Stefan Ramson, Tom Braun, Gabriela Pipa, Toni Mattis (editors)

Proceedings of the 2020 Joint Workshop of the German Research Training Groups in Computer Science

Dagstuhl

June 8–9, 2020

DFG Deutsche Forschungsgemeinschaft

Preface

Since 2007, researchers of the German Research Training Groups (RTG), funded by the Deutsche Forschungsgemeinschaft (DFG) in the field of computer science, meet annually at Schloss Dagstuhl – Leibniz Center for Informatics, one of the world's premier venues for computer science-related seminars. The goal of these workshops is to maintain an interchange of ideas and experiences and to strengthen the connection within the German computer science community. These events allow graduate students to present and discuss their current research topics and scientific results among each other and with invited guests of the computer science community.

This year's meeting was impacted by the Covid-19 pandemic – thus we changed it to an online event to maintain the ongoing exchange in the German research community. We transformed the workshop to an online format using the BigBlueButton platform, shortened the event from 3 to 2 days, and allowed for RTGs to introduce themselves and Ph.D. students present their projects and discuss their posters. Three invited speakers held keynote-talks. Also, the DFG contributed to this special event with an informative presentation on funding opportunities and a discussion session. Even a "chat-café" had been opened to offer a little "Dagstuhl" feeling... However, **we all hope to see each other soon again in the wonderful Schloss Dagstuhl – one of the best places to meet and talk!**
The organizers:
Gabriela Pipa, Toni Mattis, and Stefan Ramson

This year's meeting had been organized jointly by the RTG 2340 "Computational Cognition" from Osnabrück University and the HPI Research Schools from the University of Potsdam. These proceedings contain abstracts of the Ph.D. projects of the RTG graduate students within the computer science community and provide insight into current research trends in Germany.

Contents

GRK 1763: Quantitative Logics and Automata

Prof. Dr.-Ing. Franz Baader
Email: franz.baader@tu-dresden.de
Technische Universität Dresden and Universität Leipzig
Internet: https://lat.inf.tu-dresden.de/quantla/

Both automata and logics are employed as modelling approaches in Computer Science, and these approaches often complement each other in a synergetic way. In Theoretical Computer Science the connection between finite automata and logics has been investigated in detail since the early nineteen sixties. This connection is highly relevant for numerous application domains. Examples are the design of combinatorial and sequential circuits, verification, controller synthesis, knowledge representation, or natural language processing. Classical logics and automata models support modelling of qualitative properties. For many Computer Science applications, however, such purely functional models are not sufficient since also quantitative phenomena need to be modelled. Examples are the vagueness and uncertainty of a statement, length of time periods, spatial information, and resource consumption. For this reason, different kinds of quantitative logics and automata models have been introduced. However, their connection is not as well-investigated as in the classical qualitative case. The aim of this research training group is to investigate quantitative logics and automata as well as their connection in a thorough and complete manner, using methods from Theoretical Computer Science. As possible applications we consider problems from verification, knowledge representation, and constraint solving.

The qualification and supervision concept aims at providing the doctoral students with as much freedom as possible for their research work, while optimally preparing them for and supporting them in their research activities. The curriculum consists — in addition to the weekly research seminar — of Reading Groups, a Summer School in the first year of every cohort, advanced lectures, and an annual workshop. In addition, the doctoral students participate in soft-skills courses offered by the participating universities.

Explication of Description Logic Reasoning

Christian Alrabbaa (alrabbaa@tu-dresden.de)
Supervisor: Prof. Dr.-Ing. Franz Baader, PD. Dr.-Ing. Anni-Yasmin Turhan

Cyber-physical systems that interact autonomously among each other, or with users, must continuously make decisions based on sensor data, user input, previously provided knowledge or even knowledge acquired during runtime. To make such systems perspicuous, they need to be able to explain their decisions to the user or, after something has gone wrong, to the accident investigators.

Knowledge representation based on Description Logics (DLs) can be used to provide descriptions of the environment and the current states of the system, as well as background information about conditions that these states satisfy. Using the knowledge usually involves reasoning about the knowledge, i.e., computing consequences, which can then be used by other components of the system to make decisions. In order to explicate the behavior of the system, one thus also needs to explicate the components that reason about the knowledge.

The main objective of this project is to develop techniques for explicating consequences and non-consequences of DL-reasoning in a way that can adapt to different user types. A consequence can, for example, be explicated by showing a proof of the consequence in an appropriate calculus, whereas a non-consequence can be demonstrated using an appropriate counter-interpretation. One of the problems that needs to be overcome in this setting is that proofs and counter-interpretations may become very large, and thus one must develop techniques that can condense them. This gives rise to the following questions: What are the good proofs and counter-interpretations in the context of explicability; how can we compute them, and how expensive is it to do so. Furthermore, proofs and counter-interpretations for DL consequences can be seen as different types of graphs, hence we develop visualisation techniques that support the user in understanding why a certain graph, that represents a proof, backs the consequence, whereas another, that represents a counter-interpretation, really refutes the consequence.

