MEMICS 2017

12^{th} Doctoral Workshop on Mathematical and Engineering Methods in Computer Science

Jan Kofroň David Šafránek Adam Rogalewicz

October 13–15, 2017

Preface

This volume contains the proceedings of the 12th Doctoral Workshop on Mathematical and Engineering Methods in Computer Science (MEMICS 2017) held in Telč, Czech Republic, during October 13-15, 2017.

The aim of the MEMICS workshop series is to provide an opportunity for PhD students to present and discuss their work in an international environment. MEMICS focuses broadly at formal and mathematical methods in computer science and engineering and their applications.

This year, the MEMICS 2017 workshop invites PhD students to submit a presentation of their recent research results that have already undergone a rigorous peer-review process and have been presented at a high-quality international conference or published in a recognized journal. Additionally, students are also invited to present their ongoing work in the form of poster.

There were 23 submissions from PhD students. We received 12 presentation abstracts and 11 poster abstracts, all of which were accepted for presentation at the workshop.

The highlights of the MEMICS 2017 program included three keynote lectures delivered by internationally recognized researchers from various areas of computer science. The invited talks include:

- Georg Weissenbacher (TU Wien): Interpolation-based Model Checking and IC3
- Loïc Paulevé (CNRS/U. Paris-Sud): Formal methods for capturing dynamics of biological networks
- Alessandro Abate (University of Oxford): Formal verification of complex systems: model-based and data-driven methods

The successful organization of MEMICS 2017 would not have been possible without generous help and support from the organizing institutions: Masaryk University and Brno University of Technology.

We thank the Organizing Committee members who helped to create a unique and relaxed atmosphere that distinguishes MEMICS from other computer science meetings. We also gratefully acknowledge the support of the EasyChair system.

October 2017

Jan Kofroň
David Šafránek
Adam Rogalewicz

Organization

The 12th Doctoral Workshop on Mathematical and Engineering Methods in Computer Science MEMICS 2017 took place in Telč, Czech Republic, during October 13–15, 2017. More information about the MEMICS workshop series is available at `http://www.memics.cz`.

Presentation abstracts

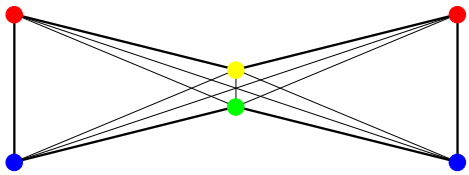
On Colourability of Polygon Visibility Graphs*

Onur Çağırıcı, Petr Hliněný, and Bodhayan Roy

Department of Computer Science, Masaryk University at Brno, Czechia

Abstract. We study the problem of colouring the visibility graphs of polygons. In particular, we provide a polynomial algorithm for 4-colouring of the polygon visibility graphs, and prove that the 6-colourability question is already NP-complete for them†.

Given an n-vertex polygon P (not necessarily convex) in the plane, two points p and q of P are said to be *mutually visible* if, and only if the line segment $\overline{pq}$ does not intersect the exterior of P. The n-vertex visibility graph $G(V, E)$ of P is defined as follows. The vertex set V of G contains a vertex v_i if, and only if, the polygon P contains the point p_i as its vertex. The edge set E of G contains an edge $\{v_i, v_j\}$ if, and only if, the points p_i and p_j are mutually visible. An example polygon visibility graph with proper vertex coloring is shown below.



In this paper we settle (nearly in full) the complexity question of the general problem of colouring polygonal visibility graphs, which was declared open in 1995 by Lin and Skiena. We provide a polynomial-time algorithm to find a 4-colouring of the visibility graph of a given polygon, if such a colouring exists. On the other hand, we provide a reduction showing that the question of k-colourability of the visibility graph of a given simple polygon is NP-complete for any $k \geq 6$. Only the case of 5 colours is left open.

* P. Hliněný and O. Çağırıcı are supported by the Czech Science Foundation, project no. 17-00837S.

† This abstract is based on a paper submitted to FSTCCS 2017

Lazy Automata Techniques for WS1S (PRESENTATION)

Tomáš Fiedor[1], Lukáš Holík[1], Petr Janků[1], Ondřej Lengál[1], and Tomáš Vojnar[1]

FIT, Brno University of Technology, IT4Innovations Centre of Excellence, Czech Republic

Weak monadic second-order logic of one successor (WS1S) is a powerful language for reasoning about regular properties of finite words. It has found numerous uses, from software and hardware verification through controller synthesis to computational linguistics, and further on. Most of the successful applications were due to the tool MONA [1], which implements classical automata-based decision procedures for WS1S. The worst case complexity of WS1S is nonelementary [2] and, despite many optimizations implemented in MONA and other tools, the complexity sometimes strikes back.

The classical WS1S decision procedure builds an automaton A_φ accepting all models of the given formula φ in a form of finite words, and then tests A_φ for language emptiness. The bottleneck of the procedure is the size of A_φ, which can be huge due to the fact that the derivation of A_φ involves many nested automata product constructions and complementation steps, preceded by determinization.

The main point of this paper is to avoid the state-space explosion involved in the classical *explicit* construction by representing automata *symbolically* and testing the emptiness *on the fly*, while constructing A_φ, and by omitting the state space irrelevant to the emptiness test. This is done using two main principles: *lazy evaluation* and *subsumption-based pruning*. These principles have, to some degree, already appeared in the so-called antichain-based testing of language universality and inclusion of finite automata [3]. The richer structure of the WS1S decision problem allows us, however, to elaborate on these principles in novel ways and utilize their power even more.

We have implemented our decision procedure in a prototype tool called GASTON and compared its performance with other WS1S solvers. GASTON was able to significantly outperform MONA and other solvers on a number of formulae obtained from various formal verification tasks. We believe that the efficiency of our approach can be pushed much further, making WS1S scale enough for new classes of applications.

This presentation is based on a paper [4] with the same name that appeared in the proceedings of TACAS 2017.

Acknowledgement. This work was supported by the Czech Science Foundation (projects 16-17538S and 16-24707Y), the BUT FIT project FIT-S-17-4014, and the IT4IXS: IT4Innovations Excellence in Science project (LQ1602).

