Monday, May 29th – Lundi 29 mai

10:30 Accueil

Session *Transducers*

11:00 Emmanuel Filliot

A decidable logic for transductions of finite words

Transductions are binary relations of finite words. After introducing the main computational models for transductions, namely transducers, the talk will survey known connections with a logical model based on monadic-second order logic, defined by Courcelle in the context of graphs. A new logic, tailored to transductions of finite words, is presented, as well as its applications to model-checking and synthesis of transducers. Finally, an equivalence with a (decidable) logic for data words (words over infinite alphabets) is given.

12:00 Bruno Guillon

Which classes of origin graphs are generated by transducers?

This talk is about transductions, which are binary relations on words. We are interested in various models computing transductions (ie, transducers), namely two-way automata with outputs, streaming string transducers and string-to-string MSO transductions. We observe that each of these formalisms provides more than just a set of pairs of words. Indeed, one can also reconstruct origin information, which says how positions of the output string originate from positions of the input string. On the other hand, it is also possible to provide any pair of words in a relation with an origin mapping, indicating an origin input position for each output position, in a similar way. This defines a general object called origin graph. We characterise the families of origin graphs which corresponds to the semantics of some classical models of transducer. We also prove the decidability of the MSO satisfiability problem on the classes of origin graphs generated by streaming string transducers or equivalently by string-to-string MSO transductions.
This is joint work with Mikołaj Bojańczyk, Laure Daviaud and Vincent Penelle.

12:30 Lunch

Bâtiment P, salle P1 008

Session *Probabilities and Logic*

14:30 Matteo Mio

Riesz Modal Logic for Markov Processes

We investigate a modal logic for expressing properties of Markov processes whose semantics is real-valued, rather than Boolean, and based on the mathematical theory of Riesz spaces (lattice ordered vector spaces). We use the duality theory of Riesz spaces to provide a connection between Markov processes and the logic. This takes the form of a duality between the category of coalgebras of the Radon monad (modeling Markov processes) and the category of a new class of algebras (algebraizing the logic) which we call modal Riesz spaces. As a result, we obtain a sound and complete axiomatization of the Riesz Modal logic.

15:30 Valeria Vignudelli

Bisimulations for probabilistic higher-order languages

In this talk we present techniques for proving behavioral equivalence in languages with both probabilistic and higher-order operators. In particular, we focus on bisimulations for probabilistic lambda-calculi, and on the problem of deriving proof techniques that are fully abstract with respect to contextual equivalence. As representative calculi, probabilistic call-by-name and call-by-value lambda-calculus, and a probabilistic (call-by-value) lambda-calculus extended with references (i.e., a store) are considered. Full abstraction results for probabilistic environmental bisimilarity are derived in each case.

16:00 Break

16:30 Paulin Fournier

Automates alternants probabilistes pour la satisfiabilité de $PCTL^*$

Nous étudions la satisfaibilité de la logique $PCTL^*$. Cette logique permet de combiner des opérateurs temporels ainsi que des quantificateurs de chemins qui peuvent être déterministes (il existe un chemin ou pour tout chemin) ou probabilistes (par exemple : pour un ensemble de chemins de mesure positive). Pour résoudre ce problème pour le fragment qualitatif de la logique nous introduisons des automates alternant avec des conditions de gains probabilistes et déterministes. Nous montrons que pour la classe d'automates ainsi obtenue le problème du vide est décidable. Nous obtenons donc une procédure de décision pour la satisfiabilité de $PCTL^*$ en 3-NEXPTIME.

17:00 Etienne Lozes

Synchronizability of Communicating Finite State Machines is not decidable

Communicating Finite State Machines (CFSM) are a simple model of agents that exchange messages through asynchronous communication channels. This model has been widely used e.g for modeling and analyzing web services, systems on cheap, parallel computing, etc. If the communications were synchronous, or if the communication channels were bounded, these systems would be relatively easy to analyse, but the unboundedness of the communication channels make them a Turing complete computational model. A tempting approach for analyzing such systems is therefore to assume that they are slack elastic, i.e. that their behavior is the same whether communications are synchronous or asynchronous. Synchronizablility is a special form of slack elasticity where the observed behavior is the trace semantics of the systems restricted to the send actions. The question whether a given CFSM is synchronizable was claimed decidable in several papers, either for peer-to-peer, socket-like (1-1) channels, or for mailbox. Erlang-like ($*-1$) channels, or for unordered (bag) channels. The claim relied every time on a form of small model property.
We will show that this small model property actually does not hold, for none of these models of channels. This raises again the question of the decidability of synchronizability. We will show that, for the peer-to-peer (1-1) model, synchronizability actually is undecidable. Somehow repairing the original proof, we will show that synchronizability can be decided for a ring-like communication topology. Finally, we will also discuss the decidability of synchronzability for the other models of channels.
This is a joint work with Alain Finkel.