We have introduced a general framework in which proofs are represented as hypergraphs. We have investigated the complexity of deciding whether a certain consequence has a proof of size at most n, and presented an approach for generating proofs for expressive Description Logics. [1]

[1] C. Alrabbaa, F. Baader, S. Borgwardt, P. Koopmann, and A. Kovtunova, "Finding Small Proofs for Description Logic Entailments – Theory and Practice", in the proceedings of the International Conference on Logic for Programming, Artificial Intelligence and Reasoning, LPAR-23 (To appear)

Automatic Extraction of Matrix-Space Models of Language

Shima Asaadi (shima.asaadi@tu-dresden.de)
Supervisor: Prof. Dr. Sebastian Rudolph, Prof. Dr.-Ing. Heiko Vogler

Quantitative models of language have been the subject of intense research in the last two decades: statistical and vector-space models and their variations are prominently used in different applications of natural language processing (NLP). In the application of meaning representation of words in NLP, Vector-Space Models (VSMs) embody the distributional hypothesis of meaning, according to which words tend to have similar meaning if they (co-)occur in similar contexts. Recently, much attention has been paid to the meaning representation of complex text structures (e.g. compositional phrases). Among recent compositional distributional models, Rudolph and Giesbrecht(2010) proposed a Compositional Matrix-Space Model (CMSM) which is based on matrix multiplication of word matrices to obtain the meaning representation of text in a matrix space. They showed that CMSM subsumes many of the known models, both quantitative (vector-space models) and qualitative (regular languages). Although this framework has been shown to be a theoretically elegant way to represent compositional aspects of language, automatic acquisition of such models is required, so they can be used in NLP applications.
In this work, we first showed a correspondence between CMSMs and Weighted Automata (WA).[1] Based on this mapping, word matrices can be obtained by learning WA (e.g., using spectral learning methods). However, these methods turned out to not scale well. A promising alternative approach to learning CMSMs is supervised machine learning techniques such as linear regression with gradient descent optimization algorithms. Thus, we developed a task-specific (sentiment analysis) approach for learning CMSMs using linear regression methods.[2] The proposed method learns the word matrices to capture the compositional sentiment value of phrases using the matrix product in sentiment analysis. Our method outperforms a previous approach for learning CMSMs in this task. Finally, to examine CMSMs on semantic composition in general and compare with existing compositional VSMs, we proposed a fine-grained semantic relatedness dataset.[3]

[1] S. Asaadi and S. Rudolph, "On the Correspondence between Compositional Matrix-Space Models of Language and Weighted Automata" in *Proceedings of StatFSM 2016*, 2016, pp. 70–74.

[2] S. Asaadi and S. Rudolph, "Gradual Learning of Matrix-Space Models of Language for Sentiment Analysis" in *Proceedings of RepL4NLP*, 2017, pp. 70–74.

[3] S. Asaadi, S. M. Mohammad, and S. Kiritchenko, "A Fine-Grained Semantic Relatedness Dataset for English Bigrams: A Resource For Examining Semantic Composition" in *Proceedings of NAACL-HLT*, 2019, pp. 505–516.

Practical Reasoning in Description Logics with Expressive Cardinality Constraints

Filippo De Bortoli (filippo.de_bortoli@tu-dresden.de)
Supervisor: Prof. Dr.-Ing. Franz Baader, Prof. Dr. Sebastian Rudolph

Description Logics (DLs)[1] are a prominent class of logic-based knowledge representation languages that are used to formalize ontologies and perform automated reasoning over them. Applications of such ontologies can be found in many domains, such as medicine, biology, and the Semantic Web. A relevant concept in the domain of interest is formalized in DLs in terms of necessary and sufficient conditions that an *individual* in such a domain must fulfill to belong to the concept. Terminological axioms can then be used to constrain the interpretation of concepts.

Simple counting quantifiers that can be used to restrict the number of individuals with certain properties that belong to a concept or are related to an individual in a concept have been employed in DLs for more than two decades under the respective names of *cardinality restrictions on concepts* and *number restrictions*. Recently, the expressivity of such quantifiers has been considerably extended by allowing to impose set and cardinality constraints stated in the quantifier-free fragment of Boolean Algebra with Presburger Arithmetic (QFBAPA)[2]. In spite of the increased expressivity[3], it has been proved that this extension does not increase the complexity of reasoning. However, the algorithms used to establish these complexity result are not suitable for implementation purposes, as they are based on non-deterministic guessing or show a best-case behavior that is identical to the worst-case complexity of the problem.

One task of my research project is to investigate the expressivity of DLs with expressive cardinality constraints in detail, both for the case of finite and infinite models. On the more practical side, the main task is to develop decision procedures for such DLs that overcome the problems mentioned above, and thus can be used to implement reasoning services with an acceptable runtime for application ontologies. In particular, the goal is to enhance the existing techniques by using well-established methods from other fields, such as satisfiability modulo theories (SMT) and integer linear programming (ILP). One notable example is *column generation*, an ILP method that is useful in solving systems of linear (in)equations with a large number of variables.

[1] Franz Baader, Ian Horrocks, Carsten Lutz, Ulrike Sattler: An Introduction to Description Logic. Cambridge University Press 2017

[2] Franz Baader: Expressive Cardinality Restrictions on Concepts in a Description Logic with Expressive Number Restrictions. ACM SIGAPP Applied Computing Review, 19:5–17, 2019.

[3] Franz Baader and Filippo De Bortoli: Description Logics That Count, and What They Can and Cannot Count. In Laura Kovacs, Konstantin Korovin, and Giles Reger, editors, ANDREI-60. Automated New-era Deductive Reasoning Event in Iberia, volume 68 of EPiC Series in Computing, pages 1–-25. EasyChair, 2020.

