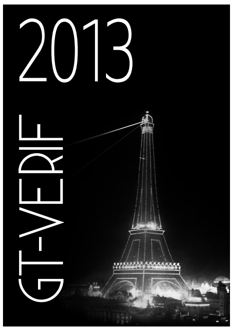


GT-Vérif

Journées annuelles 2013
ENS Cachan

Programme

Lundi 17 juin

9:30–9:45 Accueil

9:45–10 Mots de bienvenue

10–11 Exposé invité (chair: Véronique Cortier)

- Gilles Barthe, *Computer-Aided Cryptographic Proofs*

11–11:30 Pause café

11:30–12:30 Analyse de programmes (chair: Béatrice Bérard)

- Manamiary Bruno Andriamarina, *Formal Analysis of Distributed Algorithms using Refinement*
- Richard Genestier et Alain Giorgetti, *Deductive Verification of Iterators on Dyck Words*

12:30–14 Repas

14–16 Preuve et certification de programmes (chair: Gilles Barthe)

- Thomas Genet et Yann Salmon, *Analyse statique de programmes fonctionnels par automates d'arbres*
- Jad Hamza, *Verifying Concurrent Programs against Sequential Specifications*
- Amira Henaien, *Performing Implicit Induction Reasoning with a Certifying Proof Environment*
- Érik Martin-Dorel, *Vérification formelle de certificats fondés sur le lemme de Hensel*

16–16:30 Pause café

16:30–18 Systèmes distribués (chair: Denis Lugiez)

- Stefan Haar, *Observe and Derive*
- César Rodríguez, *Efficient Reachability of Petri Nets with Read Arcs*
- Rémy Chrétien, *From Security Protocols to Pushdown Automata*

20–23 Dîner au Bouillon Racine, 3 rue Racine, Paris 6e

Mardi 18 juin

8:30–9 Accueil

9–10 Exposé invité (chair: Sylvain Schmitz)

- Nathalie Bertrand, *Towards Parameterized Verification of Probabilistic Systems*

10–10:30 Pause café

10:30–12:30 Systèmes à compteurs (chair: Nathalie Bertrand)

- Amit Kumar Dhar, *On the Complexity of Verifying Regular Properties on Flat Counter Systems*
- Vincent Penelle, *On the Context-Freeness of Vector Addition Systems*
- Jérôme Leroux, *Presburger Vector Addition Systems*
- Christoph Haase, *Reachability in Register Machines with Polynomial Updates*

12:30–14 Repas

14–15:30 Logique temporelle, systèmes temporisés (chair: Nicolas Markey)

- Étienne Renault
- Aleksandra Jovanovic, *Parametric Interrupt Timed Automata*
- Paulin Fournier, *Parameterized Verification of Networks with many Identical Probabilistic Timed Processes*

15:30–16 Pause café

16–17 Logique de stratégie (chair: Catalin Dima)

- Bastien Maubert, *Uniform Strategies with Rational Relations*
- Sophie Pinchinat, *Extensions of the μ-Calculus for Strategic Reasoning*

Résumés

- Gilles Barthe, *Computer-Aided Cryptographic Proofs*

  EasyCrypt is a tool for constructing and verifying cryptographic proofs. EasyCrypt can be used as a stand-alone application, or as a verifying back-end for cryptographic compilers. The presentation will outline the language-based methods that underlie the design of EasyCrypt and illustrate some of their applications. If time allows, I will present ZooCrypt, an automated tool for analyzing the security of padding-based public-key encryption schemes (i.e. schemes built from trapdoor permutations and hash functions).

  More info at `http://www.easycrypt.info` and `http://zoo.easycrypt.info`.

- Manamiary Bruno Andriamarina, *Formal Analysis of Distributed Algorithms using Refinement*

  Distributed algorithms tend to become increasingly complex: the distributed systems, in which these algorithms are running, may change over time, react to environment factors, etc. Moreover, distributed algorithms exhibit non-functional properties that need to be taken into account. Therefore, the formal verification of distributed algorithms becomes difficult. The combination of refinement and temporal formalisms, by the means of the correct-by-construction, call-as-event and service-as-event emerges as a promising approach for the formal analysis of these algorithms. We abstract the behaviours and services provided by the algorithms using simple liveness properties and then, add details to them with refinement.

