ACI Sécurité Informatique PERSÉE

www.labri.fr/Perso/~herbrete/persee/

---

rapport final

Ph. Schnoebelen
LSV
CNRS & ENS de Cachan

A. Bouajjani
LIAFA
CNRS & Univ. Paris 7

G. Sutre
LaBRI
CNRS & Univ. Bordeaux

novembre 2006

Table des matières

1 Description générale

Le projet PERSÉE vise à développer des techniques de vérification symbolique pour les *systèmes hétérogènes*, c.-à-d. des systèmes modélisés par un graphe de contrôle agissant sur des variables non-bornées et de types différents. Ces systèmes sont des modèles naturels pour les systèmes embarqués, les protocoles, les algorithmes distribués, les systèmes sur puce, etc.

Les principaux axes de travail envisagés concernent :

- la mise au point de modèles, de méthodes symboliques (en particulier à base d'accélérations), et de structures de données avancés ;
- la construction de modèles abstraits de haut niveau ;
- la proposition d'un cadre pour la combinaison de représentations symboliques ;
- le développement d'un environnement permettant d'utiliser différents outils symboliques en combinaison.

Le but du projet est aussi de favoriser des échanges et des synergies entre des équipes reconnues au plan international, dont les compétences sont complémentaires, mais qui n'avaient pas encore pris l'habitude de travailler en collaboration.

2 Participants

Les chercheurs participant au projet PERSÉE sont issus des trois équipes suivantes :

1. L'axe INFINI du Laboratoire Spécification & Vérification (LSV) à Cachan :
   - Ph. Schnoebelen, DR, CNRS ;
   - A. Finkel, PU, ENS Cachan ;
   - D. Nowak, CR, CNRS ;
   - A. Halbert, IE, ENS Cachan ;
   - Ch. Darlot, postdoctorant (de sep. 2003 à août 2004) ;
   - J. Leroux, postdoctorant[1] ;
   - S. Bardin, doctorant ;
   - N. Bertrand, doctorante (depuis oct. 2003).
2. L'équipe Modélisation et Vérification du Laboratoire d'Informatique Algorithmique, Fondements et Applications (LIAFA) à Paris 7 :
   - A. Bouajjani, PU Paris 7 ;
   - P. Habermehl, MdC Paris 7 ;
   - Y. Jurski, MdC Paris 7 ;
   - M. Sighireanu, MdC Paris 7 ;
   - T. Touili, doctorante puis CR CNRS ;
   - A. Meyer, doctorant puis MdC Paris 7 ;
   - P. Moro, doctorant (depuis oct. 2003).
3. L'équipe MVTSI du Laboratoire Bordelais de Recherche en Informatique (LaBRI) à Bordeaux :
   - G. Sutre, CR CNRS ;
   - J.-M. Couvreur, MdC Bordeaux (jusqu'à sep. 2005) ;
   - F. Herbreteau, MdC Bordeaux ;

[1] J. Leroux, ancien doctorant du LSV, a effectué un séjour postdoctoral à Montréal en 2003–2004, puis un séjour postdoctoral à Rennes en 2004–2005. Durant ces deux années, il a poursuivi ses collaborations avec A. Finkel et S. Bardin dans le cadre de PERSÉE. Il a ensuite été recruté comme CR CNRS au LaBRI dans l'équipe MVTSI.

– A. Griffault, MdC Bordeaux ;
– K. Musumbu, MdC Bordeaux ;
– A. Vincent, doctorant puis MdC Bordeaux ;
– M. Adélaïde, ATER (de sep. 2002 à sep. 2004) ;
– T. Q. Tran, doctorant (depuis oct. 2004).

À ce jour, cinq réunions plénières rassemblant l'essentiel des participants ont eu lieu :

1. le 24 nov 2003 à Paris,
2. le 15 mar 2004 à Paris,
3. les 7 et 8 juin 2004 à Cachan,
4. les 14 et 15 septembre 2004 à Bordeaux,
5. le 26 mai 2005 à Paris.

Le programme de ces journées est disponible sur le site Web du projet.

D'autres réunions, n'impliquant en général qu'un groupe de travail, se sont tenues par ailleurs.

3 Résultats scientifiques

Cette section décrit succinctement les principaux résultats scientifiques du projet Persée (et donnent les références de publications ou rapports techniques concernés). Elle est découpée en quatre sous-sections correspondant exactement aux quatre axes de travail du projet.

3.1 Calcul symbolique d'accessibilité

3.1.1 Théorie des accélérations

Une théorie des accélérations plates a été développée dans [BFLS05] pour les propriétés de sûreté, puis généralisée à la logique CTL* dans [DFGv06]. Ce travail a permis de formaliser certaines des notions sous-jacentes à l'approche développée au LSV pour l'analyse symbolique des systèmes complexes, et de dégager des principes heuristiques d'application générale, et qui sont en particulier appliqués dans l'outil FAST [BFL04, BDF04, BLP06].

