

# Track B

1. **Best paper in Track B**

**John Fearnley and Marcin Jurdziński.** *Reachability in Two-Clock Timed Automata is PSPACE-complete*

Abstract: A recent result by Haase et al. has shown that reachability in two-clock timed automata is log-space equivalent to reachability in bounded one-counter automata. We show that reachability in bounded one-counter automata is PSPACE-complete.

2. **Best student paper in Track B**

**Nicolas Basset.** *A maximal entropy stochastic process for a timed automaton*

Abstract: Several ways of assigning probabilities to runs of timed automata (TA) have been proposed recently. When only the TA is given, a relevant question is to design a probability distribution which represents in the best possible way the runs of the TA. This question does not seem to have been studied yet. We give an answer to it using a maximal entropy approach. We introduce our variant of stochastic model, the stochastic process over runs which permits to simulate random runs of any given length with a linear number of atomic operations. We adapt the notion of Shannon (continuous) entropy to such processes. Our main contribution is an explicit formula defining a process  $Y^*$  which maximizes the entropy. This formula is an adaptation of the so-called Shannon-Parry measure to the timed automata setting. The process  $Y^*$  has the nice property to be ergodic. As a consequence it has the asymptotic equipartition property and thus the random sampling wrt.  $Y^*$  is quasi uniform.

3. **Marcus Gelderie.** *Strategy Composition in Compositional Games*

Abstract: When studying games played on finite arenas, the arena is given explicitly, hiding the underlying structure of the arena. We study games where the global arena is a product of several smaller, constituent arenas. We investigate how these "global games" can be solved by playing "component games" on the constituent arenas. To this end, we introduce two kinds of products of arenas. Moreover, we define a suitable notion of strategy composition and show how, for the first notion of product, winning strategies in reachability games can be composed from winning strategies in games on the constituent arenas. For the second kind of product, the complexity of solving the global game shows that a general composition theorem is equivalent to proving  $Pspace = Exptime$ .

4. **Pierre-Malo Denielou and Nobuko Yoshida.** *Multiparty Compatibility in Communicating Automata: Characterisation and Synthesis of Global Session Types*

Abstract: Multiparty session types are a type system that can ensure the safety and liveness of distributed peers via the global specification of their interactions. To construct a global specification from a set of distributed uncontrolled behaviours, this paper explores the problem of fully characterising multiparty session types in terms of communicating automata. We equip global and local session types with labelled transition systems (LTSs) that faithfully represent asynchronous communications through unbounded buffered channels. Using the equivalence between the two LTSs, we identify a class of communicating automata that exactly correspond to the projected local types. We exhibit an algorithm to synthesise a global type from a collection of communicating automata. The key property of our findings is

the notion of multiparty compatibility which non-trivially extends the duality condition for binary session types.

5. **Luca Padovani.** *Fair Subtyping for Open Session Types*

Abstract: Fair subtyping is a liveness-preserving refinement relation for session types akin to (but coarser than) the well-known should-testing precongruence. The behavioral characterization of fair subtyping is challenging essentially because fair subtyping is context-sensitive: two session types may or may not be related depending on the context in which they occur, hence the traditional coinductive argument for dealing with recursive types is unsound in general. In this paper we develop complete behavioral and axiomatic characterizations of fair subtyping and we give a polynomial algorithm to decide it.

6. **David Janin.** *Algebras, automata and logic for languages of labeled birooted trees*

Abstract: In this paper, we study languages of labeled finite birooted trees: Munn's birooted trees extended with vertex labeling. We define a notion of finite state birooted tree automata that is shown to capture the class of languages that are upward closed w.r.t. the natural order and definable in Monadic Second Order Logic. Then, relying on the inverse monoid structure of labeled birooted trees, we derive a notion of recognizable languages by means of (adequate) premorphisms into finite (adequately) ordered monoids. This notion is shown to capture finite boolean combinations of languages as above. As a particular case, a simple encoding of finite (mono-rooted) labeled trees in an antichain of labeled birooted trees shows that classical regular languages of finite (mono-rooted) trees are also recognized by such premorphisms and finite ordered monoids.