Sequentiality of Group-Weighted Tree Automata

Frederic Dörband (frederic.doerband@tu-dresden.de)
Supervisor: Prof. Dr.-Ing. Heiko Vogler, Prof. Dr. Manfred Droste

This is joint work with K. Stier (Uni Leipzig) and T. Feller (TU Dresden).

In Daviaud et al.[1], the concept of group-weighted (string) automata is introduced. This concept of a group-weighted automaton can be embedded into the concept of seimring-weighted automata. The ground set of the semiring is the set of finite subsets of the group, the multiplication is the group operation lifted to sets and the addition is union of finite sets.

Let $k \in \mathbb{N}_+$ and let $\mathcal{A}$ be a group-weighted automaton. Daviaud et al. introduce three properties: $\mathcal{A}$ is k-sequential (if $\mathcal{A}$ is equivalent to a union of k sequential weighted automata), $[\![\mathcal{A}]\!]$ satisfies the Lipschitz property of order k (see Definition 3 in Daviaud et al.), and $\mathcal{A}$ satisfies the branching twinning property of order k (see Definition 4 in Daviaud et al.). The main theorem in Daviaud et al. states the following: $\mathcal{A}$ is k-sequential iff $[\![\mathcal{A}]\!]$ satisfies the Lipschitz property of order k iff $\mathcal{A}$ satisfies the branching twinning property of order k.

The proof is an inductive proof over k and Béal and Carton[2] supply the induction base $k = 1$.

The field of determinisation of weighted automata is very sparsely explored. Many results cover only very limited weight structures and supply only sufficient conditions for determinisability. The presented literature, however, provides a full characterization of sequentiality of group-weighted automata. We believe that the proof of Daviaud et al. has a high potential for reusability and generalisability.

We want to lift Daviaud et al. to the case of group-weighted tree automata. In order to do this, we have first proven Béal and Carton for this automaton model. Our next step will be to lift the remaining inductive proof from Daviaud et al.

Moreover, we have compared different notions of "twinning property" from the existing literature with the twinning property we adapted from Daviaud et al. The result is, that all notions coincide for our automaton model.

We believe that our new understanding of Daviaud et al. for the tree case will help us find more general classes of semirings for which we can show an equivalence between the twinning property and sequentiality.

[1] Laure Daviaud et al., "Degree of sequentiality of weighted automata," FOSSACS 2017, vol. 10203 of LNCS, pages 215–230, 2017

[2] Marie-Pierre Béal and Olivier Carton, "Determinization of transducers over finite and infinite words," Theoretical Computer Science, vol. 289(1), pages 225–251, 2002

Weighted Pushdown Automata and Logics for Infinite Processes

Sven Dziadek (dziadek@informatik.uni-leipzig.de)
Supervisor: Prof. Dr. Manfred Droste, Prof. Dr.-Ing. Franz Baader

The first part of my thesis will deal with weighted ω-pushdown automata. Pushdown automata are of general interest because their recognized languages, the context-free languages, are used for describing and parsing of programming languages.

An extension of pushdown automata are ω-pushdown automata handling infinite words. Cohen, Gold[1] published some major results about ω-pushdown automata including various recognition modes such as Büchi and Muller acceptance.

While context-free languages are widely used for parsers, it is in some contexts important to differentiate between multiple possible parse trees. This quantitative distinction can be accomplished by adding weights. Weighted pushdown automata were introduced by Kuich, Salomaa[2].

My work is based on Droste, Kuich[3] and Droste, Ésik, Kuich[4]. They combine ω-pushdown automata with weighted pushdown automata into the new automaton model *weighted ω-pushdown automata*. Additionally to the automaton, they provide two further characteristics for the newly created class of languages: algebraic systems are a generalization of context-free grammars and ω-algebraic expressions generalize regular expressions.

Another representation of language classes additionally to automata and grammars are logics. For finite automata, this equivalence dates back to Büchi-Elgot and Trakhtenbrot. For weighted finite automata over ω-words, Droste, Meinecke[5] introduced an equivalent monadic second-order (MSO) logic.

My part is to find an equivalent MSO logic for weighted ω-pushdown automata. I will use the automaton model defined in Droste, Ésik, Kuich[4] and adapt the MSO logic defined in Droste, Perevoshchikov[6] for weighted timed pushdown automata to form an equivalence.

---

[1] R. S. Cohen, A. Y. Gold, "Theory of ω-Languages I: Characterizations of ω-Context-Free Languages". *Journal of Computer and System Sciences*, vol. 15(2), pp. 169–184, 1977.

[2] W. Kuich, A. Salomaa, "Semirings, Automata, Languages", *EATCS Monographs on Theoretical Computer Science*, vol. 5, Springer, 1986.

[3] M. Droste, W. Kuich, "A Kleene Theorem for Weighted ω-Pushdown Automata", *Acta Cybern.*, vol. 23(1), pp. 43-59, 2017.

[4] M. Droste, Z. Ésik, W. Kuich, "The Triple-Pair Construction for Weighted ω-Pushdown Automata", *AFL*, pp. 101-113, 2017.

[5] M. Droste, I. Meinecke, "Weighted Automata and Weighted MSO Logics for Average and Long-Time Behaviors", *Information and Computation*, vol. 220, pp. 44–59, 2012.