Une retombée théorique très surprenante est due à Leroux et Sutre, qui ont montré qu'un très grand nombre de classes de systèmes à compteurs pour lesquels l'ensemble d'accessibilité avait été prouvé semilinéaire et effectif sont en fait des systèmes aplatissables [LS04, LS05]. Ainsi, notre algorithme générique d'accélération plate (et donc l'outil FAST) s'applique à ces systèmes, est garanti de terminer, et remplace utilement les algorithmes ad-hoc proposés indépendamment pour chacune des classes.

3.1.2 Au-delà des propriétés de sûreté

Propriétés de vivacité. Les techniques classiques permettant de réduire la vérification des propriétés de vivacité à des questions d'accessibilité ne s'étendent pas aux systèmes infinis. Les réponses à cette difficulté sont en général en partie ad-hoc, dépendant à la fois d'une famille de modèles, d'une classe de propriétés, et d'une technique algorithmique de vérification.

L'étude des aspects pratiques de cette question dans un cadre de *regular model checking* est abordée dans [BLW05], où les configurations des systèmes peuvent être représentées par des mots finis arbitrairement longs, voire par des mots *infinis* dans le cadre du *omega-regular model checking*.

Une autre contribution est fournie par [BS04, ABRS05, BBS07, BBS06a], où les modèles sont des processus de décision markoviens modélisant des protocoles asynchrones dans lesquels les pertes de messages obéissent à des lois probabilistes naturelles. Cette approche a permis de vérifier automatiquement la vivacité de divers protocoles [BBS06c].

Résolution de jeux. Plus généralement, la vivacité des *systèmes ouverts* se décrit naturellement sous la forme de jeux. Dans [ABdO03, ABdO05, BBS06b], nous avons proposé des techniques de résolution de ces jeux dans le cas de systèmes bien structurés.

3.2 Représentation symbolique des ensembles de configurations

3.2.1 Nouvelles représentations symboliques

Pour l'analyse des programmes manipulant des pointeurs, les techniques de vérification automatique sont encore dans une phase très exploratoire. Dans le cadre du projet PERSÉE, les techniques de *regular model checking* ont été mises en œuvre via des représentations linéaires spéciales des configurations des pointeurs [BHMV05]. Une autre approche est basée sur les SMS, une structure de données symbolique originale, à base de graphes pondérés par des expressions arithmétiques [BFN04].

Pour l'analyse de programmes récursifs multi-threads, les approches symboliques sont en général des extensions des pushdown-systems pouvant aller jusqu'au *process rewrite systems* de Mayr et au-delà. Ces extensions peuvent varier en complexité suivant qu'on autorise ou non la création dynamique de threads et qu'on permet plus ou moins de communication et de synchronisation entre les threads. Autour d'A. Bouajjani, les chercheurs de l'équipe Modélisation et Vérification ont contribué puissamment à cette direction de recherche [BT03, BET05, BM04, BT05, BMOT05].

3.2.2 Algorithmique des représentations symboliques

L'amélioration des performances de nos model-checkers passe aussi par les progrès algorithmiques au niveau des représentations symboliques.

Dans cette direction, le projet PERSÉE est à l'origine de deux résultats importants :

1. la mise au point par J.-M. Couvreur d'une notion d'*automates partagés*, une représentation canonique des automates finis déterministes qui permet de voir un automate comme le dag de ses composantes fortement connexes et de partager les sous-arbres identiques entre ses dags [Cou05].
2. l'étude fine de l'algorithmique des *Unambiguous Binary Automata* (UBA), cf. [FL05, FL04b, FL04a]. Cette étude a conduit à un résultat dérivé exceptionnel, la résolution par J. Leroux du problème classique de la synthèse efficace d'une formule de Presburger définissant une partie reconnaissable de $\mathbb{N}^m$ [Ler05].

Dans le cas de systèmes distribués, les techniques de réduction par ordres partiels sont cruciales pour le passage à l'échelle des model-checkers. La technique de dépliage, initialement développée pour la vérification des systèmes finis, a été étendue dans [HST07] aux systèmes infinis monotones.

3.2.3 Combinaison de représentations symboliques

L'analyse symbolique de systèmes manipulant des variables de différents types pose la question de combiner les représentations symboliques associées aux différents types. Cette question est bien

connue et soulève des problèmes algorithmiques ardus. Dans le cadre du model-checking symbolique, elle a été abordée sous l'angle des calculs de successeurs (ou prédécesseurs) immédiats, combinés aux tests d'inclusion et de vacuité.