References

1. Elgaard, J., Klarlund, N., Møller, A.: MONA 1.x: new techniques for WS1S and WS2S. In: In Proc. of CAV 1998, BRICS, Department of Computer Science, Aarhus University, Springer
2. Meyer, A.R.: Weak monadic second order theory of successor is not elementary-recursive. In: Logic Colloquium—Symposium on Logic Held at Boston, 1972–73, Springer
3. Wulf, M.D., Doyen, L., Henzinger, T.A., Raskin, J.F.: Antichains: A new algorithm for checking universality of finite automata. In: Proc. of CAV'06, Springer
4. Fiedor, T., Holík, L., Janků, P., Lengál, O., Vojnar, T.: Lazy automata techniques for ws1s. In: Proc. of TACAS'17, Springer

Counterexample Validation and Interpolation-Based Refinement for Forest Automata (PRESENTATION)

Lukáš Holík, Martin Hruška, Ondřej Lengál, Adam Rogalewicz, and Tomáš Vojnar

FIT, Brno University of Technology, Czech Republic

The talk will present the current progress in forest automata-based shape analysis that we published in proceedings of the conference VMCAI'17 [3]. The FORESTER tool implenting this approach participated in SV-COMP'17 [4].

In the context of shape analysis, counterexample validation and abstraction refinement are complex and so far not sufficiently resolved problems. We provide a novel solution to both of these problems in the context of fully-automated and rather general shape analysis based on forest automata [1]. Our counterexample validation is based on *backward symbolic execution* of a candidate counterexample trace on the level of FAs (with no abstraction on the FAs) while checking *non-emptiness of its intersection* with the forward symbolic execution (which was abstracting the FAs). For that, we have to revert not only abstract transformers corresponding to program statements but also various meta-operations that are used in the forward symbolic execution.

Our abstraction on FAs is a modification of the so-called *predicate language abstraction* [2]. This particular abstraction collapses those states of component TAs that have non-empty intersection with the same predicate languages, which are obtained from the backward execution. We show that, in case the intersection of the set of configurations of the above described forward and backward symbolic runs is empty, we can derive from it an *automata interpolant* allowing us to get more predicate languages and to refine the abstraction such that progress of the CEGAR loop is guaranteed (in the sense that we do not repeat the same abstract forward run).

We have implemented the approach in the FORESTER tool which allowed us to verify some programs that were out of our reach before due to handling finite domain data stored in the heap.

Acknowledgement. Martin Hruška is a holder of the Brno Ph.D. Talent Scholarship, funded by the Brno City Municipality. Supported by the Czech Science Foundation (projects 14-11384S and 16-24707Y) and the IT4IXS: IT4Innovations Excellence in Science project (LQ1602).

References

1. Habermehl, P., Holík, L., Rogalewicz, A., Šimáček, J., Vojnar, T.: Forest Automata for Verification of Heap Manipulation. Formal Methods in System Design, **41**(1), Springer, 2012.
2. Bouajjani, A., Habermehl, P., Rogalewicz, A., Vojnar, T.: Abstract regular (tree) model checking. International Journal on Software Tools for Technology Transfer, **14**(2), Springer, 2012.
3. Holík, L., Hruška M., Lengál, O., Rogalewicz, A., Šimáček, J., Vojnar T.: Counterexample Validation and Interpolation-Based Refinement for Forest Automata. In *Proc. of VMCAI'17*, LNCS 10145, Springer, 2017.
4. Holík, L., Hruška M., Lengál, O., Rogalewicz, A., Šimáček, J., Vojnar T.: Forester: From Heap Shapes to Automata Predicates. In *Proc. of TACAS'17*, LNCS 10206, Springer, 2017.

A Reduction of Finitely Expandable Deep Pushdown Automata (PRESENTATION)*

Lucie Dvořáková and Alexander Meduna

Brno University of Technology, Faculty of Information Technology
Božetěchova 2, 612 66 Brno, Czech Republic
{icharvatl,meduna}@fit.vutbr.cz

Abstract. For a positive integer n, n-expandable deep pushdown automata always contain no more than n occurrences of non-input symbols in their pushdowns during any computation. As its main result, the presentation demonstrates that these automata are as powerful as the same automata with only two non-input pushdown symbols—$ and #, where # always appears solely as the pushdown bottom. Moreover, the presentation demonstrates an infinite hierarchy of language families that follows from this main result. The presentation also points out that if # is the only non-input symbol in these automata, then they characterize the family of regular languages. In its conclusion, the presentation suggests open problems and topics for the future investigation.

In essence, deep pushdown automata represent language-accepting models based upon new stack-like structures, which can be modified deeper than on their top. As a result, these automata can make expansions deeper in their pushdown lists as opposed to ordinary pushdown automata, which can expand only the very pushdown top. At present, the study of deep pushdown automata represent a vivid trend in formal language theory (see references in [1]).

This presentations narrows its attention to n-expandable deep pushdown automata, where n is a positive integer. In essence, during any computation, their pushdown lists contain #, which always appears as the pushdown bottom, and no more than $n-1$ occurrences of other non-input symbols. As its main result, the presentation demonstrates how to reduce the number of their non-input pushdown symbols different from # to one symbol, denoted by $, without affecting the power of these automata. Based on this main result, the presentation shows that an infinite hierarchy of language families resulting from these reduced versions of n-expandable deep pushdown automata can be established. More precisely, consider n-expandable deep pushdown automata with pushdown alphabets containing #, $, and input symbols. The presentation shows that $(n+1)$-expandable versions of these automata are stronger than their n-expandable versions, for every positive integer n. In addition, it points out that these automata with # as its only non-input symbol characterize the family of regular languages. In its conclusion, this presentation formulates several open problem areas related to the subject of this presentation for the future study.

The presentation is based on the paper accepted to Schedae Informaticae [1].

References

1. Lucie Dvorakova and Alexander Meduna. A reduction of finitely expandable deep pushdown automata. *Schedae Informaticae*, In press.

* The work was supported by the TAČR grant TE01020415; and the BUT grant FIT-S-17-3964.

Restful-based Mobile Web Service Migration Framework (Presentation)

M. Mohanned Kazzaz
Department of Information Systems
Faculty of Information Technology
Brno University of Technology
Brno, Czech Republic
ikazzaz@fit.vutbr.cz

Marek Rychlý
Department of Information Systems
Faculty of Information Technology
Brno University of Technology
IT4Innovations Centre of Excellence
Brno, Czech Republic
rychly@fit.vutbr.cz

In this abstract we present our work [1]. The original paper describes the RESTful-based framework proposed for Mobile Web service migration and provisioning on both Android-based mobile devices and Java-based stationary devices in P2P wireless network. The proposed Web service migration framework enables deploying, publishing, discovering, provisioning and migrating Web services to satisfy service providers' and Web services' preferences and improve *QoS* performance.

We proposed service migration to improve service performance by moving a mobile hosted Web service to another mobile device that satisfies its preferences. For experiments, we used a video transcoding service as an example service and compared between its performace before and after the migration. Moreover, we collected the consumptions of mobile device resources (i.e., CPU and Battery power) by the service migration.