[6] M. Droste, V. Perevoshchikov, "Logics for Weighted Timed Pushdown Automata", *Fields of Logic and Computation II*, Springer, pp. 153–173, 2015

Model-Theoretic Characteristics of Decidable Knowledge Representations

Thomas Feller (thomas.feller@tu-dresden.de)
Supervisor: Prof. Dr. Sebastian Rudolph

Decidability is a crucial property for automated reasoning support for knowledge representation (KR) formalisms. Therefore, significant research effort is spent on the identification of very expressive, yet decidable, formalisms from language families such as description logics or existential rules. In many cases, the decidability of these formalisms can be established by abstract model-theoretic means (such as the finite model property, the tree-model property etc.). At the core of the current PhD project is the identification of a very general model-theoretic notion which subsumes bounded tree-width but also encompasses formalisms for which decidability is hitherto only known to follow from proof-theoretic principles. Such an abstract principle is then expected to give rise to new concrete decidable classes of very expressive KR formalisms. In the course of the last year, a candidate notion has been uncovered. Now the focus lies on making this notion fruitful for application to the aforementioned problem.

Weighted Alternating Finite Automata

Gustav Grabolle (grabolle@informatik.uni-leipzig.de)
Supervisor: Prof. Dr. Manfred Droste, Prof. Dr.-Ing. Heiko Vogler

Several different concepts of alternation in weighted finite automata have been proposed[1][2]; most recently, a general model for weighted alternating finite automata (WAFA) with weights taken from arbitrary, commutative semirings was introduced[3]. Nevertheless, the concepts of alternation in weighted automata remains sparsely investigated.

This research project aims to analyze the expressive power of WAFA. To this purpose, we characterized the class of quantitative languages recognized by WAFA via a Nivat like theorem and via a weighted logic based on weighted MSO for trees[4]. We could prove decidability of equivalence for WAFA over zero-sum free semirings, as well as the rationals. Moreover, we could show that in general WAFA are less expressive than unrestricted weighted MSO for words.

Next, we considered restrictions of WAFA. This led to the introduction of leveled automata. In weighted finite automata we assign to each transition a constant; we call these 1-level automata. For an $(n+1)$-level automaton we assign to each transition an n-level automaton. Then, during a run the weight of this transition is equal to the weight of the assigned n-level automaton on the remainder of the word. This hierarchy of automata corresponds to a hierarchy of classes of weighted languages. Moreover, for many prominent semirings such as $\mathbb{Z}$, or $\mathbb{R}$ this hierarchy is strict. We introduced a new logic based on weighted LDL introduced in [5] and proved that it is expressively equivalent to leveled automata. In addition, we showed that weighted languages recognized by leveled automata are a proper subclass of weighted languages recognized by WAFA. These proofs are constructive, hence we can reduce weighted equivalence for our new logic to the corresponding problem for WAFA.

As a further step we want find a fragment of weighted MSO which is as expressive as leveled automata. Furthermore, we want to examine WAFA for quantitative ω-languages and quantitative tree-languages and compare them to their non-alternating counterparts.

---

[1] Chatterjee, Krishnendu and Doyen, Laurent and Henzinger, Thomas A., "Alternating Weighted Automata", *Fundamentals of Computation Theory* (eds. Kutyłowski, Mirosław and Charatonik, Witold and Gębala, Maciej), p. 3–13, 2009

[2] Almagor, Shaull and Kupferman, Orna, "Max and Sum Semantics for Alternating Weighted Automata", *Automated Technology for Verification and Analysis* (eds. Bultan, Tevfik and Hsiung, Pao-Ann), p. 13–27, 2011

[3] Kostolányi, Peter and Mišún, Filip, "Alternating weighted automata over commutative semirings", *Theoretical Computer Science*, vol. 740, p. 1–27, 2018

[4] Droste, Manfred and Vogler, Heiko, "Weighted tree automata and weighted logics", *Theoretical Computer Science*, vol. 366, p. 228–247, 2006

[5] Droste, Manfred and Rahonis, George, "Weighted Linear Dynamic Logic" *Proc. of 7th GandALF*, pp. 149–163, 2016

Polynomial-Time Combinations of Decision Procedures for Constraint Satisfaction Problems

Johannes Greiner (johannes.greiner@tu-dresden.de)
Supervisor: Prof. Dr. Manuel Bodirsky, Prof. Dr.-Ing. Franz Baader

A Constraint Satisfaction Problem (CSP) of a relational structure $\mathbb{A}$, such as $(\mathbb{Q}; <, \neq)$, is the computational problem of deciding the satisfiability of a given primitive positive formula in $\mathbb{A}$. A primitive positive formula is a conjunction of atomic formulas where some variables can be existentially quantified, for instance $\exists x_1, x_2 \colon x_1 < x_3 \wedge x_4 \neq x_2$. Any decision problem is polynomial-time equivalent to CSP($\mathbb{A}$) for some $\mathbb{A}$[1]. My PhD project is concerned with the borderline between polynomial-time tractability and NP-hardness of CSP($\mathbb{A}$), where $\mathbb{A}$ has an infinite domain and the theory of $\mathbb{A}$ has only one countable model up to isomorphism, i.e. $\mathbb{A}$ is ω-categorical. More specifically, I am interested in structures $\mathbb{A}$ that have the same CSP as the combination of two theories, i.e., CSP($T_1 \cup T_2$), where T_1, T_2 are (complete) theories of ω-categorical structures with disjoint signatures. The CSP of a theory T over a signature τ is defined as the computational problem of deciding whether there is some model for $T \cup \phi$, where ϕ is a primitive positive τ-sentence.