7. **Artur Jež.** *One-variable word equations in linear time*

Abstract: In this paper we consider word equations with one variable (and arbitrary many appearances of it). A recent technique of recompression, which is applicable to general word equations, is shown to be suitable also in this case. While in general case it is non-deterministic, it determinises in case of one variable and the obtained running time is  $O(n)$  (in RAM model).

8. **James Worrell.** *On the Complexity of Multitape Automata Equivalence*

Abstract: The decidability of determining equivalence of deterministic multitape automata (or transducers) was a longstanding open problem until it was resolved by Harju and Karhumäki in the early 1990s. The proof of decidability yields a  $\text{co-NP}$  upper bound, but apparently not much more is known about the complexity of the problem. In this paper we give a new decidability proof that follows the basic strategy of Harju and Karhumäki, but replaces their use of group theory with results on matrix algebras. From our proof we obtain a simple randomised algorithm for deciding equivalence of deterministic multitape automata, as well as automata with transition weights in the field of rational numbers. The algorithm runs in polynomial time for each fixed number of tapes.

9. **Markus Lohrey, Benjamin Steinberg and Georg Zetsche.** *Rational subsets and submonoids of wreath products*

Abstract: It is shown that membership in rational subsets of wreath products  $H \wr V$  with  $H$  a finite group and  $V$  a virtually free group is decidable. On the other hand, it is shown that there exists a fixed finitely generated submonoid in the wreath product  $Z \wr Z$  with an undecidable membership problem.

10. **Oliver Friedmann, Felix Klaedtke and Martin Lange.** *Ramsey Goes Visibly Pushdown*

Abstract: Checking whether one formal language is included in another is vital to many verification tasks. In this paper, we provide solutions for checking the inclusion of the languages given by visibly pushdown automata over both finite and infinite words. Visibly pushdown automata are a richer automaton model than the classical finite-state automata, which allows one, e.g., to reason about the nesting of procedure calls in the executions of recursive imperative programs. The highlight of our solutions is that they do not comprise automata constructions for determinization and complementation. Instead, our solutions are more direct and generalize the so-called Ramsey-based inclusion-checking algorithms, which apply to classical finite-state automata and proved effective there, to visibly pushdown automata. We also experimentally evaluate our algorithms thereby demonstrating the virtues of avoiding determinization and complementation constructions.

11. **Saguy Benaim, Michael Benedikt, Witold Charatonik, Emanuel Kieronski, Rastislav Lenhardt, Filip Mazowiecki and James Worrell.** *Complexity of two-variable logic over finite trees*

Abstract: We consider the satisfiability problem for the two-variable fragment of first-order logic over finite unranked trees. We work with signatures consisting of some unary predicates and the binary navigational predicates  $v$  (child),  $\rightarrow$  (right sibling), and their respective transitive closures  $v^+$ ,  $\rightarrow^+$ . We prove that the satisfiability problem for the logic containing all these predicates,  $\text{FO2}[v, \rightarrow, v^+, \rightarrow^+]$ , is  $\text{ExpSpace}$ -complete. Further, we consider the restriction of the class of structures to singular trees, i.e., we assume that at every node precisely one unary predicate holds. We observe that  $\text{FO2}[v, v^+, \rightarrow, \rightarrow^+]$  and even  $\text{FO2}[v, v^+]$  remain  $\text{ExpSpace}$ -complete over finite singular trees, but the complexity decreases for some weaker logics. Namely, the logic with one binary predicate,  $v^+$ , denoted  $\text{FO2}[v^+]$ , is  $\text{NExpTime}$ -complete, and its guarded version,  $\text{GF2}[v^+]$ , is  $\text{PSPACE}$ -complete over finite singular trees, even though both these logics are  $\text{ExpSpace}$ -complete over arbitrary finite trees.