The migration mechanism considers matching between services and service providers preferences described as Jena rules based on their owl/rdf semantic properties. Based on service and service provider properties and preferences a suggested list of possible migration is provided. The framework chooses the best migration to perform through the proposed AHP multi-criteria decision making process.

Based on the performed experiments, we see that our framework enables a seamless adaptation in SOA to redistribute system components and improves service (i.e., the utilized video transcoding service) performance with low consumptions of mobile resources. Moreover, The experiments shows the service performance improvements gained by the migration.

References

[1] M. Mohanned Kazzaz & Marek Rychlỳ (2017): *Restful-based Mobile Web Service Migration Framework*. In: *2017 IEEE International Conference on AI & Mobile Services, AIMS 2017*, IEEE, pp. 70–75.

Using Off-the-Shelf Exception Support Components in C++ Verification*

Vladimír Štill
Faculty of Informatics, Masaryk University
Brno, Czech Republic

Petr Ročkai
Faculty of Informatics, Masaryk University
Brno, Czech Republic

Jiří Barnat
Faculty of Informatics, Masaryk University
Brno, Czech Republic

An important step toward adoption of formal methods in software development is comprehensive support for mainstream programming languages. Unfortunately, these languages are often rather complex and come with substantial standard libraries. By choosing a suitable intermediate language, most of the complexity can be delegated to existing execution-oriented (as opposed to verification-oriented) compiler frontends and standard library implementations. In this work, we explore how support for C++ exceptions can take advantage of the same principle. Our work is based on DiVM, an LLVM-derived, verification-friendly intermediate language and implemented in the DIVINE model checker.

Our implementation consists of 2 parts: the first one is an implementation of the `libunwind` platform API, which is linked to the program under test and provides language agnostic primitives for stack manipulation. The other part is a preprocessor for LLVM bitcode, which prepares exception-related metadata and replaces associated special-purpose LLVM instructions. The preprocessing contains both language agnostic and C++ specific parts.

These components allow us to reuse existing `libc++abi` runtime library for C++, which is responsible for the language-specific work of searching for exception handlers. Together, this allows for a full analysis of C++ programs with exception handling in DIVINE. Moreover, we show that this approach avoids problems with corner cases present in other verifiers with C++ exception support. These problems are often related to the handler block search, which is one of the most complex parts of exception support. This part is reused with our approach and therefore behaves exactly as in production environment.

This work has been published in proceedings of the IEEE International Conference on Software Quality, Reliability and Security (QRS 2017) [1]. The paper and presentation was awarded best paper award.

References

[1] Vladimír Štill, Petr Ročkai & Jiří Barnat (2017): *Using Off-the-Shelf Exception Support Components in C++ Verification*. In: *IEEE International Conference on Software Quality, Reliability and Security (QRS)*, pp. 54–64, doi:10.1109/QRS.2017.15. Available at `http://ieeexplore.ieee.org/document/8009908/`.

*This work has been partially supported by the Czech Science Foundation grant No. 15-08772S and by Red Hat, Inc.

Coincer: Decentralised Trustless Platform for Exchanging Cryptocurrencies (PRESENTATION)

Michal Zima

Faculty of Informatics, Masaryk University,
Brno, Czech Republic

xzima1@fi.muni.cz

We address the problem of a trustless decentralised exchange of cryptocurrencies. Centralised exchanges are neither trustworthy nor secure. As of 2017, there has been more than 26 million US dollars' worth of cryptocurrencies stolen from (or by) centralised exchanges and we expect this number to further grow. Our goal with Coincer is to allow any two users to exchange their diverse cryptocurrencies directly between them, yet with no need to trust each other, i. e., completely removing centralised exchanges and other trust requiring third parties from the process.

Former approaches either do not do without a server or rely on a trusted issuer of exchangeable tokens, i. e., they do not create a fully decentralised environment—instead they move trust to different elements. Our approach is to fully eliminate any elements susceptible to becoming a single point of failure. Coincer therefore leverages an efficient anonymous P2P overlay and an atomic protocol for exchanging money across different cryptocurrencies. Further, we build a decentralised market upon the P2P overlay and also leverage this network structure for serverless communication between users.

The atomic protocol extends former work with a complete overhaul of its cryptocurrency scripts, building upon new scripting capabilities of cryptocurrencies. As a result, we also fix vulnerabilities of former protocols which broke atomicity of those protocols and allowed a possibility to steal money from one's trading counterpart.

However, applicability of our approach is limited. Cryptocurrencies that do not support compatible cryptographic primitives cannot be directly exchanged. Instead, an intermediary cryptocurrency has to be used.

Coincer is implemented as free software and has been successfully tested with Bitcoin and Litecoin.

The work was presented at the 11th International Conference, NSS 2017, in Helsinki, Finland, and published in proceedings LNCS 10394.

DOI: 10.1007/978-3-319-64701-2_53

A Model Checking Approach to Discrete Bifurcation Analysis* (PRESENTATION)

Nikola Beneš, Luboš Brim, Martin Demko, Samuel Pastva and David Šafránek

Systems Biology Laboratory, Faculty of Informatics, Masaryk University
Botanická 68a, 602 00 Brno, Czech Republic

{xbenes3,brim,xdemko,xpastva,safranek}@fi.muni.cz

Presented at the 21st International Symposium on Formal Methods [1].

Continuous dynamical systems can be used to study a wide variety of phenomena in biology [2], economy [3], engineering [4] and computer science [5]. These systems usually contain parameters which significantly influence their behaviour. Such influence is traditionally studied using the apparatus of bifurcation analysis [6]. However, current numerical and analytical methods for bifurcation analysis are hard to automatise, do not scale well in the number of parameters, and are often limited to specific canonical models.

In this work, we present a novel approach to bifurcation analysis which assumes a suitable discrete abstraction of the continuous system and employs model checking to discover the critical parameter values, referred to as bifurcation points. To distinguish a qualitative change in the system's behaviour, we rely on the notion of behavioural patterns (cycle, equilibrium, saddle, etc.), also known as phase portraits. We define a hybrid extension of CTL logic with direction formulae in order to specify such patterns.

We demonstrate the method on a model of a bistable genetic switch mechanism taken from systems biology.

References

[1] Beneš, N., Brim, L., Demko, M., Pastva, S., Šafránek, D. In: A Model Checking Approach to Discrete Bifurcation Analysis. Springer International Publishing, Cham (2016) 85–101

[2] Kitano, H.: Systems biology: A brief overview. Science **295**(5560) (2002) 1662–1664

[3] Tesfatsion, L.: Agent-based computational economics: modeling economies as complex adaptive systems. Information Sciences **149**(4) (2003) 262 – 268

[4] Detroux, T., Renson, L., Masset, L., Kerschen, G.: The harmonic balance method for bifurcation analysis of large-scale nonlinear mechanical systems. Computer Methods in Applied Mechanics and Engineering **296** (2015) 18 – 38

[5] Raina, G., et al.: Local stability and hopf bifurcation analysis of a rate control protocol with two delays. In: Control and Decision Conference (CCDC), 2015 27th Chinese, IEEE (2015) 3111–3116

[6] Champneys, A., Tsaneva-Atanasova, K. In: Dynamical Systems Theory, Bifurcation Analysis. Springer New York, New York, NY (2013) 632–637

*This work has been supported by the Czech Science Foundation grant GA15-11089S and by the Czech National Infrastructure grant LM2015055.