  Joint work with Dominique Méry and Neeraj Kumar Singh.

- Richard Genestier et Alain Giorgetti, *Deductive Verification of Iterators on Dyck Words*

  One challenge in software engineering is to design and implement efficient algorithms for automated test generation. We focus on unitary testing of functions whose parameters are complex data structures (arrays, lists, trees, etc) satisfying some properties. The effectiveness of algorithms generating these test data depends on their capacity to avoid producing data that do not satisfy these properties. Among these algorithms, we focus on iterators, producing one after another all data with a given (small) size, because they are often sufficient to detect coding errors, while providing counterexamples of minimal size. We propose to check C or Java implementations of these algorithms by deductive verification, with as much automation support as available in the most recent proving tools.

  Well-balanced parenthesis words (aka. Dyck words) are typical structures underlying structured documents. We present an encoding of Dyck words by arrays of integers with structural properties, a C implementation of an iterator on these arrays, and an ACSL formal specification of their properties. We show how to adapt this code and its specification to the automated proof capabilities of the most recent release of the WP plugin of the frama-c verification tool, with the help of Why3 and SMT solvers.

- Thomas Genet et Yann Salmon, *Analyse statique de programmes fonctionnels par automates d'arbres*

  La complétion d'automates d'arbres est une technique permettant d'approcher l'ensemble des termes accessibles par réécriture. On peut voir la complétion d'automate comme une technique d'ARTMC (Abstract Regular Tree Model Checking) particulière. Si l'on code un programme fonctionnel (pur) par un système de réécriture, la complétion permet d'obtenir un sur-ensemble des résultats de ce programme, i.e. une sur-approximation de l'image de cette fonction. Actuellement, nous étudions l'application de ce principe à l'analyse statique de langages comme Ocaml. A terme, l'objectif sera de proposer un mécanisme de vérification complétant l'inférence de type. Sur la route, plusieurs défis sont à relever: garantir la terminaison et la précision de l'analyse, prendre en compte les stratégies d'évaluation, prendre en compte l'ordre supérieur, prendre en compte les types built-ins, automatiser la transformation de Ocaml vers les systèmes de réécriture, etc. Concernant ces problèmes, je présenterai l'état des lieux de nos réflexions et travaux ainsi que les questions encore ouvertes.

- Jad Hamza, *Verifying Concurrent Programs against Sequential Specifications*

  We investigate the algorithmic feasibility of checking whether concurrent implementations of shared-memory objects adhere to their given sequential specifications; sequential consistency, linearizability, and conflict serializability are the canonical variations of this problem. While verifying sequential consistency of systems with unbounded concurrency is known to be undecidable, we demonstrate that conflict serializability, and linearizability with fixed linearization points are EXPSPACE-complete, while the general linearizability problem is undecidable.

  Our (un)decidability proofs, besides bestowing novel theoretical results, also reveal novel program explorations strategies. For instance, we show that every violation to conflict serializability is captured by a conflict cycle whose length is bounded independently from the number of concurrent operations. This suggests an incomplete detection algorithm which only remembers a small subset of conflict edges, which can be made complete by increasing the number of remembered edges to the cycle-length bound. Similarly, our undecidability proof for linearizability suggests an incomplete detection algorithm which limits the number of "barriers" bisecting non-overlapping operations. Our decidability proof of bounded-barrier linearizability is interesting on its own, as it reduces the consideration of all possible operation serializations to numerical constraint solving. The literature seems to confirm that most violations are detectable by considering very few conflict edges or barriers.

  Joint work with Ahmed Bouajjani, Michael Emmi, and Constantin Enea.

- Amira Henaien, *Performing Implicit Induction Reasoning with a Certifying Proof Environment*

  The induction-based proving techniques are fully adapted to reason on unbounded and recursive data structures. We propose a way to automatically generate and certify induction proofs, as those produced by the Spike automated theorem prover, using a new tactic for the certifying proof environment of the Coq proof assistant. The tactic is able to automatically prove conjectures whose proofs require mutual induction as well as non-trivial and multiple induction steps.

Joint work with Sorin Stratulat.