17:30 Vincent Jugé

Courcelle's theorem made dynamic

Dynamic complexity is concerned with the complexity of updating a solution to a problem when its input changes. A typical example is as follows: given an directed graph G and two pointed vertices s and t, you wish to know whether there exists a path from s to t in G. After your computation is complete, the graph is modified (e.g. by adding or deleting an edge): how should you proceed to update your answer at the least cost? Computing and storing auxiliary data, such as maintaining a covering forest, might be helpful in that regard.
In this talk, we will consider a specific class for dynamic complexity, called DynFO. A dynamic problem belongs to this class if updates can be performed by applying first-order formulas. We will show that a dynamic variant of Courcelle's theorem belongs to DynFO (with some mild precomputation step), and we will apply this result to computing optimal strategies in 2-player reachability or parity games.
This talk is based on joint a work with Patricia Bouyer-Decitre and Nicolas Markey.

Tuesday, May 30th – Mardi 30 mai

Session *Databases*

10:00 Amélie Gheerbrant

Incomplete information in databases

The talk will survey the state of the art and new challenges regarding incomplete information in databases. The focus will be on relational data and no prior knowledge of the domain will be assumed.

11:00 Break

11:30 Paolo Guagliardo

Correct Answers to SQL Queries on Databases with Nulls

Multiple issues with SQL's handling of nulls have been well documented. Having efficiency as its key goal, SQL disregards the standard notion of correctness on incomplete databases – certain answers – due to its high complexity. As a result, it may produce answers that are just plain wrong. It was recently shown that SQL evaluation can be modified, at least for first-order queries, to return only correct answers. But while these modifications came with good theoretical complexity bounds, they have not been tested in practice.
In this talk I will show that, for some typical SQL queries involving negation in real-world scenarios, wrong answers are very common. On the other hand, existing solutions for fixing the problem do not work in practice at all. By analyzing the reasons for this, we come up with a new modified way of rewriting SQL queries that restores correctness. We conduct experiments that show the feasibility of our solution: the small price tag it imposes can be often tolerated to ensure correct results, and we do not miss correct answers that the usual SQL evaluation produces. The overall conclusion is that correct evaluation can be realistically achieved in the presence of nulls, at least for the SQL fragment that corresponds to first-order queries.

12:00 Xiao XU

Alternating Data Automata

Alternating automata have been widely used to model and verify systems that handle data from finite domains, such as communication protocols or hardware. The main advantage of the alternating model of computation is that complementation is possible in linear time, thus allowing to concisely encode trace inclusion problems that occur often in verification. In this presentation, we consider alternating automata over infinite alphabets, whose transition rules are formulae in a combined theory of booleans and some infinite data domain, that relate past and current values of the data variables. The data theory is not fixed, but rather it is a parameter of the class. We show that union, intersection and complementation are possible in linear time in this model and, though the emptiness problem is undecidable, we provide two efficient semi-algorithms, inspired by two state-of-the-art abstraction refinement model checking methods: lazy predicate abstraction and the Impact semi-algorithm.

12:30 Lunch

Bâtiment P, salle P1-008

Session *Games and verification*

14:30 Laurent Doyen

Two-player games in system design

We present an introduction on two-player games in system design. Using reachability and safety games with perfect information, We discuss their fundamental properties, and basic ingredients for algorithmic solutions and complexity analysis.
We present two applications in automatic system design and verification to illustrate the need to consider games with partial observation, and we discuss the main differences as compared to perfect-information games, such as determinacy, power of randomization, complexity and algorithmic analysis.