12. **Hubie Chen and Daniel Marx.** *Block-Sorted Quantified Conjunctive Queries*

Abstract: We study the complexity of model checking in quantified conjunctive logic, that is, the fragment of first-order logic where both quantifiers may be used, but conjunction is the only permitted connective. In particular, we study block-sorted queries, which we define to be prenex sentences in multi-sorted relational first-order logic where two variables having the same sort must appear in the same quantifier block. We establish a complexity classification theorem that describes precisely the sets of block-sorted queries of bounded arity on which model checking is fixed-parameter tractable. This theorem strictly generalizes, for the first time, a known classification for existential conjunctive logic to a logic in which both quantifiers are present.

13. **Daniel Leivant and Jean-Yves Marion.** *Evolving graph-structures and their implicit computational complexity*

Abstract: Dynamic data-structures are ubiquitous in programming, and they use extensively underlying directed multi-graph structures, such as labeled trees, DAGs, and objects. This paper adapts well-established static analysis methods, namely data ramification and language-based information flow security, to programs over such graph structures. Our programs support the creation, deletion, and updates of both vertices and edges, and are related to pointer machines. The main result states that a function over graph-structures is

computable in polynomial time iff it is computed by a terminating program whose graph manipulation is ramified, provided all edges that are both created and read in a loop have the same label.

14. **Mukund Raghothaman and Rajeev Alur.** *Decision Problems for Additive Regular Functions*

Abstract: Additive Cost Register Automata (ACRA) map strings to integers using a finite set of registers that are updated using assignments of the form " $x := y + c$ " at every step. The corresponding class of additive regular functions has multiple equivalent characterizations, appealing closure properties, and a decidable equivalence problem. In this paper, we solve two decision problems for this model. First, we define the register complexity of an additive regular function to be the minimum number of registers that an ACRA needs to compute it. We characterize the register complexity by a necessary and sufficient condition regarding the largest subset of registers whose values can be made far apart from one another. We then use this condition to design a PSPACE algorithm to compute the register complexity of a given ACRA, and establish a matching lower bound. Our results also lead to a machine-independent characterization of the register complexity of additive regular functions. Second, we consider two-player games over ACRAs, where the objective of one of the players is to reach a target set while minimizing the cost. We show the corresponding decision problem to be EXPTIME-complete when costs are non-negative integers, but undecidable when costs are integers.

15. **Rémy Chrétien, Véronique Cortier and Stephanie Delaune.** *From security protocols to pushdown automata*

Abstract: 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 (only symmetric encryption, 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.

16. **Roberto Di Cosmo, Jacopo Mauro, Stefano Zacchiroli and Gianluigi Zavattaro.** *Component Reconfiguration in the Presence of Conflicts*

Abstract: Components are traditionally modeled as black-boxes equipped with interfaces that indicate provided/required ports and, often, also conflicts with other components that cannot coexist with them. In modern tools for automatic system management, components become grey-boxes that show relevant internal states and the possible actions that can be acted on the components to change such state during the deployment and reconfiguration phases. However, state-of-the-art tools in this field do not support a systematic management of conflicts. In this paper we investigate the impact of conflicts by precisely characterizing the increment of complexity on the reconfiguration problem.

17. **Blaise Genest, Hugo Gimbert, Anca Muscholl and Igor Walukiewicz.** *Asynchronous Games over Tree Architectures*

Abstract: We consider the distributed control problem in the setting of Zielonka asynchronous automata. Such automata are compositions of finite processes communicating via shared actions and evolving asynchronously. Most importantly, processes participating in a shared action can exchange complete information about their causal past. This gives more power to controllers, and avoids simple pathological undecidable cases as in the setting of Pnueli and Rosner. We show the decidability of the control problem for Zielonka automata over acyclic communication architectures. We provide also a matching lower bound, which is  $2^{\Omega(h)}$ -fold exponential,  $h$  being the height of the architecture tree.