Le projet PERSÉE a élargi cette question en prenant aussi en compte la dimension des algorithmes d'accélération. Ainsi, dans [BHJ03*, BH06] les techniques d'accélérations combinent les aspects discrets et les aspects continus de systèmes hybrides.

La problématique générale est considérée dans [BF04] où sont donnés des premiers résultats prometteurs sous la forme de critères génériques suffisants pour la combinaison effective de résultats d'accélération.

3.3 Abstractions et méthodes symboliques

Pour l'analyse de systèmes de grande taille, il est parfois indispensable de mettre en œuvre des techniques d'abstractions les plus automatiques possible.

Dans un cadre de *regular model-checking*, [HV05] montre comment des techniques de généralisation (ou d'apprentissage) d'automates à partir d'exemples et de contre-exemples permettent d'obtenir des approximations supérieures très pertinentes des ensembles d'accessibilité.

Dans le même cadre, [BHV04] montre comment combiner la démarche « *abstract–check–refine* » de [HJMS02*, HJMS03*] avec le *regular model checking*.

Des techniques de vérification symbolique et de calcul automatique d'abstraction ont été développées dans [AS07] pour l'analyse comportementale de systèmes hybrides paramétrés modélisant des réseaux (biologiques) de régulation génétique.

Pour les systèmes manipulant des compteurs, [Ler04] montre comment calculer automatiquement la meilleure approximation supérieure pouvant s'écrire comme combinaison booléenne de contraintes linéaires.

3.4 Environnement intégré pour la vérification symbolique

Un des objectifs du projet PERSÉE est de construire un outil de model-checking symbolique "ouvert" permettant de combiner (en les réutilisant) les structures de données, les représentations symboliques et les algorithmes, d'outils tels que TReX [ABS01*], FAST [BFLP03*] et Mec 5 [GV04] (pour commencer). Dans cette direction, les travaux réalisés sont les suivants :

- La spécification formelle des interfaces génériques et du langage de scripts pour les stratégies symboliques [BHS+05], ainsi qu'une étude comparative des techniques d'accélération de FAST et TReX [DFV05].
- L'extension du langage AltaRica [GV03*, GPV04] de façon à ce qu'il prenne en compte des types de données définies par l'utilisateur et puisse ainsi manipuler les modèles considérés au sein du projet [GP06, GPV06]. Un traducteur d'AltaRica vers FAST a été implémenté afin de permettre la vérification de modèles AltaRica infinis.
- La refonte des architectures logicielles de TReX et de FAST [BLP06] de façon à ce que ces outils s'adaptent à l'interface définie plus haut.

4 Autres éléments d'appréciation

4.1 Publications

D'ores et déjà, le projet Persée a publié 6 articles de journaux et plus de 40 communications dans des conférences internationales (cf. liste page 7). D'autres publications, en particulier dans des journaux, devraient paraître dans un futur proche.

Les journaux en question (*Information & Computation*, *ACM Trans. Computational Logic*, *Formal Methods in System Design*, *Theor. Comp. Sci.*, ...) sont parmi les plus prestigieux du domaine. Les conférences figurent parmi les plus réputées du domaine : 6 CAV, 5 ATVA, 4 TACAS, 3 FST&TCS, 2 CONCUR, 2 RTA, mais aussi LICS, FOSSACS, CSL, SAS.

4.2 Thèses et HDR soutenues

Six doctorants ont effectué leur thèse dans le cadre du projet Persée :

Nom	Localisation	Date début	Date soutenance
BARDIN Sébastien	LSV, Cachan	sep. 2002	oct. 2005 [Bar05]
BERTRAND Nathalie	LSV, Cachan	sep. 2003	sep. 2006 [Ber06]
MORO Pierre	LIAFA, Paris	oct. 2003	prévue en juin 2007
MEYER Antoine	LIAFA, Paris	oct. 2002	oct. 2005 [Mey05]
TRAN The Quang	LaBRI, Bordeaux	oct. 2004	prévue fin 2007
VINCENT Aymeric	LaBRI, Bordeaux	oct. 2000	déc. 2003 [Vin03]

Par ailleurs, J.-M. Couvreur, alors MdC Bordeaux, a effectué un séjour de deux ans en délégation à Cachan dans le cadre du projet Persée, au terme de laquelle il a soutenu son HDR [Cou04].

4.3 Événements organisés par le projet

La dynamique et les synergies instaurées par le projet PERSÉE nous ont conduit à organiser (ou participer à l'organisation de) plusieurs workshops autour de la thématique du projet, ainsi que d'autres événements scientifiques contribuant à la sa visibilité.

JSI 2005 : Le projet Persée a été l'organisateur des cinquièmes Journées Systèmes Infinis (JSI 2005), qui se sont tenues à Cachan les 10 et 11 mai 2005. Les JSI sont une manifestation irrégulière démarrée en 1998, qui permet de rassembler la communauté française travaillant sur la vérification des systèmes infinis. Nous renvoyons à `www.lsv.ens-cachan.fr/~phs/jsi2005.php` pour le programme des journées.