- Érik Martin-Dorel, *Vérification formelle de certificats fondés sur le lemme de Hensel*

  Dans cet exposé, je présenterai les travaux effectués dans le cadre du projet TaMaDi (`http://tamadi.gforge.inria.fr/`) visant à certifier formellement les résultats des algorithmes conçus pour trouver les pires cas pour l'arrondi correct des fonctions mathématiques. Les calculs menant à ces pires cas sont très longs (plusieurs années×CPU) et sont effectués en utilisant des programmes largement optimisés qui implantent des algorithmes très complexes. D'où l'intérêt d'utiliser un outil formel d'aide à la preuve tel que le logiciel COQ, afin de garantir formellement la correction de ces données numériques.

  Dans ce travail, nous nous intéressons en particulier à l'algorithme Stehlé-Lefèvre-Zimmermann, qui consiste en une phase de découpage du domaine et d'approximation polynomiale, suivie de la résolution de myriades d'instances du problème ISValP (Integer Small Value Problem), qui revient grosso modo à trouver toutes les petites valeurs d'un polynôme à coefficients entiers, modulo un grand entier. La dernière étape de ces calculs s'appuie notamment sur la version bivariée du lemme de Hensel.

  Le lemme de Hensel est un outil clé en calcul formel qui, étant donné un polynôme sur les entiers et une racine modulo un nombre premier p, construit itérativement des racines modulo p^{2^k}, sous des hypothèses faciles à vérifier. La force du lemme de Hensel réside notamment en la présence d'une assertion d'existence (il existe un relèvement) et d'unicité (ce relèvement est unique). Nous avons formalisé ce dernier résultat (dans les cas univarié ainsi que bivarié) au sein d'une bibliothèque pour l'assistant de preuves COQ.

  En s'appuyant sur ces preuves formelles, nous avons conçu puis formellement prouvé un vérificateur de certificats pour le problème ISValP. Nous avons également rendu effectif ce vérificateur de certificats, dont je présenterai plusieurs benchmarks.

  Il s'agit d'un travail en commun avec Guillaume Hanrot, Micaela Mayero et Laurent Théry.

- Stefan Haar, *Observe and Derive*

  Complex systems often need to be monitored by a supervisor that has only a partial view of events occurring in the system. Partially observable automata or Petri nets are natural models for these situations. Among the problems to be solved in this context, we will focus on (event) diagnosis and diagnosability: given a stream of observations, is it possible to detect occurrence of specific unobservable events (faults) from the observation alone?

  We will recall some of the existing approaches and investigate more closely the situation for partial order semantics for distributed systems, in the light of recent results on "reveals" relations.

- César Rodríguez, *Efficient Reachability of Petri Nets with Read Arcs*

  Model checking is a practical way of ensuring the correctness of concurrent systems, but suffers from the problem of state-space explosion (SSE). In this talk we discuss three sources of SSE and propose methods to cope with them.

  One source of SSE is the explicit representation of concurrent actions by their interleavings. Petri nets are a modelling language for concurrent systems, and their unfoldings are a well-established approach for coping with this source of SSE. In a precise sense, an unfolding is a partial order that compactly represents the reachable markings of a net, where concurrent actions are left unordered.

  Another source of SSE is concurrent read access to shared resources, where concurrent actions check that a resource is available without consuming it. Petri net models of such system can only consume and produce the resource to model such behaviour, entailing a loss of concurrency between the readers. As a consequence, the unfolding explicitly represents the interleavings of the readers. Contextual nets (c-nets) extend Petri nets with read arcs, which let transitions to check for the presence of tokens without consuming them. They adequately model concurrent read access and their unfoldings are smaller in these cases.

  A third source of SSE is sequences of choices. Here, the system visits a sequence of states making conflicting choices on the way from one state to the next. Unfoldings are tree-like structures that represent such exponentially many choices as different branches. Merged Processes have been proposed as solution for this. They 'fold back' those branches, often producing a condensed representation orders of magnitude smaller than the unfolding.

  In this talk, we propose an efficient method for constructing contextual unfoldings, and report on experiments performed with a tool implementing it. We next focus on the analysis of c-nets by means of their unfoldings. We sketch an encoding of the deadlock and coverability problems into SAT, and compare the performance of our method and other unfolding-based verification tools.

  Finally, we present Contextual Merged Processes (CMPs), a technique that integrates contextual unfoldings and merged processes, coping with the three aforementioned sources of SSE. We discuss reachability algorithms for CMPs and present experimental evidence showing that the approach is practical.