Such combinations come up in program verification and decision procedures for them are used in SMT-solvers ("satisfiability modulo theories"). Furthermore, CSP($T_1 \cup T_2$) where T_1, T_2 are the theories of two structures $\mathbb{A}, \mathbb{B}$ respectively, is interesting algorithmically because there is hope to combine the algorithms for CSP($\mathbb{A}$) and CSP($\mathbb{B}$) so that they solve CSP($T_1 \cup T_2$).

A major tool in my project is the usage of relational structures which have the same CSP as CSP($T_1 \cup T_2$). These structures are called generic combinations and help to treat the problem with the "universal-algebraic approach", which uses methods of universal algebra and model-theory to classify families of structures according to the complexity of their CSP. The universal-algebraic approach was an essential tool in the recently finished complexity classification for CSPs of structures with finite domain, proving a conjecture of Feder and Vardi which has been open for more than 20 years.

So far, we have discovered a class where "convexity" characterizes the borderline between polynomial-time tractability and NP-hardness[2] and we prepare further publications dealing with reducts of first-order expansions of unary structures and of the rationals with strict order. These will include polynomial-time tractable cases which are not convex.

[1] Manuel Bodirsky and Martin Grohe, "Non-dichotomies in Constraint Satisfaction Complexity", Proceedings of the 35th International Colloquium on Automata, Languages, and Programming (ICALP 2015), pages 184-196, 2008

[2] Manuel Bodirsky and Johannes Greiner, "The Complexity of Combinations of Qualitative Constraint Satisfaction Problems", Logical Methods in Computer Science, Volume 16, Issue 1 (February 20, 2020) lmcs:6129

Weighted Automata with Storage

Luisa Herrmann (luisa.herrmann@tu-dresden.de)
Supervisor: Prof. Dr.-Ing. Heiko Vogler, Prof. Dr. Manfred Droste

Due to the large number of upcoming new automata models in the 1960s, Dana Scott advocated[1] a homogeneous point of view on sequential programs working on machines. There, a program is a flowchart over a set of predicate symbols and of (partial) function symbols, and a machine consists of a memory set and the interpretation of the predicate and function symbols as predicates and functions on the memory set. In this research project we take up this concept and call it *finite-state automata with storage*, where the finite-state automata correspond to sequential programs and storages correspond to machines.

Moreover, we extend the concept of automata with storage in two steps: after introducing K*-weighted automata with storage*, where K is a unital valuation monoid, we developed this model to that of K*-weighted tree automata with storage* where K is a *multioperator monoid*. Multioperator monoid-weighted tree automata extend usual semiring-weighted tree automata by generalizing the product by allowing arbitrary operations from some Σ-algebra. The aim of this research project is the *theoretical investigation* of weighted (tree) automata with storage regarding their closure properties and by extending classical characterizations.

After investigating weighted automata with storage[2] (among others, we proved closure properties, showed a Chomsky-Schützenberger result, and provided a logical characteriation), we extended our model to the case of an infinite alphabet[3]. Moreover, also for the tree case we took a comprehensive examination of this model[4], including a characterization by decomposition and by extended MSO logic. Additionally, I proved a homomorphic closure property for the weighted tree languages recognized by linear weighted tree automata with storage. Finally, apart from a storage, I investigated representable weighted tree languages and showed a Medvedev characterization[5].

This research project will be finished soon as I will submit my dissertation within a short time.

---

[1] D. Scott, "Some definitional suggestions for automata theory", J. Comput. System Sci., vol. 1, p. 187–212, 1967

[2] L. Herrmann, M. Droste, and H. Vogler, "Weighted Automata with Storage", Information and Computation, vol. 269, 2019

[3] L. Herrmann and H. Vogler, "Weighted Symbolic Automata with Data Storage", Developments in Language Theory - 20th International Conference, Lecture Notes in Computer Science, vol. 9840, p. 203–215, 2016

[4] Z. Fülöp, L. Herrmann, and H. Vogler, "Weighted Regular Tree Grammars with Storage", Discrete Mathematics and Theoretical Computer Science, vol. 20, 2018

[5] L. Herrmann, "A Medvedev Characterization of Recognizable Tree Series", Developments in Language Theory - 21st International Conference, Lecture Notes in Computer Science, vol. 10396, p. 210–221, 2017

Model Transformation in Description Logic

Willi Hieke (willi.hieke@tu-dresden.de)
Supervisor: PD. Dr.-Ing. Anni-Yasmin Turhan, Prof. Dr.-Ing. Heiko Vogler

In the field of knowledge representation and reasoning, description logics are commonly used to design and reason about ontologies. Various techniques have been introduced to solve reasoning problems, the most widely used among them being tableau algorithms. These algorithms are employed in highly optimized reasoner systems, which return the first model they find by their strategy optimized for low run-time. However, these models need not look intuitive or natural to ontology users, hampering human understanding of entailments or concepts. Next to explanation purposes, ontology engineers might also require models that exhibit certain properties. For instance, presenting small models to users might ease comprehension of complex entailments inferred by reasoner systems.[1] Similarly, in order to present prototypical instances of some concepts of the knowledge base, acyclic models or models that only use parts of the signature might be more suitable than models computed by reasoner systems. Consequently, the main idea is to transform reasoner generated models into suitably shaped models.