MOVEP 2006 : Les membres du projet PERSÉE ont co-organisé la septième édition de l'école d'été Modélisation et Vérification des Systèmes Parallèles 2006 (MOVEP 2006), qui s'est déroulée à Bordeaux du 19 au 23 juin 2006. MOVEP est une école "jeunes chercheurs" qui a lieu tous les deux ans depuis 1994. Cette édition a rassemblé 111 personnes, et le programme de l'école portait principalement sur la modélisation, la spécification et la vérification des systèmes (infinis) temps-réel et réactifs.

INFINITY 2003–2006 : INFINITY est un workshop annuel dédié à la vérification des modèles à infinité d'états ainsi qu'aux techniques symboliques associées. Il a lieu traditionnellement en satellite de la conférence CONCUR. Depuis 2003, le projet Persée a toujours été partie prenante de son comité de programme. En particulier, nous avons été responsable de l'organisation scientifique des éditions 2003 (Marseille) [Sch04] et 2006 (Bonn, Allemagne) [Bou07].

4.4 Mobilité interne au projet

Le projet PERSÉE a favorisé la mobilité entre les équipes participantes :
- J.-M. Couvreur, MdC Bordeaux au LaBRI, a effectué une délégation au CNRS au sein du LSV (de sep. 2002 à août 2004) ;
- J. Leroux, doctorant du LSV a rejoint le LaBRI en sep. 2005 via le concours de recrutement des CR CNRS.

5 Bibliographie du projet Persée

La bibliographie de ce rapport final recense toutes les publications issues du projet Persée, ainsi que quelques références (marquées d'un $*$) qui sont utilisées dans ce rapport sans être issues du projet.

[ABdO03] P. A. Abdulla, A. Bouajjani, and J. d'Orso. Deciding monotonic games. In *Proc. 17th Int. Workshop Computer Science Logic (CSL 2003) and 8th Kurt Gödel Coll. (KGL 2003), Vienna, Austria, Aug. 2003*, volume 2803 of *Lecture Notes in Computer Science*, pages 1–14. Springer, 2003.

[ABdO05] P. A. Abdulla, A. Bouajjani, and J. d'Orso. Monotonic and downward closed games. Long version of [ABdO03], August 2005.

[ABRS05] P. A. Abdulla, N. Bertrand, A. Rabinovich, and Ph Schnoebelen. Verification of probabilistic systems with faulty communication. *Information and Computation*, 202(2) :141–165, 2005.

[ABS01*] A. Annichini, A. Bouajjani, and M. Sighireanu. TReX : A tool for reachability analysis of complex systems. In *Proc. 13th Int. Conf. Computer Aided Verification (CAV 2001), Paris, France, July 2001*, volume 2102 of *Lecture Notes in Computer Science*, pages 368–372. Springer, 2001.

[ACBJ04] P. A. Abdulla, A. Collomb-Annichini, A. Bouajjani, and B. Jonsson. Using forward reachability analysis for verification of lossy channel systems. *Formal Methods in System Design*, 25(1) :39–65, 2004.

[AS07] M. Adélaïde and G. Sutre. Parametric analysis and abstraction of genetic regulatory networks. In *Proc. 2nd Workshop on Concurrent Models in Molecular Biology (BioCONCUR'04), London, UK, Aug. 2004*, Electronic Notes in Theor. Comp. Sci. Elsevier Science, 2007. To appear.

[Bar05] S. Bardin. *Vers un model checking avec accélération plate de systèmes hétérogènes*. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, October 2005.

[BBH+06] A. Bouajjani, M. Bozga, P. Habermehl, R. Iosif, P. Moro, and T. Vojnar. Programs with lists are counter automata. In *Proc. 18th Int. Conf. Computer Aided Verification (CAV 2006), Seattle, WA, USA, Aug. 2006*, volume 4144 of *Lecture Notes in Computer Science*, pages 517–531. Springer, 2006.

[BBS06a] C. Baier, N. Bertrand, and Ph. Schnoebelen. A note on the attractor-property of infinite-state Markov chains. *Information Processing Letters*, 97(2) :58–63, 2006.

[BBS06b] C. Baier, N. Bertrand, and Ph. Schnoebelen. On computing fixpoints in well-structured regular model checking, with applications to lossy channel systems. In *Proc. 13th Int. Conf. on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR 2006), Phnom Penh, Cambodia, Nov. 2006*, volume 4246 of *Lecture Notes in Artificial Intelligence*, pages 347–361. Springer, 2006.