- Rémy Chrétien, *From Security Protocols to Pushdown Automata*

  Formal methods have been very successful in analyzing security protocols for reachability properties such as secrecy or authentication. In contrast, there are very few results for equivalence-based properties, crucial for studying e.g. privacy-like properties such as anonymity or vote secrecy.

  We study the problem of checking equivalence of security protocols for an unbounded number of sessions. Since replication leads very quickly to undecidability (even in the simple case of secrecy), we focus on a limited fragment of protocols (standard primitives but pairs, one variable per protocol's rules) for which the secrecy preservation problem is known to be decidable. Surprisingly, this fragment turns out to be undecidable for equivalence. Then, restricting our attention to deterministic protocols, we propose the first decidability result for checking equivalence of protocols for an unbounded number of sessions. This result is obtained through a characterization of equivalence of protocols in terms of equality of languages of (generalized, real-time) deterministic pushdown automata.

Joint work with Véronique Cortier and Stéphanie Delaune.

- Nathalie Bertrand, *Towards Parameterized Verification of Probabilistic Systems*

  On the one hand, model-checking of finite probabilistic systems (Markov chains and Markov decision processes) is now well-established. The traditional questions concern the verification of these models against probabilistic logics. We distinguish qualitative questions—that compare probabilities to the extreme values 0 and 1—and quantitative ones—for which the thresholds are arbitrary.

  On the other hand, parameterized verification (dating back the 80's) aims at checking at once many instances of a problem. This reasoning is typically useful when one considers protocols that execute over networks of many identical processes: one wants to verify the protocol for all possible number of processes. As an example, parameterized verification has been recently studied in the context of ad hoc networks.

  We will start the talk by reviewing fundamental results about probabilistic model-checking as well as parameterized model-checking. Then, we will expose the problem of parameterized verification of probabilistic systems which encompasses the two approaches, and provide preliminary results on the subject.

- Amit Kumar Dhar, *On the Complexity of Verifying Regular Properties on Flat Counter Systems*

  Among the approximation methods for the verification of counter systems, one of them consists in model-checking their flat unfoldings. Unfortunately, the complexity characterization of model-checking problems for such operational models is not always well studied except for reachability queries or for Past LTL. In this paper, we characterize the complexity of model-checking problems on flat counter systems for the specification languages including first-order logic, linear mu-calculus, infinite automata, and related formalisms. Our results span different complexity classes (mainly from PTime to PSpace) and they apply to languages in which arithmetical constraints on counter values are systematically allowed. As far as the proof techniques are concerned, we provide a uniform approach that focuses on the main issues.

  Joint work with Stéphane Demri and Arnaud Sangnier.

- Vincent Penelle, *On the Context-Freeness of Vector Addition Systems*

We revisit the proof of decidability of the context-freeness of vector addition systems, giving a quite short proof. This talk is inspired from a paper accepted at LICS 2013 which is a joint work with Jérôme Leroux and Grégoire Sutre.

- Jérôme Leroux, *Presburger Vector Addition Systems*

  The reachability problem for Vector Addition Systems (VAS) is a central problem of net theory. The problem is known to be decidable by inductive invariants definable in the Presburger arithmetic. When the reachability set is definable in the Presburger arithmetic, the existence of such an inductive invariant is immediate. However, in this case, the computation of a Presburger formula denoting the reachability set is an open problem. In this paper we close this problem by proving that if the reachability set of a VAS is definable in the Presburger arithmetic, then the VAS is flatable, i.e. its reachability set can be obtained by runs labeled by words in a bounded language. As a direct consequence, classical algorithms based on acceleration techniques effectively compute a formula in the Presburger arithmetic denoting the reachability set.

- Christoph Haase, *Reachability in Register Machines with Polynomial Updates*

  In this talk I will introduce a class of register machines whose registers range over the integers and can be updated by polynomial functions when a transition is taken. In addition, the domain of the registers can be constrained by linear constraints. This model generalises a variety of known models such as VASS. The main result I am going to present is that reachability is PSpace-complete in the presence of a single register. I will also discuss some undecidability results in the presence of more registers.

  Joint work with Alain Finkel and Stefan Göller.