POSTER - String Constraints with Concatenation and Transducers Solved Efficiently

String analysis is the problem of reasoning about how strings are manipulated by a program. It has numerous applications including automatic detection of cross-site scripting, and automatic test-case generation. A popular string analysis technique includes symbolic executions, which at their core use constraint solvers over string domains, a.k.a. string solvers. Such solvers typically reason about constraints expressed in theories over strings with the concatenation operator as an atomic constraint. In recent years, researchers started to recognise the importance of incorporating the replace-all operator (i.e. replace all occurrences of a string by another string) and, more generally, finite-state transductions in the theories of strings with concatenation. Such string operations are typically crucial for reasoning about XSS vulnerabilities in web applications, especially for modelling sanitisation functions and implicit browser transductions (e.g. innerHTML). Although this results in an undecidable theory in general, it was recently shown that the straight-line fragment of the theory is decidable, and is sufficiently expressive in practice for many applications. In this work, we provide the first string solver that can reason about constraints involving both concatenation and finite-state transductions, and that is a decision procedure for several relevant fragments, including straight-line. The main challenge that we address in the work is the prohibitive worst-case computational complexity of the theory (double-exponential time), which is exponentially harder than the case without finite-state transductions. To this end, we propose a method that exploits succinct alternating finite-state automata as concise symbolic representations of string constraints. Compared to methods that use representations based on nondeterministic machines, alternation offers not only (expected) exponential savings in space when representing Boolean combinations of transducers, but, importantly, also a possibility of succinct representation of otherwise costly combinations of transducers and concatenation. Reasoning about the emptiness of the AFA language requires a state-space exploration in an exponential-sized graph. To this end, we use the model checking algorithms like IC3 for solving the problem. We have implemented our algorithm and demonstrated its efficacy on string benchmarks that are derived from cross-site scripting analysis and other examples in the literature.

On Simplification of Formulas with Unconstrained Variables and Quantifiers (PRESENTATION)

Martin Jonáš Jan Strejček
Masaryk University, Brno, Czech Republic
{xjonas,strejcek}@fi.muni.cz

Preprocessing of the input formula is an essential part of all modern SMT solvers. This presentation elaborates on one particular kind of preprocessing rules: the simplification of formulas containing unconstrained variables, i.e. variables that occur only once in the whole formula. It has been independently observed by Bruttomesso in 2008, Brummayer in 2010, and Franzén in 2010 that formulas coming from software and hardware verification tasks often contain a large number of unconstrained variables and that such variables can be used to significantly reduce the size and complexity of the formula.

We extend the idea of previously known simplifications in two directions. First, we introduce the notion of a *partially constrained term* and show some simplification rules relying on this notion. One example of a partially constrained term from the theory of bit-vectors is a multiplication of an unconstrained variable by an even constant. Although this term cannot be simplified using known simplifications techniques, it can be simplified by the proposed simplifications using partially constrained terms. Second, since the known simplifications are not correct for quantified formulas, we introduce a refined definition of an unconstrained variable, which takes the order of quantifiers in the formula into account. We show that such a refined definition yields correct simplifications even for quantified formulas. Moreover, we show how both these extensions can be combined in order to simplify partially constrained terms in formulas with quantifiers. We experimentally evaluate the proposed simplifications on two sets of quantified formulas in the bit-vector theory and show their benefit to the performance of state-of-the-art SMT solvers Boolector, Q3B and Z3.

The presentation is based on the paper

- Martin Jonáš and Jan Strejček. "On Simplification of Formulas with Unconstrained Variables and Quantifiers". In: *Theory and Applications of Satisfiability Testing – SAT 2017 – 20th International Conference, Melbourne, VIC, Australia, August 28 – September 1, 2017, Proceedings*. 2017, pp. 364–379.

Approximating Complex Arithmetic Circuits with Formal Error Guarantees (PRESENTATION)*

Milan Ceska, Jiri Matyas, Tomas Vojnar, Vojtech Mrazek,
Lukas Sekanina and Zdenek Vasicek

Faculty of Information Technology, Brno University of Technology

Approximate computing was established as a new research field in the recent years with the purpose to examine, how could computer systems be made better by relaxing the requirement of always performing correct computations. Approximate computing can be employed in so called error resilient applications, which can produce acceptable results despite the fact that its constituent computations are performed imperfectly.

In this presentation we focus on approximate arithmetic circuits and their design techniques. The currently available methods usually rely on generating a great number of approximate solutions derived from a golden solution. Each such candidate solution has to be evaluated and checked, whether it fulfils the error (and various other) constraints. Many different approaches to candidate solution evaluations have already been tried (full and random simulation, SAT solvers, etc. ...) but all of them run into severe scalability problems.

In this work we design and present a new method with the objective to synthesize complex approximate arithmetic circuits with formal bounds on the approximation error. Our method fundamentally improves the scalability of the synthesis process; it successfully approximates multipliers with up to 32-bit inputs, while other current methods are usable either only for smaller circuits (10-bit inputs) or resort to statistical testing only.

The key idea of our method is to employ a novel search strategy that drives the search towards promptly verifiable approximate circuits. We have implemented the strategy within the ABC tool and extended the underlying equivalence checking algorithm to support queries on the worst case error.

The proposed method was evaluated in the task of functional approximation of multipliers (with up to 32 bit operands). This is for the first time when such complex approximate arithmetic circuits with formally guaranteed error bounds have been presented. This shows that our approach significantly outperforms existing methods. The presentation is based on the paper that has been accepted to the International Conference on Computer Aided Design 2017 [1].

References

1. Ceska, M., Matyas, J., Vojnar, T., Mrazek, V., Sekanina, L., and Vasicek, Z. Approximating complex arithmetic circuits with formal error guarantees: 32-bit multipliers accomplished. In *Proceedings of 36th IEEE/ACM ICCAD* (2017).

* The work is supported by the Czech Science Foundation (projects 14-11384S, 16-24707Y), and the IT4IXS: IT4Innovations Excellence in Science (LQ1602).