[BBS06c] C. Baier, N. Bertrand, and Ph. Schnoebelen. Symbolic verification of communicating systems with probabilistic message losses : liveness and fairness. In *Proc. 26th IFIP WG6.1 Int. Conf. Formal Techniques for Networked and Distributed Systems (FORTE 2006), Paris, France, Sep. 2006*, volume 4229 of *Lecture Notes in Computer Science*, pages 212–227. Springer, 2006.

[BBS07] C. Baier, N. Bertrand, and Ph. Schnoebelen. Verifying nondeterministic probabilistic channel systems against ω-regular linear-time properties. *ACM Trans. Computational Logic*, 2007. To appear. Available at http://arxiv.org/abs/cs.LO/0511023.

[BDF04] S. Bardin, Ch. Darlot, and A. Finkel. FAST : un model-checker pour systèmes à compteurs. In J. Julliand, editor, *Actes du 6ème Atelier sur les Approches Formelles dans l'Assistance au Développement de Logiciels (AFADL 2004), Besançon, France, June 2004*, pages 377–380, June 2004.

[BE06] A. Bouajjani and J. Esparza. Rewriting models of boolean programs. In *Proc. 17th Int. Conf. Term Rewriting and Applications (RTA 2006), Seattle, WA, USA, Aug. 2006*, volume 4098 of *Lecture Notes in Computer Science*, pages 136–150. Springer, 2006.

[Ber06] N. Bertrand. *Modèles stochastiques pour les pertes de messages dans les protocoles asynchrones et techniques de vérification automatique*. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, September 2006.

[BESS05] A. Bouajjani, J. Esparza, S. Schwoon, and J. Strejček. Reachability analysis of multithreaded software with asynchronous communication. In *Proc. 25th Conf. Found. of Software Technology and Theor. Comp. Sci. (FST&TCS 2005), Hyderabad, India, Dec. 2005*, volume 3821 of *Lecture Notes in Computer Science*, pages 348–359. Springer, 2005.

[BET03*] A. Bouajjani, J. Esparza, and T. Touili. A generic approach to the static analysis of concurrent programs with procedures. *Int. J. Foundations of Computer Science*, 14(4) :551–582, 2003.

[BET05] A. Bouajjani, J. Esparza, and T. Touili. Reachability analysis of synchronized PA systems. In *Proc. 6th Int. Workshop on Verification of Infinite State Systems (INFINITY 2004), London, UK, Sep. 2004*, volume 138(3) of *Electronic Notes in Theor. Comp. Sci.*, pages 153–178. Elsevier Science, 2005.

[BF04] S. Bardin and A. Finkel. Composition of accelerations to verify infinite heterogeneous systems. In *Proc. 2nd Int. Symp. Automated Technology for Verification and Analysis (ATVA 2004), Taipei, Taiwan, Nov. 2004*, volume 3299 of *Lecture Notes in Computer Science*, pages 248–262. Springer, 2004.

[BFL04] S. Bardin, A. Finkel, and J. Leroux. FASTer acceleration of counter automata in practice. In *Proc. 10th Int. Conf. Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2004), Barcelona, Spain, Apr. 2004*, volume 2988 of *Lecture Notes in Computer Science*, pages 576–590. Springer, 2004.

[BFLP03*] S. Bardin, A. Finkel, J. Leroux, and L. Petrucci. FAST : Fast Acceleration of Symbolic Transition systems. In *Proc. 15th Int. Conf. Computer Aided Verification (CAV 2003), Boulder, CO, USA, July 2003*, volume 2725 of *Lecture Notes in Computer Science*, pages 118–121. Springer, 2003.

[BFLS05] S. Bardin, A. Finkel, J. Leroux, and Ph. Schnoebelen. Flat acceleration in symbolic model checking. In *Proc. 3rd Int. Symp. Automated Technology for Verification and Analysis (ATVA 2005), Taipei, Taiwan, Oct. 2005*, volume 3707 of *Lecture Notes in Computer Science*, pages 474–488. Springer, 2005.

[BFN04] S. Bardin, A. Finkel, and D. Nowak. Toward symbolic verification of programs handling pointers. In Ramesh R. Bharadwaj, editor, *Proc. 3rd Int. Workshop on Automated Verification of Infinite-State Systems (AVIS 2004), Barcelona, Spain, Apr. 2004*, 2004.

[BH06] B. Boigelot and F. Herbreteau. The power of hybrid acceleration. In *Proc. 18th Int. Conf. Computer Aided Verification (CAV 2006), Seattle, WA, USA, Aug. 2006*, volume 4144 of *Lecture Notes in Computer Science*, pages 438–451. Springer, 2006.

[BHJ03*] B. Boigelot, F. Herbreteau, and S. Jodogne. Hybrid acceleration using real vector automata. In *Proc. 15th Int. Conf. Computer Aided Verification (CAV 2003), Boulder, CO, USA, July 2003*, volume 2725 of *Lecture Notes in Computer Science*, pages 193–205. Springer, 2003.