- Étienne Renault, *Strength-Based Decomposition of the Property Büchi Automaton for Faster Model Checking*

  The automata-theoretic approach for model checking of linear-time temporal properties involves the emptiness check of a large Büchi automaton. Specialized emptiness-check algorithms have been proposed for the cases where the property is represented by a weak or terminal automaton.

  When the property automaton does not fall into these categories, a general emptiness check is required. This paper focuses on this class of properties. We refine previous approaches by classifying strongly-connected components rather than automata, and suggest a decomposition of the property automaton into three smaller automata capturing the terminal, weak, and the remaining strong behaviors of the property. The three corresponding emptiness checks can be performed independently, using the most appropriate algorithm.

  Such a decomposition approach can be used with any automata-based model checker. We illustrate the interest of this new approach using explicit and symbolic LTL model checkers.

  Joint work with Alexandre Duret-Lutz, Fabrice Kordon, and Denis Pointrenaud.

- Aleksandra Jovanovic, *Parametric Interrupt Timed Automata*

  Parametric reasoning is particularly relevant for timed models, but very often leads to undecidability of reachability problems. We propose a parametrised version of Interrupt Timed Automata (an expressive model incomparable to Timed Automata), where polynomials of parameters can occur in guards and updates. We prove that different reachability problems, including robust reachability, are decidable for this model, and we give complexity upper bounds for a fixed or variable number of clocks and parameters.

  Joint work with Béatrice Bérard, Serge Haddad, and Didier Lime

- Paulin Fournier, *Parameterized Verification of Networks with many Identical Probabilistic Timed Processes*

  Parameterized verification aims at certifying infinite-state models by verifying systems independently of the number of processes involved. We introduce a new model Probabilistic timed networks, and show undecidability (resp. decidabilty) of quantitative verification problems in the case without (resp. with) mobility.

- Bastien Maubert, *Uniform Strategies with Rational Relations*

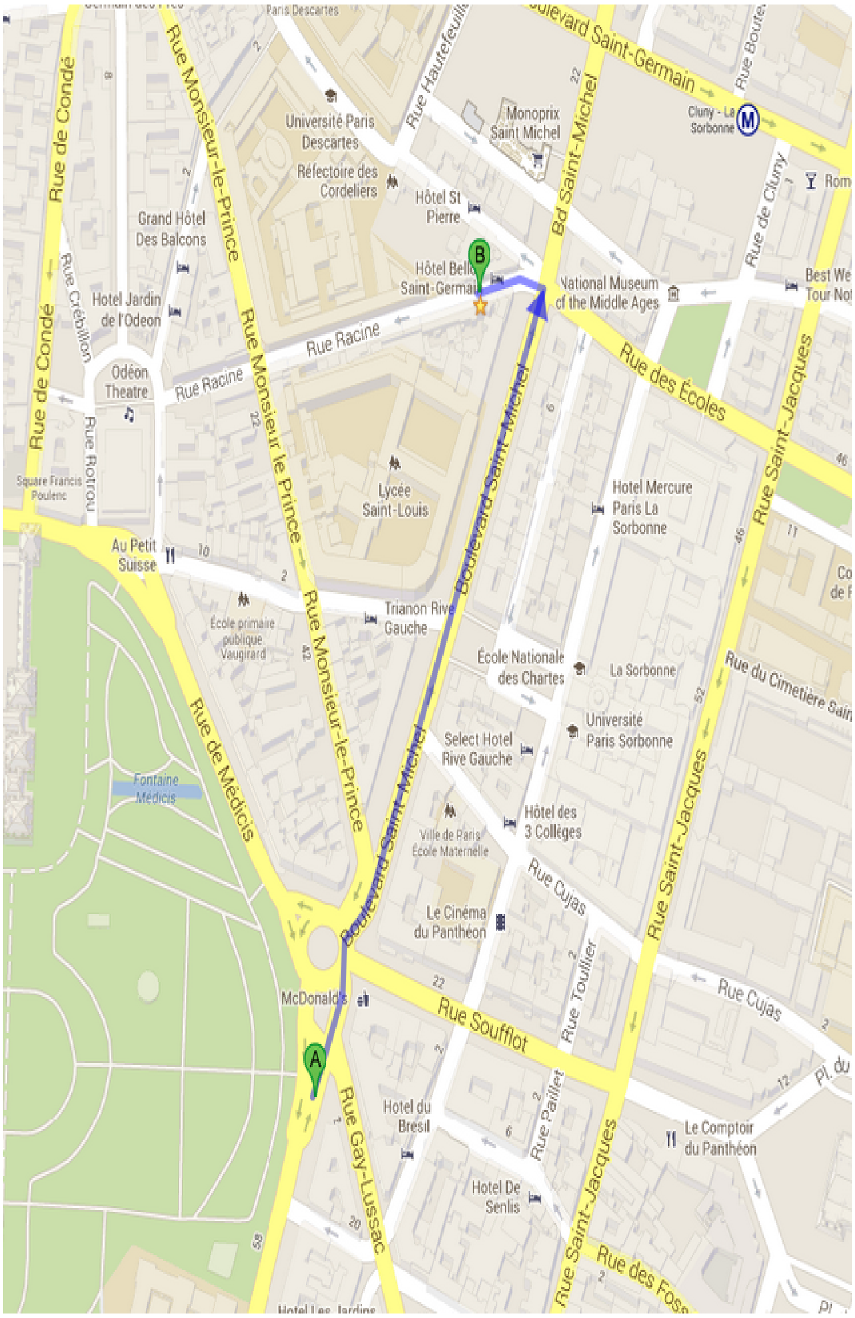
  We study a general notion of uniform strategies that subsumes several existing notions of strategies subject to some uniformity constraints, like for example in games with imperfect information or model checking games for dependence logic. We present a logical language to specify such uniformity constraints. This language is basically LTL augmented with a knowledge-like operator R, where R phi means that phi holds in all related plays. One particularity of this work concerns the semantics of the R modality. Instead of choosing a specific relation over plays, like synchronous perfect-recall for example, we allow for any binary rational relation. This class of relations is very general, and in particular it contains all relations classically used in games with imperfect information and logics of knowledge and time (perfect/imperfect recall, synchronous/asynchronous...). Rational relations are recognized by finite state transducers, which allows us to study the decidability and complexity of synthesizing uniform strategies for different subclasses of rational relations. Our results imply the decidability of the model checking of LTLKn with asynchronous perfect recall, and more generally we have that the strategy problem in games with a winning condition expressed in LTLK is decidable as long as the relation that represents the knowledge is rational.