FO model checking of geometric graphs (PRESENTATION)*

Petr Hliněný Filip Pokrývka Bodhayan Roy
Faculty of Informatics, Masaryk University Brno, Czech Republic
{hlineny,xpokryvk,b.roy}@fi.muni.cz

We study the FO model checking problem for dense graph classes definable by geometric means (intersection and visibility graphs). We obtain new nontrivial FPT results, e.g., for restricted subclasses of *circular-arc, circle, box, disk, and polygon-visibility graphs*. We also complement the tractability results by related hardness reductions.

Algorithmic metatheorems are results stating that all problems expressible in a certain language are efficiently solvable on certain classes of structures, e.g. of finite graphs. Note that the model checking problem for *first-order logic* – given a graph G and an FO formula ϕ, we want to decide whether G satisfies ϕ (written as $G \models \phi$) – is trivially solvable in time $|V(G)|^{\mathcal{O}(|\phi|)}$. "Efficient solvability" hence in this context often means *fixed-parameter tractability* (FPT); that is, solvability in time $f(|\phi|) \cdot |V(G)|^{\mathcal{O}(1)}$ for some computable function f.

Our results mainly concern graph classes which are related to interval graphs. Namely, we prove that FO model checking is FPT on *circular-arc graphs* (these are interval graphs on a circle) if there is no long chain of arcs nested by inclusion. We similarly show tractability of FO model checking of interval-overlap graphs, also known as *circle graphs*, of bounded independent set size, and of restricted subclasses of *box and disk graphs* which naturally generalize interval graphs to two dimensions.

On the other hand, for all of the studied cases we also show that whenever we relax our additional restrictions (parameters), the FO model checking problem becomes as hard on our intersection classes as on all graphs. Some of our hardness claims hold also for the weaker $\exists$FO model checking problem.

Another well studied dense graph class in computational geometry are *visibility graphs* of polygons, which have been largely explored in the context of recognition, partition, guarding and other optimization problems.

We consider some established special cases, involving *weak visibility, terrain* and *fan* polygons. We prove that FO model checking is FPT for the visibility graphs of a weak visibility polygon of a convex edge, with bounded number of reflex (non-convex) vertices. On the other hand, without bounding reflex vertices, FO model checking remains hard even for the much more special case of polygons that are terrain and convex fans at the same time.

This work was accepted to the *12th International Symposium on Parameterized and Exact Computation (IPEC 2017, September 6-8, Vienna, Austria)*.

*P. Hliněný and F. Pokrývka are supported by the Czech Science Foundation project No. 17-00837S.

Poster abstracts

WalDis: Mining Discriminative Patterns within Dynamic Graphs (POSTER)

Karel Vaculík Luboš Popelínský
KD Lab, FI MU Brno, Czech Republic
xvaculi4@fi.muni.cz popel@fi.muni.cz

Introduction. Real-world networks typically evolve through time, which means there are various events occurring, such as edge additions or attribute changes of vertices or edges. In order to understand such events, one must be able to discriminate between different events. Existing approaches typically discriminate whole graphs, which are mostly static [1, 2, 3]. We present a new, as yet unpublished, algorithm WalDis for mining discriminate patterns of events in dynamic graphs. The discriminative patterns are subgraphs appearing, possibly inexactly, in the neighbourhood of the *positive* events and not appearing in the neighbourhood of the *negative* events. For example, the positive events may be the vertex attribute changes from "*A*" to "*B*" and the negative events the changes from "*A*" to "*C*". The proposed algorithm uses sampling and greedy approaches in order to keep the performance high and to deal with inexact graph matching.

Method. The algorithm consists of two phases. First, it explores the local neighbourhoods of the events by using a random walk technique and computes the statistics about these neighbourhoods. Then, it utilizes the computed statistics to extract the patterns by taking edges with high *score*. More precisely, edges occurring around many positive events get high score, however, this score may be substantially lowered if they also occur frequently around negative events.

Experiments and Results. Experiments were performed on three real-world graph datasets. The first graph was created from DBLP database[1], where paper collaboration on selected data mining conferences was used to build the network. The second graph was constructed from email correspondence in Enron company[2]. The third graph was obtained from a partnership telecommunication company, where phone calls formed the graph structure. In all experiments, the events were divided into a training and a test set. WalDis used the training events for discovering the patterns and then it checked their occurrences in the test set. The algorithm successfully found patterns prevailing in the context of positive events. WalDis is a novel method that outperformed state-of-the-art methods in generality of patterns being found.

References

[1] Fuksova, A., Kuzelka, O., Szaboova, A.: A method for mining discriminative graph patterns. *NIPS Workshop on Machine Learning in Computational Biology*, 2013.

[2] Jin, N., and Wang, W.: LTS: Discriminative Subgraph Mining by Learning from Search History. In *Proceeding ICDE '11*, pp. 207–218, 2011.

[3] Zong, B., et al.: Behavior Query Discovery in System-Generated Temporal Graphs. In *Proc. VLDB Endow.*, pp. 240–251, 2015.

[1] http://dblp.uni-trier.de/

[2] http://www.cis.jhu.edu/~parky/Enron

(POSTER) E-cyanobacterium.org: A Web-based Platform for Systems Biology of Cyanobacteria

Matej Troják, David Šafránek,
Jakub Hrabec, Jakub Šalagovič,
Františka Romanovská, Matej Hajnal
Systems Biology Laboratory
Faculty of Informatics, Masaryk University
Brno, Czech Republic
sybila@fi.muni.cz

Jan Červený
Global Change Research Centre AS CR
Brno, Czech Republic
cerveny.j@czechglobe.cz

The understanding of a complex cellular machinery is a crucial problem in current systems biology, especially for photosynthetic organisms such as cyanobacteria. To challenge this uneasy task we have developed an online platform [2] which consists of three interconnected modules.

- **Biochemical Space** (BCS) [1] allows to formally describe (bio)chemical reactions facilitated by cyanobacteria molecular entities. Such reactions are represented in a generalised form of rules specified in the Biochemical Space Language – a novel rule-based language. The rules form a hierarchy of (bio)chemical processes covering transport, metabolism, circadian clock, photosynthesis, and carbon concentrating mechanism.
- **Model Repository** is a collection of related mathematical models accompanied with simulation and static analysis algorithms. Linkage of model components to BCS determines their exact biological meaning. This feature is also present in models exported to SBML standard format.
- **Experiments Repository** serves to import, store, and plot time-series experiments. The measured variables are connected to BCS in the same manner as in the case of model components. Individual experiments possess additional references to related models.

In addition, data annotation is available in all modules of the platform. In consequence, BCS, models, and experiments are well-noted and referenceable. Moreover, the usability of the platform is enhanced with visualisations provided for process hierarchy and reaction networks in BCS, simulations in Model Repository, and time-series plots in Experiment Repository.