While there is some related work on making entailments more intelligible for users of reasoner systems[2] and, just to give one example, work on computing minimal models for first-order logic[3], no general framework for transforming models has been introduced yet. We define and investigate such a model transformation framework focusing on description logic. Since description logics use unary and binary relations only, models can be represented as labeled directed graphs. The initial underlying transformation formalism of choice for transforming models is monadic second-order graph transductions[4] which provide a powerful tool to specify mappings from graphs onto graphs using logical formulae with free variables. We construct several model transductions, prove that they are model-preserving (with respect to a given ontology), show that they yield models admitting the desired property and analyze the computational complexity of applying the transductions. Future research addresses alternative model transformation formalisms such as graph rewriting systems.

---

[1] Matthew Horridge, Johannes Bauer, Bijan Parsia, and Ulrike Sattler, "Understanding entailments in OWL", in *Proceedings of the Fifth OWLED Workshop on OWL: Experiences and Directions (OWLED, CEUR)*, 2008.

[2] Johannes Bauer, Ulrike Sattler, and Bijan Parsia, "Explaining by example: Model exploration for ontology comprehension", in *Proceedings of the 22nd International Workshop on Description Logics (DL 2009)*, 2009.

[3] Peter Baumgartner, Alexander Fuchs, Hans de Nivelle, and Cesare Tinelli, "Computing finite models by reduction to function-free clause logic", *J. of Applied Logic*, vol. 7, no. 1, pp. 58–74, 2009.

[4] Bruno Courcelle, "Monadic second-order definable graph transductions: a survey", *Theoretical Computer Science*, vol. 126, no. 1, pp. 53-75, 1994.

Explications for Probabilistic Model Checking

Simon Jantsch (simon.jantsch@tu-dresden.de)
Supervisor: Prof. Dr. Christel Baier, PD. Dr. Karin Quaas

Computing systems have become increasingly more powerful over the last decades. Now they are entering more and more domains where their actions have potentially huge consequences, both economically and regarding human life. Examples of such systems include electronic voting systems, automated trading software and autonomously acting robots. While our capabilities to build such systems have increased steadily, our methods for *explaining* the behaviour of a system is lagging behind. This, however, is crucial in domains where safety and accountability is essential.

Our aim is to introduce new methods for computing and working with explications for probabilistic systems. A standard example of an explication is a counterexample: a witness to the violation of a property. Whereas the notion of counterexample is generally clear in classical systems, where a counterexample is usually a path violating the property, different types of counterexamples exist for probabilistic systems. A related notion is that of *certification*: if a system satisfies a given property it is desirable to have an easily verifiable proof of this fact.

As a first step, we have considered probabilistic reachability constraints in Markov decision processes. In this setting we have shown how *witnessing subsystems* (subsystems that by themselves carry enough probability to satisfy the reachability constraint, henceforth called WS), can be related to abstract, easily verifiable certificates.[1]. The main idea is to rephrase the probabilistic reachability constraint in terms of satisfiability of a linear inequation system. Vectors satisfying this system are easily verifiable certificates (we call them Farkas certificates, as Farkas lemma is a key technical tool that we use). We then observe that there is a connection between Farkas certificates and WS. In particular, from a Farkas certificate with k non-zero entries, a WS with k states can be constructed (and vice-versa). From this fact we derive new algorithms and heuristics for computing minimal (or small) WS.

The next step will be to extend this approach to richer classes of probabilistic systems and other types of properties. We will further investigate the approach of using tools from linear algebra for the generation of WS, and implement a tool that features the techniques developed so far.

We have also worked on translation algorithms from LTL to unambiguous Büchi automata[2], which are useful for probabilistic model checking, and could potentially be used in the generation of explications for ω-regular properties.

[1] Florian Funke, Simon Jantsch, Christel Baier, "Farkas certificates and minimal witnesses for probabilistic reachability constraints", to appear in *Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, 2020

[2] Simon Jantsch, David Müller, Christel Baier, Joachim Klein, "From LTL to Unambiguous Büchi Automata via Disambiguation of Alternating Automata", *Formal Methods Symposium (FM)*, 2019

Valued Constraint Satisfaction Problems over Infinite Domains

Simon Knäuer (simon.knaeuer@tu-dresden.de)
Supervisor: Prof. Dr. Manuel Bodirsky, Prof. Dr.-Ing. Franz Baader

Many computational problems can be seen as consistency checks for some given input set of restrictions. So the answer for such problems is either consistent or inconsistent. In the study of Valued Constraint Satisfaction Problems we generalize this concept to 'more consistent' or 'less consistent'.

We start with a fixed set D, the domain, and a set Γ of fixed functions from D^n to $\mathbb{Q} \cup \{\infty\}$, called the *language*. A *constraint* over some set of variables W is an expression of the form $f(x_1, \ldots, x_n)$ where $f \in \Gamma$ and $x_1, \ldots, x_n \in W$. An instance of VCSP$(D; \Gamma)$ is a set of variables W, together with a set Φ of constraints over W. Now the computational problem is to find a assignment to the variables of W in D, such that the sum over all constraints (evaluated with values under the assignment of the variables) is minimal. The complexity of this problem depends on Γ.