18. **Georg Zetsche.** *Silent Transitions in Automata with Storage*

Abstract: We consider the computational power of silent transitions in one-way automata with storage. Specifically, we ask which storage mechanisms admit a transformation of a given automaton into one that accepts the same language and reads at least one input symbol in each step. We study this question using the model of valence automata. Here, a finite automaton is equipped with a storage mechanism that is given by a monoid. This work presents generalizations of known results on silent transitions. For two classes of monoids, it provides characterizations of those monoids that allow the removal of  $\lambda$ -transitions. Both classes are defined by graph products of copies of the bicyclic monoid and the group of integers. The first class contains pushdown storages as well as the blind counters while the second class contains the blind and the partially blind counters.

19. **Wojciech Czerwiński, Wim Martens and Tomas Masopust.** *Efficient Separability of Regular Languages by Subsequences and Suffixes*

Abstract: When can two regular word languages  $K$  and  $L$  be separated by a simple language? We investigate this question and consider separation by piecewise- and suffix-testable languages and variants thereof. We give characterizations of when two languages can be separated and present an overview of when these problems can be decided in polynomial time if  $K$  and  $L$  are given by nondeterministic automata.

20. **Colin Stirling.** *Proof Systems for Retracts in Simply Typed Lambda Calculus*

Abstract: This paper concerns retracts in simply typed lambda calculus assuming beta eta-equality. We provide a simple tableau proof system which characterises when a type is a retract of another type and which leads to a decision procedure (which we conjecture is in PSPACE).

21. **Stéphane Demri, Amit Kumar Dhar and Arnaud Sangnier.** *On the Complexity of Verifying Regular Properties on Flat Counter Systems*

Abstract: 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.

22. **Hyeonseung Im, Keiko Nakata and Sungwoo Park.** *Contractive Signatures with Recursive Types, Type Parameters, and Abstract Types*

Abstract: Although theories of equivalence or subtyping for recursive types have been extensively investigated, sophisticated interaction between recursive types and abstract types has gained little attention. The key idea behind type theories for recursive types is to use syntactic contractiveness, meaning every  $\mu$ -bound variable occurs only under a type constructor such as  $\rightarrow$  or  $*$ . This syntactic contractiveness guarantees the existence of the unique solution of recursive equations and thus has been considered necessary for designing a sound theory for recursive types. However, in an advanced type system, such as OCaml, with recursive types, type parameters, and abstract types, we cannot easily define the syntactic contractiveness of types. In this paper, we investigate a sound type system for recursive types, type parameters, and abstract types. In particular, we develop a new semantic notion of contractiveness for types and signatures using mixed induction and coinduction, and show that our type system is sound with respect to the standard call-by-value operational semantics, which eliminates signature sealings. Moreover we show that while non-contractive types in signatures lead to unsoundness of the type system, they may be allowed in modules. We have also formalized the whole system and its type soundness proof in Coq.

23. **Emilie Charlier, Teturo Kamae, Svetlana Puzynina and Luca Q. Zamboni.** *Self-Shuffling Words*

Abstract: In this paper we introduce and study a new property of infinite words which is invariant under the action of a morphism: We say an infinite word  $x$ , defined over a finite alphabet  $A$ , is self-shuffling if  $x$  admits factorizations:  $x = \prod_{i=1}^{\infty} U_i V_i = \prod_{i=1}^{\infty} U_i = \prod_{i=1}^{\infty} V_i$  with  $U_i, V_i \in A^+$ . In other words, there exists a shuffle of  $x$  with itself which reproduces  $x$ . The morphic image of any self-shuffling word is again self-shuffling. We prove that many important and well studied words are self-shuffling: This includes the Thue-Morse word and all Sturmian words (except those of the form  $aC$  where  $a$  is a letter and  $C$  is a characteristic Sturmian word). We further establish a number of necessary conditions for a word to be self-shuffling, and show that certain other important words (including the paper-folding word and infinite Lyndon words) are not self-shuffling. In addition to its morphic invariance, which can be used to show that one word is not the morphic image of another, this new notion has other unexpected applications: For instance, as a consequence of our characterization of self-shuffling Sturmian words, we recover a number theoretic result, originally due to Yasutomi, which characterizes pure morphic Sturmian words in the orbit of the characteristic.