[BHMV05] A. Bouajjani, P. Habermehl, P. Moro, and T. Vojnar. Verifying programs with dynamic 1-selector-linked structures in regular model checking. In *Proc. 11th Int. Conf. Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2005), Edinburgh, Scotland, UK, Apr. 2005*, volume 3440 of *Lecture Notes in Computer Science*, pages 13–39, 2005.

[BHRV06a] A. Bouajjani, P. Habermehl, A. Rogalewicz, and T. Vojnar. Abstract regular tree model checking. In *Proc. 7th Int. Workshop on Verification of Infinite State Systems (INFINITY 2005), San Francisco, CA, USA, Aug. 2005*, volume 149(1) of *Electronic Notes in Theor. Comp. Sci.*, pages 37–48. Elsevier Science, 2006.

[BHRV06b] A. Bouajjani, P. Habermehl, A. Rogalewicz, and T. Vojnar. Abstract regular tree model checking of complex dynamic data structures. In *Proc. 13th Int. Symp. Static Analysis (SAS 2006), Seoul, Korea, Aug. 2006*, volume 4134 of *Lecture Notes in Computer Science*, pages 52–70. Springer, 2006.

[BHS+05] S. Bardin, F. Herbreteau, M. Sighireanu, G. Sutre, and A. Vincent. Intégration des outils PERSÉE (proposition d'architecture). Livrable 3.1–Partie 1 du Projet PERSÉE de l'ACI Sécurité Informatique, June 2005. 35 pages.

[BHV04] A. Bouajjani, P. Habermehl, and T. Vojnar. Abstract regular model checking. In *Proc. 16th Int. Conf. Computer Aided Verification (CAV 2004), Boston, MA, USA, July 2004*, volume 3114 of *Lecture Notes in Computer Science*, pages 372–386. Springer, 2004.

[BLP06] S. Bardin, J. Leroux, and G. Point. FAST Extended Release. In *Proc. 18th Int. Conf. Computer Aided Verification (CAV 2006), Seattle, WA, USA, Aug. 2006*, volume 4144 of *Lecture Notes in Computer Science*, pages 63–66. Springer, 2006.

[BLW05] A. Bouajjani, A. Legay, and P. Wolper. Handling liveness properties in (omega-) regular model checking. In *Proc. 6th Int. Workshop on Verification of Infinite State Systems (INFINITY 2004), London, UK, Sep. 2004*, volume 138(3) of *Electronic Notes in Theor. Comp. Sci.*, pages 101–115. Elsevier Science, 2005.

[BM04] A. Bouajjani and A. Meyer. Symbolic reachability analysis of higher-order context-free processes. In *Proc. 24th Conf. Found. of Software Technology and Theor. Comp. Sci. (FST&TCS 2004), Chennai, India, Dec. 2004*, volume 3328 of *Lecture Notes in Computer Science*, pages 135–147. Springer, 2004.

[BMOT05] A. Bouajjani, M. Müller-Olm, and T. Touili. Regular symbolic analysis of dynamic networks of pushdown systems. In *Proc. 16th Int. Conf. Concurrency Theory (CONCUR 2005), San Francisco, CA, USA, Aug. 2005*, volume 3653 of *Lecture Notes in Computer Science*, pages 473–487. Springer, 2005.

[Bou06] A. Bouajjani. Regular model checking for programs with dynamic memory. In E. M. Clarke et al., editors, *Proc. NATO Advanced Research Workshop on Verification of Infinite State Systems with Applications to Security (VISSAS 2005), Timisoara, Romania, Mar. 2005*, pages 17–22. IOS Press, 2006.

[Bou07] A. Bouajjani, editor. *Proc. 8th Int. Workshop on Verification of Infinite State Systems (INFINITY 2006), Bonn, Germany, Aug. 2006*, Electronic Notes in Theor. Comp. Sci. Elsevier Science, August 2007. To appear.

[BP04] S. Bardin and L. Petrucci. From PNML to counter systems for accelerating Petri nets with FAST. In Ekkart Kindler, editor, *Proc. Workshop on Interchange Format for Petri Nets, Bologna, Italy, June 2004*, pages 26–40, 2004.

[BS04] N. Bertrand and Ph. Schnoebelen. Verifying nondeterministic channel systems with probabilistic message losses. In Ramesh R. Bharadwaj, editor, *Proc. 3rd Int. Workshop on Automated Verification of Infinite-State Systems (AVIS 2004), Barcelona, Spain, Apr. 2004*, 2004.