In conclusion, our platform provides a unique solution based on integrating three different approaches to stimulate collaboration between experimental and computational systems biologists.

References

[1] T. Děd, D. Šafránek, M. Troják, M. Klement, J. Šalagovič & L. Brim (2016): *Formal Biochemical Space with Semantics in Kappa and BNGL. Electronic Notes in Theoretical Computer Science* 326, pp. 27–49, doi:10.1016/j.entcs.2016.09.017. Available at https://doi.org/10.1016/j.entcs.2016.09.017.

[2] M. Troják, D. Šafránek, J. Hrabec, J. Šalagovič, F. Romanovská & J. Červený (2016): *E-Cyanobacterium.org: A Web-Based Platform for Systems Biology of Cyanobacteria*. In: *CMSB 2016, LNBI* 9859, Springer, pp. 316–322, doi:10.1007/978-3-319-45177-0_20. Available at http://dx.doi.org/10.1007/978-3-319-45177-0_20.

(POSTER) System Control Using the Modern Taylor Series Method

Petr Veigend[1], Václav Šátek, and Jiří Kunovský

Brno University of Technology, Faculty of Information Technology
Božetěchova 2, 612 66 Brno, Czech Republic
{iveigend}@fit.vutbr.cz

Solution of system control problems with PI controllers can be difficult. When parameters of the used solver (e.g. step size or relative/absolute tolerance) are not optimal. The new method based on the Taylor series (Modern Taylor series Method, MTSM) has some favourable properties not present in the widely used methods. The method can be used to replace state of the art Runge-Kutta methods in system control. The example system (Figure 1) was analysed. The numerical experiments were performed in MATLAB using newly implemented MTSM solver and ode solvers integrated in MATLAB.

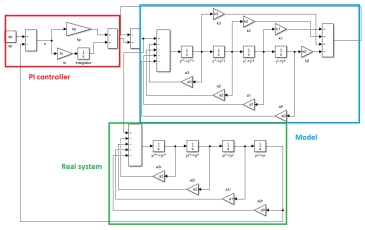


Fig. 1. Block algebra representation of the complete control system

Table 1 shows the positive properties of MTSM for the presented problem. The original work was presented at the ICNAAM 2017 conference [1].

Solver	Method order	Number of steps	Time of calculation [s]
RK2 (ode23)	2 – 3	6575	0.174585
RK4 (ode45)	4 – 5	2408	0.042736
MTSM	40 – 50	40	0.007860

Table 1. Results of the experiments

References

1. Veigend, P.,Šátek, V. and Kunovský J., *System control using the Modern Taylor series Method*, In *15th International Conference of Numerical Analysis and Applied Mathematics*, 2017.

(POSTER) Numerical Solution of Wave Equation Using Higher Order Methods

Gabriela Nečasová[1], Václav Šátek[1], and Jiří Kunovský[1]

Faculty of Information Technology, Brno University of Technology, Božetěchova 1/2, 612 66, Brno, Czech Republic
inecasova@fit.vutbr.cz

The poster deals with the numerical solution of partial differential equations using higher order methods. The one-dimensional wave equation was chosen for experiments. The chosen problem was solved in the spatial domain using higher order Method of Lines which transforms the partial differential equation into the system of ordinary differential equations. The solution in time domain remains continuous, and the Modern Taylor Series Method was used for solving the system of initial value problems. On the other hand, the spatial discretization is performed using higher order finite difference formulas, which can be unstable. The necessity of the variable precision arithmetic to stabilize the solution is discussed in this poster. The seven point difference formula is analysed as an example of higher order finite difference formulas (Figure 1).

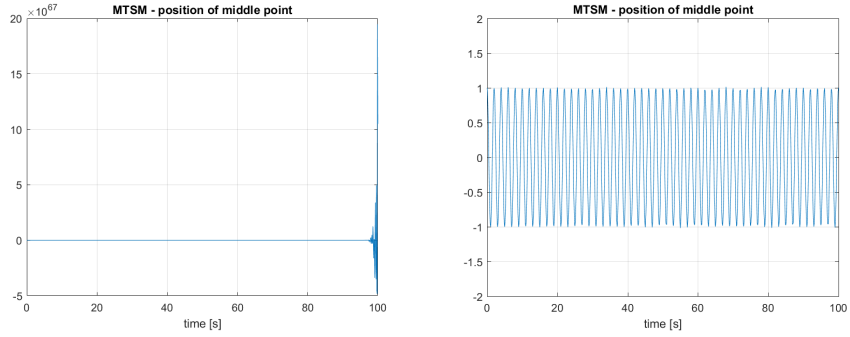


Fig. 1. Combined difference formulas – default precision 16 SD (left), default VPA precision 32 SD (right), order $N = 7$

The original work was presented in the conference ICNAAM 2017[1] [1].

References

1. Gabriela Nečasová, Václav Šátek, and Jiří Kunovský. Numerical Solution of Wave Equation Using Higher Order Methods. In *15th International Conference of Numerical Analysis and Applied Mathematics*, 2017.

[1] http://icnaam.org

Towards Shape Analysis in 2LS POSTER

Viktor Malík

Brno University of Technology
Faculty of Information Technology
Brno, Czech Republic
imalik@fit.vutbr.cz

2LS is a tool combining multiple approaches to formal analysis into a single, scalable framework. It integrates different program analysis techniques to work simultaneously and exchange information, which both allows it to analyse different classes of program properties as well as to identify errors in programs. One of the important features that 2LS currently lacks is to perform shape analysis of programs that work with dynamic data structures, i.e. to analyse reachable shapes of dynamic data structures. 2LS already contains good numerical analysis and its combination with shape analysis could bring new possibilities for analysing interesting program properties.

The goal of this project is to propose a shape analysis suitable for the specific context of 2LS, which differs from what is common in other frameworks. These are mostly based on some form of abstract interpretation that symbolically executes a given program using abstraction to summarize reachable sets of program states. 2LS differs from these tools in two important aspects: (1) it is heavily based on the bit-vector logic, ultimately using SAT solving, and (2) it uses a significantly different computation loop. This loop is based on combining k-induction, a notion of invariants based on so-called templates, and a rather specific form of abstract interpretation [1]. Incorporating shape analysis into this framework hence requires a rather specific solution.

In this project, we propose a solution to the above problem. In particular, we propose a novel domain for representing sets of reachable heap shapes that can be well integrated into the approach of 2LS. Namely, we represent sets of heap configurations using a concept of pointer access paths. This representation does not concretely describe the shape of the heap, it only expresses reachability of heap objects from variables in the analysed program via chains of pointers. Moreover, we propose all algorithms needed for integrating the domain into 2LS, both within intraprocedural as well as interprocedural analysis.