- Sophie Pinchinat, *Extensions of the μ-Calculus for Strategic Reasoning*

  We study the state of the art of a family of logics for the qualitative analysis of multi-agent systems in the perfect information setting in terms of the mu-calculus logic, and we introduce some possible extensions to handle imperfect information.

Dîner du 17 juin

Le dîner des journées est organisé au *Bouillon Racine* à 20h le 17 juin (B sur la carte ci-dessous). La station la plus proche est le RER B à l'arrêt *Luxembourg* (A sur la carte). Un départ groupé sera possible à 19h15 depuis l'ENS de Cachan.


B
A
Rue de Condé
Rue Monsieur-le-Prince
Université Paris Descartes
Réfectoire des Cordeliers
Rue Hautefeuille
Monoprix Saint Michel
Boulevard Saint-Germain
Cluny - La Sorbonne
M
Rue Boutebrie
Rue de Cluny
Hôtel St Pierre
Grand Hôtel Des Balcons
Hotel Jardin de l'Odeon
Rue Crébillon
Hôtel Belloy Saint-Germain
Bd Saint-Michel
National Museum of the Middle Ages
Best Western Tour Notre-Dame
Rue Racine
Odéon Theatre
Rue des Écoles
Rue Saint-Jacques
Rue Rotrou
Square Francis Poulenc
Lycée Saint-Louis
Boulevard Saint-Michel
Hotel Mercure Paris La Sorbonne
Au Petit Suisse
École primaire publique Vaugirard
Trianon Rive Gauche
École Nationale des Chartes
La Sorbonne
Rue du Cimetière Saint-Benoît
Université Paris Sorbonne
Select Hotel Rive Gauche
Rue de Médicis
Fontaine Médicis
Hôtel des 3 Collèges
Ville de Paris École Maternelle
Rue Cujas
Le Cinéma du Panthéon
Rue Toullier
McDonald's
Rue Soufflot
Rue Gay-Lussac
Hotel du Bresil
Rue Paillet
Le Comptoir du Panthéon
Hotel De Senlis
Rue des Fossés
Hotel Les Jardins