[BST07] A. Bouajjani, J. Strejček, and T. Touili. On symbolic verification of weakly extended PAD. In *Proc. 13th Int. Workshop on Expressiveness in Concurrency (EXPRESS 2006), Bonn, Germany, Aug. 2005*, Electronic Notes in Theor. Comp. Sci. Elsevier Science, 2007. To appear.

[BT03] A. Bouajjani and T. Touili. Reachability analysis of Process Rewrite Systems. In *Proc. 23rd Conf. Found. of Software Technology and Theor. Comp. Sci. (FST&TCS 2003), Mumbai, India, Dec. 2003*, volume 2914 of *Lecture Notes in Computer Science*, pages 74–87. Springer, 2003.

[BT05] A. Bouajjani and T. Touili. On computing reachability sets of process rewrite systems. In *Proc. 16th Int. Conf. Term Rewriting and Applications (RTA 2005), Nara, Japan, Apr. 2005*, volume 3467 of *Lecture Notes in Computer Science*, pages 484–499. Springer, 2005.

[CCG+05] S. Chaki, E. M. Clarke, O. Grumberg, J. Ouaknine, N. Sharygina, T. Touili, and H. Veith. State/event software verification for branching-time specifications. In *Proc. 5th Int. Conf. Integrated Formal Methods (IFM 2005), Eindhoven, The Netherlands, Nov.–Dec. 2005*, volume 3771 of *Lecture Notes in Computer Science*, pages 53–69. Springer, 2005.

[CCK+06] S. Chaki, E. M. Clarke, N. Kidd, Th. W. Reps, and T. Touili. Verifying concurrent message-passing C programs with recursive calls. In *Proc. 12th Int. Conf. Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2006), Vienna, Austria, Mar.-Apr. 2006*, volume 3920 of *Lecture Notes in Computer Science*, pages 334–349. Springer, 2006.

[Cou04] J.-M. Couvreur. *Contribution à l'algorithmique de la vérification*. Mémoire d'habilitation, Université de Bordeaux I, Bordeaux, France, July 2004.

[Cou05] J.-M. Couvreur. A BDD-like implementation of an automata package. In *Proc. 9th Int. Conf. Implementation and Application of Automata (CIAA 2004), Queen's University, Kingston, ON, Canada, July 2004*, volume 3317 of *Lecture Notes in Computer Science*, pages 310–311. Springer, 2005.

[DFGv06] S. Demri, A. Finkel, V. Goranko, and G. van Drimmelen. Towards a model-checker for counter systems. In *Proc. 4th Int. Symp. Automated Technology for Verification and Analysis (ATVA 2006), Beijing, ROC, Oct. 2006*, volume 4218 of *Lecture Notes in Computer Science*, pages 493–507. Springer, 2006.

[DFV05] Ch. Darlot, A. Finkel, and L. Van Begin. About Fast and TReX accelerations. In *Proc. 4th Int. Workshop on Automated Verification of Critical Systems (AVoCS 2004), London, UK, Sep. 2004*, volume 128(6) of *Electronic Notes in Theor. Comp. Sci.*, pages 87–103. Elsevier Science, 2005.

[FL04a] A. Finkel and J. Leroux. Image computation in infinite state model checking. In *Proc. 16th Int. Conf. Computer Aided Verification (CAV 2004), Boston, MA, USA, July 2004*, volume 3114 of *Lecture Notes in Computer Science*, pages 361–371. Springer, 2004.

[FL04b] A. Finkel and J. Leroux. Polynomial time image computation with interval-definable counters systems. In *Model Checking Software, Proc. 11th Int. SPIN Workshop, Barcelona, Spain, Apr. 2004*, volume 2989 of *Lecture Notes in Computer Science*, pages 182–197. Springer, 2004.

[FL05] A. Finkel and J. Leroux. The convex hull of a regular set of integer vectors is polyhedral and effectively computable. *Information Processing Letters*, 96(1) :30–35, 2005.

[GP06] A. Griffault and G. Point. On the partial translation of Lustre programs into the AltaRica language and vice versa. Technical Report 1415-06, LaBRI, Université de Bordeaux, 2006.

[GPV04] A. Griffault, G. Point, and A. Vincent. Vérification formelle des modèles AltaRica. In *Actes du Congrès LM (Maîtrise des risques et sûreté de fonctionnement, $\lambda\mu$14)*. Hermès, October 2004.

[GPV06] A. Griffault, G. Point, and A. Vincent. The grammar of the AltaRica language and its syntactic tree, March 2006. Available at `http://altarica.labri.fr/Doc/Syntax/`.

[GV03*] A. Griffault and A. Vincent. Vérification de modèles AltaRica. In *MAJECSTIC : Manifestation des jeunes chercheurs STIC, Marseille, Oct. 2003*, 2003.