We have implemented part of this approach into 2LS and currently we are working on extending the method to handle more programs and on improving experimental results. After this is done, we plan to publish this work on a conference related to formal static analysis. The work is supported by the Czech Science Foundation (project 17-12465S), the internal BUT FIT project FIT-S-17-4014, and the IT4IXS: IT4Innovations Excellence in Science (LQ1602).

References

1. Brain, M., Joshi, S., Kroening, D., Schrammel, P.: Safety Verification and Refutation by k-Invariants and k-Induction. In: SAS'15. LNCS, Springer (2015) 145–161

Simulation For Symbolic Automata (POSTER)

Juraj Síč*
Faculty of Information Technology, Brno University of Technology, Božetěchova 1/2, 612 66, Brno, Czech Republic
juraj.sic@mail.muni.cz

Symbolic automata [4] are similar to classical automata with one big difference: transitions are labelled with predicates defined in separate logical theory. This allows usage of large alphabets while taking less space. In this work we are interested in computing simulation (a binary relation over states that shows whether a language accepted by one state is a subset of a language accepted by another) for these automata. This could be then used for reducing the size of automata without the need to determinize them first. There exist few algorithms for computing simulation over Kripke structures, which were then altered to work over labelled transition systems and classical automata. In [3] we have shown three ways how one of these algorithms [2] can be modified for symbolic automata and that by using simulation we can significantly reduce the size of the input automaton. We also compare the determinization of this reduced automaton with direct determinization and conclude that simulation can have a considerable impact on the runtime of determinization algorithm.

We are also currently investigating the possibility of adapting algorithm for classical automata [1] that improves efficiency by working with equivalence classes of the current approximation of simulation instead of with individual states. However, this algorithm is complex by itself and its adaptation to symbolic setting could be very intricate. To mitigate this problem and to separate the concern of computing simulation and handling symbolic transitions, we want to use the classical algorithm as it is or with minimal changes. Our idea is to use this algorithm as subprocedure with abstraction-refinement. The abstraction is defined by choosing a small set of symbols as those relevant for the simulation relation. In each refinement loop iteration, we would compute simulation with respect to the chosen symbols only, using the algorithm of [1]. We would then test whether the obtained relation is a simulation with respect to all symbols and either conclude the computation if yes or start another iteration with a larger set of chosen symbols if not.

References

[1] Gérard Cécé (2017): *Foundation for a series of efficient simulation algorithms*. In: *32nd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2017, Reykjavik, Iceland, June 20-23, 2017*, IEEE Computer Society, pp. 1–12, doi:10.1109/LICS.2017.8005069.

[2] Lucian Ilie, Gonzalo Navarro & Sheng Yu (2004): *On NFA Reductions*. In: *Theory Is Forever*, *Lecture Notes in Computer Science* 3113, Springer, pp. 112–124, doi:10.1007/978-3-540-27812-2_11.

[3] Juraj Síč (2017): *Simulation for Symbolic Automata*. Bachelor's thesis, Brno University of Technology, Brno. Available at `http://www.fit.vutbr.cz/study/DP/BP.php?id=19745`.

[4] Margus Veanes (2013): *Applications of Symbolic Finite Automata*. In: *Proceedings of the 18th International Conference on Implementation and Application of Automata, CIAA 2013*, *Lecture Notes in Computer Science* 7982, Springer, pp. 16–23, doi:10.1007/978-3-642-39274-0_3.

*Research supported by the Czech Science Foundation (projects 14-11384S, 16-24707Y, 17-12465S), the internal BUT FIT project FIT-S-17-4014, and the IT4IXS: IT4Innovations Excellence in Science (LQ1602).

Parameter Synthesis with PITHYA*(POSTER)

Nikola Beneš, Luboš Brim, Martin Demko, Matej Hajnal,
Samuel Pastva, and David Šafránek
Systems Biology Laboratory, Faculty of Informatics, Masaryk University
Botanická 68a, 602 00 Brno, Czech Republic,

{xbenes3,brim,xdemko,xhajnal,xpastva,safranek}@fi.muni.cz

Biological systems exhibit complex behaviour emerging from non-linear interactions among system components. A system can be specified in terms of an ODE (ordinary differential equations) model typically containing parameters which can significantly affect system behaviour. In general, it is difficult to obtain exact parameters values from experimental data.

The number of parameters and their interdependence make the identification of parameters values a hard task. A common approach is to use parameter estimation from time-series data. Such data might be of low resolution or even unavailable. Instead of estimating parameters from data, an alternative approach is to specify global hypotheses on system behaviour in terms of temporal properties [4] and to use *parameter synthesis methods* based on model checking [4], a verification technique proven by decades of use in computer science.

We present a *new high-performance tool Pithya*[1] [2] that implements state-of-the-art parameter synthesis methods [1, 3]. For a given ODE model, it allows to visually explore model behaviour with respect to different parameter values. Moreover, Pithya automatically synthesises parameter values satisfying a given property and visualises the results interactively. Such property can specify various behaviour constraints, e.g., maximal reachable concentration, time ordering of events, characteristics of steady states, presence of limit cycles, etc.

References

[1] Nikola Beneš, Luboš Brim, Martin Demko, Samuel Pastva & David Šafránek (2016): *Parallel SMT-Based Parameter Synthesis with Application to Piecewise Multi-Affine Systems*. In: *ATVA 2016*, *LNCS* 9938, Springer, pp. 192–208.

[2] Nikola Beneš, Luboš Brim, Martin Demko, Samuel Pastva & David Šafránek (2017): *Pithya: A Parallel Tool for Parameter Synthesis of Piecewise Multi-Affine Dynamical Systems*. In: *CAV 2017*, *LNCS* 10426, Springer, pp. 591–598.

[3] Nikola Beneš, Luboš Brim, Martin Demko, Samuel Pastva & David Šafránek (2016): *A Model Checking Approach to Discrete Bifurcation Analysis*. In: *FM 2016*, *LNCS* 9995, Springer, pp. 85–101.

[4] Edmund M. Clarke, Orna Grumberg & Doron A. Peled (2001): *Model checking*. MIT Press.

*This work has been supported by the Czech Science Foundation grant GA15-11089S and by the Czech National Infrastructure grant LM2015055.