During the last 10 years, the study of VCSPs made great progress. A huge number of classification results and algorithmic techniques were developed. A famous result is the complete complexity classification for finite-domain VCSPs. The result states that these problems are NP-complete or polynomial-time tractable. These dramatic improvements were possible because of the usage of tools from universal algebra. One example of such a powerful tool is the concept of *fractional polymorphisms*, which is a quantitative version of the notion of polymorphisms. These polymorphisms are a well-established tool to study the complexities of many computational problems. One direction in the study of VCSPs is to consider infinite domains D. In this direction, the last years yielded classification results for the special cases when the cost functions are first-order definable in $(\mathbb{Q}, \leq, +, 1)$. Functions from this class are called *semilinear* or *piecewise linear*. Bodirsky, Mamino and Viola showed that the VCSPs of piecewise linear homogeneous submodular functions are tractable.[1]

The goal of this dissertation project is to find more conditions for NP-hardness and tractability of VCSPs on infinite domains. A first question would be whether VCSPs for semilinear submodular cost functions are in P. From a more general point of view it would be desirable to have an algebraic characterization of the expressive power of a VCSP language. The *expressive power* of a language Γ is the set of all functions that can be defined by minimizing over some variable subset of some objective function. In the study of finite domain VCSPs it turns out that one can describe the expressive power of a language by means of fractional polymorphisms. This result gives some hope to use fractional polymorphisms in the same way for infinite domains.

[1] M. Bodirsky, M. Mamino, C. Viola, "Submodular Functions and Valued Constraint Satisfaction Problems over Infinite Domain", *CSL 2018: 12:1-12:22*, ArXiv:1804.01710.

Expressiveness and Decidability of Weighted Automata and Weighted Logics

Erik Paul (epaul@informatik.uni-leipzig.de)
Supervisor: Prof. Dr. Manfred Droste, Prof. Dr.-Ing. Heiko Vogler

The goal of this project is to gain a deeper insight into the structure of different weighted automata models. The ambiguity of an automaton is a measure for the maximum number of accepting runs on a given input of an automaton. For example, if the number of accepting runs is bounded by a global constant for every input, we say that an automaton is finitely ambiguous. In the case that the number of accepting runs is bounded polynomially in the input size, we speak of polynomial ambiguity.

There are several reasons to consider the ambiguity of automata. First, ambiguity has been shown to play are role in common complexity and decidability problems. For instance, the equivalence problem for finitely ambiguous automata over the max-plus semiring is shown to be decidable, whereas for general non-deterministic automata over the max-plus semiring this problem is undecidable.

Second, we obtain a deeper insight into the structure of the automata. For example, it has been shown that finitely ambiguous word automata are essentially finite sums of unambiguous automata, i.e. automata that allow at most one accepting run for every word. Polynomially ambiguous word automata, one the other hand, are essentially (finite sums of) "chains" of unambiguous automata. These properties are particularly interesting in the weighted case, as determinizing weighted automata is only possible in special cases. I was able to obtain similar results for tree automata and use them to generalize a work by Kreutzer and Riveros[1] from words to trees, relating to each of the classes of deterministic, unambiguous, finitely ambiguous and polynomially ambiguous weighted tree automata a class of formulas from a weighted logic expressively equivalent to it.

Results obtained so far include the decidability of the equivalence, unambiguity, sequentiality, and finite sequentiality problems for finitely ambiguous max-plus tree automata.

[1] S. Kreutzer and C. Riveros, "Quantitative Monadic Second-Order Logic," in *28th Annual ACM/IEEE Symposium on Logic in Computer Science*, 2013.

Stochastic Shortest Path Problems

Jakob Piribauer (jakob.piribauer@tu-dresden.de)
Supervisor: Prof. Dr. Christel Baier, Prof. Dr.-Ing. Franz Baader

Many problems in the formal verification of probabilistic systems require the analysis of worst- or best-case resource consumption before a desirable state of the system is reached. These problems can usually be formulated as a *stochastic shortest path problem* on a *Markov decision process* and generalize the shortest path problem on a weighted directed graph. Instead of being able to choose a weighted edge leading to a successor state, a *scheduler* is allowed to choose a weighted action at each state. Each action determines a probability distribution according to which the successor state is chosen randomly.

In the classical setting, the aim is to determine a scheduler that minimizes the expected accumulated weight before reaching a goal state among all schedulers under which a goal state is reached with probability 1. However, the requirement that a goal state has to be reached almost surely is too restrictive for many applications. Important such applications include the semantics of probabilistic programs where no guarantee for almost sure termination can be given and fault-tolerance analysis (e.g., expected costs of repair mechanisms) in error scenarios that can appear with some positive, but small, probability.

In this project, non-classical variants of stochastic shortest path problems are studied: Namely, the optimization problems of conditional expectations, where the expected accumulated weight under the condition that a goal state is reached is considered, and partial expectations, where runs not reaching a goal state are assigned weight 0, are investigated. It was known that optimal conditional expectations can be computed in exponential time if all weights are non-negative.[1] A main result of this project is now that in general the optimization of partial and conditional expectations is at least as hard as the Skolem problem, a number-theoretic decision problem whose decidability has been open for many decades.[2] Nevertheless, the optimal values can be approximated in exponential time.[3] Furthermore, for related optimization problems, exponential-time algorithms under natural restrictions are provided while the general problems are shown to be Skolem-hard as well. These related problems include the optimization of the average satisfaction probability of linear temporal properties in the long-run of a system[4] and the conditional value-at-risk, an established risk measure, for accumulated weights.