[GV04] A. Griffault and A. Vincent. The mec 5 model-checker. In *Proc. 16th Int. Conf. Computer Aided Verification (CAV 2004), Boston, MA, USA, July 2004*, volume 3114 of *Lecture Notes in Computer Science*, pages 488–491. Springer, 2004.

[HJMS02*] T. A. Henzinger, R. Jhala, R. Majumdar, and G. Sutre. Lazy abstraction. In *Proc. 29th ACM Symp. Principles of Programming Languages (POPL 2002), Portland, OR, USA, Jan. 2002*, pages 58–70, 2002.

[HJMS03*] T. A. Henzinger, R. Jhala, R. Majumdar, and G. Sutre. Software verification with BLAST. In *Model Checking Software, Proc. 10th Int. SPIN Workshop, Portland, OR, USA, May 2003*, volume 2648 of *Lecture Notes in Computer Science*, pages 235–239. Springer, 2003.

[HST07] F. Herbreteau, G. Sutre, and T. Q. Tran. Unfolding concurrent well-structured transition systems. In *Proc. 13th Int. Conf. Tools and Algorithms for the Construction and Analysis*

of Systems (TACAS 2007), Braga, Portugal, Mar.-Apr. 2007, volume 4424 of *Lecture Notes in Computer Science*, pages 706–720. Springer, 2007.

[HV05] P. Habermehl and T. Vojnar. Regular model checking using inference of regular languages. In *Proc. 6th Int. Workshop on Verification of Infinite State Systems (INFINITY 2004), London, UK, Sep. 2004*, volume 138(3) of *Electronic Notes in Theor. Comp. Sci.*, pages 21–36. Elsevier Science, 2005.

[KS06] A. Kučera and Ph. Schnoebelen. A general approach to comparing infinite-state systems with their finite-state specifications. *Theoretical Computer Science*, 358(2–3) :315–333, 2006.

[Ler04] J. Leroux. Disjunctive invariants for numerical systems. In *Proc. 2nd Int. Symp. Automated Technology for Verification and Analysis (ATVA 2004), Taipei, Taiwan, Nov. 2004*, volume 3299 of *Lecture Notes in Computer Science*, pages 93–107. Springer, 2004.

[Ler05] J. Leroux. A polynomial time Presburger criterion and synthesis for number decision diagrams. In *Proc. 20th IEEE Symp. Logic in Computer Science (LICS 2005), Chicago, IL, USA, June 2005*, pages 147–156. IEEE Comp. Soc. Press, 2005.

[LS04] J. Leroux and G. Sutre. On flatness for 2-dimensional vector addition systems with states. In *Proc. 15th Int. Conf. Concurrency Theory (CONCUR 2004), London, UK, Aug.-Sep. 2004*, volume 3170 of *Lecture Notes in Computer Science*, pages 402–416. Springer, 2004.

[LS05] J. Leroux and G. Sutre. Flat counter automata almost everywhere ! In *Proc. 3rd Int. Symp. Automated Technology for Verification and Analysis (ATVA 2005), Taipei, Taiwan, Oct. 2005*, volume 3707 of *Lecture Notes in Computer Science*, pages 489–503. Springer, 2005.

[Mey04] A. Meyer. On term rewriting systems having a rational derivation. In *Proc. 7th Int. Conf. Foundations of Software Science and Computation Structures (FOSSACS 2004), Barcelona, Spain, Apr. 2004*, volume 2987 of *Lecture Notes in Computer Science*, pages 378–392. Springer, 2004.

[Mey05] A. Meyer. *Graphes infinis de présentation finie*. Thèse de doctorat, Univerisité de Rennes 1, France, October 2005.

[Sch04] Ph. Schnoebelen, editor. *Proc. 5th Int. Workshop on Verification of Infinite State Systems (INFINITY 2003), Marseille, France, Sep. 2003*, volume 98 of *Electronic Notes in Theor. Comp. Sci.* Elsevier Science, 2004.

[Tou06] T. Touili. Dealing with communication for dynamic multithreaded recursive programs. In E. M. Clarke et al., editors, *Proc. NATO Advanced Research Workshop on Verification of Infinite State Systems with Applications to Security (VISSAS 2005), Timisoara, Romania, Mar. 2005*, pages 213–227. IOS Press, 2006.

[TS07] T. Touili and M. Sighireanu. Bounded communication reachability analysis of process rewrite systems with ordered parallelism. In *Proc. 8th Int. Workshop on Verification of Infinite State Systems (INFINITY 2006), Bonn, Germany, Aug. 2006*, Electronic Notes in Theor. Comp. Sci. Elsevier Science, 2007. To appear.

[Vin03] A. Vincent. *Conception et réalisation d'un vérificateur de modèles AltaRica*. Thèse de doctorat, Laboratoire Bordelais de Recherche en Informatique, Université de Bordeaux 1, France, December 2003.