24. **Yuxi Fu.** *Checking Equality and Regularity for Normed BPA with Silent Moves*

Abstract: The decidability of weak bisimilarity on normed BPA is a long standing open problem. It is proved in this paper that branching bisimilarity, a standard refinement of weak bisimilarity, is decidable for normed BPA and that the associated regularity problem is also decidable.

25. **Robert Ganian, Petr Hlineny, Daniel Kral, Jan Obdrzalek, Jarett Schwartz and Jakub Teska.** *FO Model Checking of Interval Graphs*

Abstract: We study the computational complexity of the FO model checking problem on interval graphs, i.e., intersection graphs of intervals on the real line. The main positive result

is that this problem can be solved in time  $O(n \log n)$  for  $n$ -vertex interval graphs with representations containing only intervals with lengths from a prescribed finite set. We complement this result by showing that the same is not true if the lengths are restricted to any set that is dense in some open subset, e.g., in the set  $(1, 1 + \epsilon)$ .

26. **Gilles Barthe and Federico Olmedo.** *Beyond differential privacy: Composition theorems and Relational Logic for  $f$ -divergences between Probabilistic Programs*

Abstract:  $f$ -divergences form a class of measures of distance between probability distributions; they are widely used in areas such as information theory and signal processing. In this paper, we unveil a new connection between  $f$ -divergences and differential privacy, a confidentiality policy that provides strong privacy guarantees for private data-mining; specifically, we observe that the notion of  $\alpha$ -distance used to characterize approximate differential privacy is an instance of the family of  $f$ -divergences. Building on this observation, we generalize to arbitrary  $f$ -divergences the sequential composition theorem of differential privacy. Then, we propose a relational program logic to prove upper bounds for the  $f$ -divergence between two probabilistic programs. Our results allow us to revisit the foundations of differential privacy under a new light, and to pave the way for applications that use different instances of  $f$ -divergences.

27. **Udi Boker, Denis Kuperberg, Orna Kupferman and Michal Skrzypczak.** *Nondeterminism in the Presence of a Diverse or Unknown Future*

Abstract: Choices made by nondeterministic word automata depend on both the past (the prefix of the word read so far) and the future (the suffix yet to be read). In several applications, most notably synthesis, the future is diverse or unknown, leading to algorithms that are based on deterministic automata. Hoping to retain some of the advantages of nondeterministic automata, researchers have studied restricted classes of nondeterministic automata. Three such classes are nondeterministic automata that are good for trees (GFT; i.e., ones that can be expanded to tree automata accepting the derived tree languages, thus whose choices should satisfy diverse futures), good for games (GFG; i.e., ones whose choices depend only on the past), and determinizable by pruning (DBP; i.e., ones that embody equivalent deterministic automata). The theoretical properties and relative merits of the different classes are still open, having vagueness on whether they really differ from deterministic automata. In particular, while  $DBP \subseteq GFG \subseteq GFT$ , it is not known whether every GFT automaton is GFG and whether every GFG automaton is DBP. Also open is the possible succinctness of GFG and GFT automata compared to deterministic automata. We study these problems for automata with the Büchi acceptance condition. We show that  $DBP \subseteq GFT = GFG$ , and describe a determinization construction for GFG automata.

28. **Gregory M. Kobele and Sylvain Salvati.** *The IO and OI hierarchies revisited*

Abstract: We study languages of  $\lambda$ -terms generated by IO and OI unsafe grammars. These languages can be used to model meaning representations in the formal semantics of natural languages following the tradition of Montague. Using techniques pertaining to the denotational semantics of the simply typed  $\lambda$ -calculus, we show that the emptiness and membership problems for both types of grammars are decidable. In the course of the proof of the decidability results for OI, we identify a decidable variant of the  $\lambda$ -definability problem, and prove a stronger form of Statman's finite completeness Theorem.