15:30 David Auger

Une famille générique d'algorithmes d'itération de stratégies pour les jeux stochastiques simples

Les jeux stochastiques simples (Simple Stochastic Games, SSGs) forment une classe de jeux à somme nulle qui se jouent "à deux joueurs et demi". Les joueurs y prennent des décisions à tour de rôle, et le système change alors d'état suivant la décision prise et un facteur aléatoire. L'objectif d'un joueur est d'atteindre un certain état du jeu, et celui de l'autre joueur est de l'en empêcher, et plus globalement de trouver des stratégies qui maximisent/minimisent la probabilité d'atteindre cet état. Hormis le fait qu'elle permet de généraliser la notion de processus de décision markovien (MDP) à un contexte antagoniste, cette classe de jeux a reçu beaucoup d'attention de par la complexité algorithmique de sa résolution qui se situe dans les classes de complexité NP et co-NP, sans pour autant qu'on connaisse à l'heure actuelle d'algorithme pouvant les résoudre en temps polynomial. D'autre part, la majorité des autres classes de jeux se situant dans les classes NP et co-NP (e.g. Parity Games, Mean-payoff- Games) peuvent se réduire aux SSGs en temps polynomial. De fait, de nombreux algorithmes ont été proposés pour les SSGs, dont de nombreux algorithmes dits d'itération de stratégie. Dans cette présentation nous décrivons une vision unificatrice qui englobe la plupart de ces algorithmes (comme par exemple l'agorithme de Hoffman-Karp) et en génère également de nouveaux, ce schéma général pouvant également être utilisé pour fournir des algorithmes à complexité paramétrée pour les SSGs.

16:00 Break

16:30 Santosh Arvind Adimoolam

Augmented complex zonotopes for computing invariants of affine hybrid systems

We present the set representation called complex zonotopes and its generalization called augmented complex zonotopes for verification of discrete time affine hybrid systems. Complex zonotopes are a generalization of simple (usual) zonotopes to incorporate the possibly complex eigenstructure of linear maps during invariant computation. This allows to capture the some contractive directions of the dynamics while computing invariants, in the presence of complex eigenstructure. The augmented form of complex zonotopes has an additional facility that allows computing or reasonably over-approximating intersections with the linear guards and staying conditions that control transitions in the hybrid system. In our work, we derive a set of second-order conic constraints solved in a single convex optimization set to compute an augmented complex zonotope, an approach which, unlike the step-by-step reachability computation techniques, avoids the wrapping effect. To demonstrate the efficiency of our approach, we present results on three benchmark examples from literature and compare it with the implementation on the SpaceEx tool and other available results.

17:00 Damien Busatto-Gaston

Optimal Reachability in Divergent Weighted Timed Games

Weighted timed games are played by two players on a timed automaton equipped with weights: one player wants to minimise the accumulated weight while reaching a target, while the other has an opposite objective. Used in a reactive synthesis perspective, this quantitative extension of timed games allows one to measure the quality of controllers. Weighted timed games are notoriously difficult and quickly undecidable, even when restricted to non-negative weights. Decidability results exist for subclasses of one-clock games, and for a subclass with non-negative weights defined by a semantical restriction on the weights of cycles. In this work, we introduce the class of divergent weighted timed games as a generalisation of this semantical restriction to arbitrary weights. We show how to compute their optimal value, yielding the first decidable class of weighted timed games with negative weights and an arbitrary number of clocks.

17:30 Open steering committee

Discussion autour des GT Vérification et GT ALGA

Wednesday, May 31th – Mercredi 31 mai

Session *Population protocols*

10:00 Olivier Bournez

Protocoles de population et modèles de calcul distribués similaires

Les protocoles de population ont été introduits par Angluin et al. comme un modèle dans lequel des agents anonymes passivement mobiles calculent un prédicat sur le multi-ensemble de leurs entrées par des interactions par paires. Les prédicats calculables dans ce modèle ont été caractérisés comme étant précisément les prédicats semi-linéaires, c'est-à-dire ceux définissables en arithmétique de Presburger.
Depuis ces travaux de 2004 et 2006, plusieurs variantes ont été considérées (calculs sur des graphes, puissance étendue des agents, etc...). Le modèle a aussi été relié à des modèles de calculs par réactions chimiques stochastiques (SCRN).
L'exposé présentera plusieurs résultats connus, et tentera de relier ces modèles aux modèles classiques de la complexité et calculabilité.