[1] http://biodivine.fi.muni.cz/pithya/

Search-Based Testing Concurrent Java Programs Using the RoadRunner Analysis Framework (POSTER)

David Kozák Bohuslav Křena Hana Pluháčková Tomáš Vojnar

Faculty of Information Technology, Brno University of Technology,
Božetěchova 1/2, 612 66 Brno, Czech Republic

xkozak15@stud.fit.vutbr.cz

{krena,ipluhackova,vojnar}@fit.vutbr.cz

The main topic of this research is testing of concurrent Java programs. Concurrency errors often manifest rarely. To increase a chance to spot such errors, a technique called noise injection can be used. This technique inserts extra instructions into the application under test to disturb the scheduler and thus to explore less common thread scheduling. Because noise injection can be parametrized in many ways, a tool called SearchBestie[3] was created to handle noise-based testing as a search problem. SearchBestie used a tool called ConTest[1] for bytecode instrumentation and test execution. However, the development of ConTest has been discontinued. Therefore an alternative tool was necessary.

An open source tool called RoadRunner[2] has been chosen as a replacement for ConTest. This tool is being developed on the University of California at Santa Cruz and the Williams College. SearchBestie was connected with RoadRunner and the created infrastructure was evaluated on a set of benchmarks. The results showed that each tool is more effective on different benchmarks.

The previous version of the infrastructure used noise injection based on a random noise-placement selection. Since concurrent programs are non-deterministic, this approach provided good results. However the opportunity to select a specific set of program locations seemed as a very interesting area of research as well. Therefore new fine-grain noise-injection heuristics have been proposed and implemented. The heuristic *perProgloc* works with specific lines in code, *perObject* with attributes of objects in the program under test, *perClass* with classes and *perEventSet* with events such as variable accesses or lock accesses. Experiments proved that these heuristics achieve better results in most cases compared to random selection, however there was no silver bullet among them.

The current aim is to compare newly created heuristics in RoadRunner with ConTest. We also plan to experiment with different state space exploration strategies we have already used in connection with ConTest (such as Single-objective and Multi-objective Genetic algorithms and Boosted Decision Trees) to see which one works best with these new heuristics.

Acknowledgement. Supported by the Czech Science Foundation (project 17-12465S), AQUAS: Aggregated Quality Assurance for Systems by ECSEL (project 737475) and MŠMT (project 8A17001), the internal BUT FIT project FIT-S-17-4014, and the IT4IXS: IT4Innovations, Excellence in Science (LQ1602).

References

[1] O. Edelstein, E. Farchi, E. Goldin, Y. Nir, G. Ratsaby & S. Ur (2013): *Framework for Testing Multi-threaded Java Programs*. *Concurrency and Computation: Practice and Experience* 15, pp. 3–5.

[2] C. Flanagan & S. N. Freund (2010): *The RoadRunner dynamic analysis framework for concurrent programs*. *Program Analysis for Software Tools and Engineering (PASTE)*.

[3] B. Křena, Z. Letko, S. Ur & T. Vojnar (2010): *A Platform for Search-based Testing of Concurrent Software*. *PADTAD* 10.

(POSTER) Winning an Unwinnable Game

Luděk Matyska

Faculty of Informatics, Masaryk University, Czech Republic
makk@mail.muni.cz

Abstract. We study randomness in the setting of quantum information. In this poster we use the magic square, a two party game, to demonstrate the basic principles of quantum infomation. This game is impossible to win with certainty in the classical setting. The main objective is to present the quantum phenomenon, entanglement, as a key to solving the magic square game with probability 1. Our ongoing work is using this phenomenon to generate, verify and use randomness, a valuable resource even in classical computer science.

Bi-Abduction for Low-Level Separation Logic Focused on List Manipulation (POSTER)*

Jens Katelaan[1], Adam Rogalewicz[2], Veronika Šoková[2], Tomáš Vojnar[2], Georg Weissenbacher[1], and Florian Zuleger[1]

[1] TU Wien, Vienna, Austria
[2] FIT, Brno University of Technology, IT4Innovations Centre of Excellence, Czech Republic

Abstract. The motivation of this work in progress is to improve possibilities of analyzing low-level system programs manipulating dynamic data structures. Namely, we aim at supporting analysis of open programs of this kind, i.e., analysis of code fragments without a need to supply their environment (test harness). Indeed, constructing a suitable environment is a tedious job, requiring a deep knowledge of the code to be verified.

In order to achieve the above goal, we aim at extending the abductive approach of [1], based on separation logic, to be able to cope with list-manipulating programs using different kinds of low-level memory operations often present in system code. Such features include pointer arithmetic, address alignment, block operations, a need to work block sizes, etc.

So far, we have defined (and present in the poster) the syntax of a low-level separation logic for our domain where points-to assertions describe contiguous memory blocks of various sizes. Moreover, we have also proposed a preliminary version of abduction rules for formulas in our logic.

References

1. Calcagno, C., Distefano, D., O'Hearn, P.W., Yang, H.: Compositional Shape Analysis by Means of Bi-Abduction. Journal of the ACM 58(6), ACM (2011) 1–66

* Supported by the Czech Science Foundation project 17-12465S, the IT4IXS: IT4Innovations Excellence in Science project (LQ1602), and the internal BUT project FIT-S-17-4014.

Comparing Languages and Reducing Automata Used in Network Traffic Filtering (POSTER)*

Vojtěch Havlena
FIT, Brno University of Technology, IT4Innovations Centre of Excellence, Czech Republic
ihavlena@fit.vutbr.cz

The recent growth of cyber-crime, in particular intrusion into computer networks, has greatly increased the demand for systems detecting malicious network traffic. Due to the increasing speed of networks, network traffic filtering cannot be implemented in software, and some hardware pre-filtering is needed. These hardware solutions implement finite automata describing suspicious payloads of packets. However, computing resources available in the hardware accelerators are restricted, and so methods for reducing the size of the automata must be used.

Classical reductions that preserve language need not be sufficient. Therefore, we propose an approach based on an approximate reduction of the nondeterministic finite automata, which may change the language of the automata. In order to control the reduction in a systematic way, we propose a probabilistic distance between languages that utilizes probabilistic distribution of the input strings represented by a probabilistic automaton.

Subsequently, we propose automata reductions that are based on either under-approximating the languages of automata by pruning their states, or over-approximating the languages by introducing new self-loops (and pruning redundant states later). The reductions can be parameterized by the maximal error that is allowed, which is given with respect to the desired distance between the language of the input automaton and the language of the reduced automaton.

This poster presents work in progress. Preliminary version of this work was introduced in [1]. The results are joint work with Milan Češka, jr., Lukáš Holík, Ondřej Lengál, and Tomáš Vojnar.

References

[1] Vojtěch Havlena (2017): *Comparing Languages and Reducing Automata Used in Network Traffic Filtering*. Master's thesis, Brno University of Technology, Faculty of Information Technology.

*The work is supported by the Czech Science Foundation (projects 16-17538S and 16- 24707Y), the internal BUT FIT project FIT-S-17-4014, and the IT4IXS: IT4Innovations Excellence in Science (LQ1602)