29. **Kevin Woods.** *Presburger Arithmetic, Rational Generating Functions, and Quasi-polynomials*

Abstract: A Presburger formula is a boolean formula with variables in the natural numbers that can be written using addition, comparison ( $<$ ,  $=$ , etc.), boolean operations (and, or, not), and quantifiers ("for all" and "there exists"). We characterize sets that can be defined by a Presburger formula as exactly the sets that can be represented by a rational generating function; a geometric characterization of such sets is also given. In addition, if  $p=(p_1, \dots, p_n)$  are a subset of the unbound variables in a Presburger formula, we can define a counting function  $g(p)$  to be the number of solutions to the formula, for a given  $p$ . We show that every counting function obtained in this way may be represented as, equivalently, either a piecewise quasi-polynomial or a rational generating function. Finally, we translate known computational complexity results into this setting and discuss open directions.

30. **Tomas Petricek, Dominic Orchard and Alan Mycroft.** *Coeffects: Unified static analysis of context-dependence*

Abstract: Monadic effect typing provides a unified way of tracking effects of computations, but there is no unified mechanism for tracking how computations rely on the environment in which they are executed. This is becoming an important problem for modern software -- we need to track where distributed computations run, which resources a program uses and how they use other capabilities of the environment.

We consider three examples of context-dependence analysis: liveness analysis, tracking the use of implicit parameters, and calculating caching requirements for dataflow programs. Informed by these cases, we present a unified calculus for tracking context dependence in functional languages together with a categorical semantics based on indexed comonads. We believe that indexed comonads are the right foundation for constructing context-aware languages and type systems and that following an approach akin to monads can lead to a widespread use of the concept.

31. **Kousha Etessami, Alistair Stewart and Mihalis Yannakakis.** *Stochastic Context-Free Grammars, Regular Languages, and Newton's method*

Abstract: We study the problem of computing the probability that a given stochastic context-free grammar (SCFG),  $G$ , generates a string in a given regular language  $L(D)$  (given by a DFA,  $D$ ). This basic problem has a number of applications in statistical natural language processing, and it is also a key necessary step towards quantitative omega-regular model checking of stochastic context-free processes (equivalently, 1-exit recursive Markov chains, or stateless probabilistic pushdown processes).

We show that the probability that  $G$  generates a string in  $L(D)$  can be computed to within arbitrary desired precision in polynomial time (in the standard Turing model of computation), under a rather mild assumption about the SCFG,  $G$ , and with no extra assumption about  $D$ .

We show that this assumption is satisfied for SCFG's whose rule probabilities are learned via the well-known inside-outside (EM) algorithm for maximum-likelihood estimation (the standard method for constructing SCFGs in statistical NLP and biological sequence analysis). Thus, for these SCFGs the algorithm always runs in P-time.

32. **Facundo Carreiro, Daniel Gorín and Lutz Schröder.** *Coalgebraic announcement logics*

Abstract: In epistemic logic, dynamic operators describe the evolution of the knowledge of participating agents through communication, one of the most basic forms of communication being public announcement. Semantically, dynamic operators correspond to transformations of the underlying model. While metatheoretic results on dynamic epistemic logic so far are



largely limited to the setting of Kripke models, there is evident interest in extending its scope to non-relational modalities capturing, e.g., uncertainty or collaboration. We develop a generic framework for non-relational dynamic logic by adding dynamic operators to coalgebraic logic. We discuss a range of examples and establish basic results including bisimulation invariance, complexity, and a small model property.

33. **Georg Gottlob, Andreas Pieris and Lidia Tendera.** *Querying the Guarded Fragment with Transitivity*

Abstract: We study the problem of answering a union of Boolean conjunctive queries  $q$  against a database  $\Delta$ , and a logical theory  $\phi$  which falls in the guarded fragment with transitive guards (GFTG). We trace the frontier between decidability and undecidability of the problem under consideration. In particular, we show that query answering under GF2TG, i.e., the two-variable fragment of GFTG, is already undecidable (even without equality), but its monadic fragment is decidable; in fact, it is 2EXPTIME-complete in combined complexity and coNP-complete in data complexity. We also show that for a restricted class of queries, query answering under GFTG is decidable.