11:00 Break

11:30 Janna Burman

Space-Optimal Counting in Population Protocols

We study the fundamental problem of counting, which consists in computing the size of a system. The considered model are population protocols, which is the model of finite state, anonymous and asynchronous mobile devices (agents) communicating in pairs (according to a fairness condition). We significantly improve the previous results known for counting in this model, in terms of (exact) space complexity. Specifically, we give the first space optimal protocols solving the problem for two classical types of fairness, global and weak. Both protocols require no initialization of the counted agents. The protocol designed for global fairness, surprisingly, uses only one bit of memory (two states) per counted agent. The protocol, functioning under weak fairness, requires the necessary log P bits (P states, per counted agent) to be able to count up to P agents. Interestingly, this protocol exploits the intriguing Gros sequence of natural numbers, which is also used in the solutions to the Chinese Rings and the Hanoi Towers puzzles.

12:00 Arthur Milchior

Set of (vectors of) numbers, from deterministic automata to first-order formulae

For a fixed base b, any integer can be encoded as a finite word of alphabet of digits. In dimension $d > 0$, a vector of d integers is encoded as a word over the alphabet of vectors of d digits. A set of vector of integers is thus encoded as a language whose alphabet is the set of vector of digits. Hence, an automaton whose alphabet is the set of vector of digits recognizes a set of integers.
The class of sets of tuples of integers which can be encoded by an automaton has been characterized by Büchi-Bruyère as the class of sets definable in the first-order logic of addition and of V_b ($FO[+, V_b]$). The function V_b sends an integer n to the greatest power of b dividing n.
In this presentation, I intend to talk about the following problem : Given an automaton accepting a set R, can R be defined by a formula in a logic weaker than $FO[+, V_b]$?

12:30 Lunch

Bâtiment P, salle P1-008

Session *Verification of Verifiable Protocoles*

14:30 Jannik Dreier

Verifying Verifiability: The Case of Auctions and Exams

Verifiability has been largely studied in the context of voting protocols, where one wants to be able to verify the correctness of the election result without having to trust the system. In this talk I will discuss two other applications where the same problem arises: auctions and exams.
In online auctions the participants need to trust that the underlying protocols operate correctly. A verifiable auction protocol allows the seller, the buyer, and losing bidders to determine that the result of the auction was correct, increasing their trust in the auction outcome. We formally define and analyze verifiability for auction protocols by identifying notions of verifiability for each stakeholder. This can be done in an abstract framework which can be instantiated using both symbolic and computational models. We then use the developed framework to study the verifiability of two examples of the literature, identifying several issues with the protocol due to Curtis et al.
In exams, the main concern for institutions that organize exams is to detect when students cheat. However, since a large variety of tricks is possible, and there have been multiple cases where even exam authorities misbehaved, anyone should be allowed to look into exam's records to verify the presence or the absence of frauds. We formalize several individual and universal verifiability properties for traditional and for electronic exams, so clarifying what verifiability properties are relevant and what they mean. We validate our framework by analyzing the verifiability of two existing exam systems – an electronic and a pen-and-paper system.

15:30 Nadim Kobeissi

Automated Verification for Secure Messaging Protocols and their Implementations: A Symbolic and Computational Approach

An increasing number of popular applications now use end-to-end secure messaging protocols, the most popular being the Signal Protocol which now operates on more than a billion devices. However, these implementations exist in environments where bugs and protocol flaws lead to attacks on a variety of real-world applications. We advocate the use of automated verification tools to systematically find and eliminate such attacks. We focus on Signal Protocol and provide automated symbolic verification from source code and novel semi-automated proofs in the computational model using CryptoVerif. We find new and previously-known attacks on this protocol and suggest practical countermeasures.
To provide automatic verification of source code, we designed ProScript, a protocol programming and verification framework based on a typed subset of JavaScript. The ProScript compiler extracts formal models in the applied pi calculus directly from protocol code in JavaScript. These models are human-readable and can be seen as reference specifications for protocols that were previously only specified in code. Furthermore, they can be automatically verified for desired security properties against sophisticated threat models using the ProVerif protocol analyzer. We prove our framework's viability by releasing the first secure messenger with a formally verified protocol core, for the general public, with an isolated and formally verified Signal Protocol implementation in ProScript. Our results indicate that, with a little programming discipline, the automated security verification of complex real-world web-based cryptographic protocol implementations is now practical.

16:00 Break