait de phase (Yovine, Asarin, Schneider)
- Méthodes probabilistes pour la vérification des systèmes à canaux non fiables (Schnoebelen *et al.*)
- Heuristiques pour les techniques d’accélération (Finkel, Leroux, *et al.*)
- Algorithmes non numériques pour propriétés quantitatives (Laroussinie, Markey, Schnoebelen)
- ...

Animation scientifique

Organisation de 4 journées scientifiques :

- En déc. 2001, mars 2002, juin 2002 et nov. 2002.
- Rassemblant de 20 à 40 participants (dont Paris, Orsay, mais aussi Belgique, Orléans, Toulouse, Bordeaux, Besançon, Poitiers, ...)
- Contenu disponible via le web.

Workshop “Vérification de propriétés quantitatives” :

- 5–7 mars 2003 à Grenoble.
- Conjointement aux 4e Journées Systèmes Infinis.

Bilan – Perspectives

Bilan – Perspectives

Les convergences existent

Convergences de modèles :

Valeurs réelles vs. valeurs entières

Automates à compteurs vs. systèmes distribués vs. automates à piles

Bilan – Perspectives

Les convergences existent

Convergences de modèles :

Valeurs réelles vs. valeurs entières

Automates à compteurs vs. systèmes distribués vs. automates à piles

Convergence de représentations symboliques :

Automates pour semilinéaires, contenus de piles et files, paramètres, ...

Diagrammes de décision étendus

Bilan – Perspectives

Les convergences existent

Convergences de modèles :

Valeurs réelles vs. valeurs entières

Automates à compteurs vs. systèmes distribués vs. automates à piles

Convergence de représentations symboliques :

Automates pour semilinéaires, contenus de piles et files, paramètres, ...

Diagrammes de décision étendus

Convergence de méthodes :

Accélérations exactes

Techniques d'élargissement

Randomization

Quelle suite ?

Au delà des systèmes temporisés
et des systèmes à compteurs

Quelle suite ?

Au delà des systèmes temporisés et des systèmes à compteurs

- Stabilité numérique ?
- Probabiliste et/ou stochastique ?
- Utilisation mémoire ?
- Fiabilité ?