[1] C. Baier, J. Klein, S. Klüppelholz, and S. Wunderlich. Maximizing the conditional expected reward for reaching the goal. In TACAS'17, volume 10206 of LNCS, pages 269–285. Springer, 2017.

[2] J. Piribauer and C. Baier. On Skolem-hardness and saturation points in Markov decision processes. In ICALP'20, to appear, 2020.

[3] J. Piribauer and C. Baier. Partial and Conditional expectations in Markov decision processes with integer weights. In FoSSaCS'19, volume 11425 of LNCS, pages 436–452. Springer, 2019

[4] C. Baier, N. Bertrand, J. Piribauer, and O. Sankur. Long-run Satisfaction of Path Properties. In LICS'19, pages 1–14. IEEE, 2019

Verifying Counter Systems with Bounded Model Checking

Danny Richter (drichter@informatik.uni-leipzig.de)
Supervisor: PD. Dr. Karin Quaas, Prof. Dr. Andreas Maletti,

In my doctoral studies, I analyse the computational complexity of verification problems for systems with counters and try to find algorithmic solutions to them. Simple systems of this kind can be modelled by one-counter automata (OCA). An OCA is a finite state machine, equipped with a single counter that takes positive integer values, which can be incremented, decremented and tested for being 0. The study of quantitative extensions of Linear Temporal Logic is an active field of research. Classical verification problems such as the satisfiability and the model checking problem of OCA for such logics have been shown to be undecidable in most cases. Current research concentrates on finding suitable restrictions of the problems to regain decidability.[1]

One restriction could be a dynamic bound on the length of the considered words (resp. computations of the OCA). I try to provide techniques for the bounded verification of systems, which can be modelled by OCA and specified by these logics. This approach is called bounded model checking[2] (BMC) and has gained popularity, because in many applications the state space becomes too large to practically handle complete verification. Since BMC yields counter-examples, it is possible to use it for debugging. This is eminently important when the modelling of systems and specifications requires a framework for which verification problems are undecidable.

On the other hand it is possible to use BMC for complete verification as well. There is a branch of research that is concerned with finding ways to compute completeness thresholds (CT) for a given class of automata models and a logic. A CT is a bound k, such that if no counter-example of length smaller than k is found, then there does not exist a counter-example of arbitrary length either and the formula holds over all infinite computations of the model. Whilst this has been studied for Büchi automata and LTL[3], it is untouched for frameworks capable of modelling infinite state systems.

Furthermore, I try to extend a known result for a specific type of systems[4] to a broader class of systems. This would yield a number of new complexity results in an elegant way and highlight interesting connections between the different types of systems.

---

[1] S. Demri and A. Sangnier, "When Model-Checking Freeze LTL over Counter Machines Becomes Decidable", *FOSSACS*, p. 176–190, 2010.

[2] A. Biere, A. Cimatti, E. M. Clarke, O. Strichman and Y. Zhu, "Bounded model checking", *Advances in Computers*, vol. 58, p. 117–148, 2003.

[3] D. Kroening, J. Ouaknine, O. Strichman, T. Wahl, J. Worrell, "Linear Completeness Thresholds for Bounded Model Checking", *CAV*, p. 557–572, 2011.

[4] M. Hague and A. W. Lin, "Model Checking Recursive Programs with Numeric Data Types", *Computer Aided Verification*, p. 743–759, 2011.

User-Definable Concrete Domains

Jakub Rydval (jakub.rydval@tu-dresden.de)
Supervisor: Prof. Dr.-Ing. Franz Baader

Concrete domains were introduced to description logic with the intention to define concepts using predefined concrete objects (e.g. numbers, strings) and predicates (e.g. $<$, prefix-order). Until now, description logic systems have only used a single fixed concrete domain, that is, the user cannot have utilized a different concrete domain without changing the system itself. The long-term goal of my research project is the development of description logic systems with concrete domains that can be specified by the user in a certain defining language. Particularly promising for this purpose are *automatic structures* from the algorithmic model-theory and *homogeneous structures* from the classical model theory.

A relational structure $\mathbb{A}$ is *automatic* if its elements can be represented as words of a regular language, such that the relations of $\mathbb{A}$ are recognizable by synchronous multi-tape automata. A relational structure $\mathbb{A}$ is *homogeneous* if every isomorphism between two of its finite substructures can be extended to an automorphism. Every homogeneous structure is uniquely determined by the set of its finite substructures up to isomorphism. In many cases this set can be described through finitely many forbidden substructures. Hence both approaches yield a large class of infinite structures with a finite description.

In the context of description logics, we consider applicability of both automatic and finitely describable homogeneous structures as concrete domains. For description logics with GCIs, we want to investigate which further restrictions on both classes are sufficient for decidability of common reasoning problems such as concept satisfiability. This concerns in particular the sufficient conditions stemming from the works of Lutz and Miličić[1], and Carapelle, Kartzow and Lohrey[2].

[1] C. Lutz and M. Miličić, "A Tableau Algorithm for Description Logics with Concrete Domains and General TBoxes," *Journal of Automated Reasoning*, vol. 38, p. 227-259, 2007.

[2] C. Carapelle, A.-Y. Turhan, "Description Logics Reasoning w.r.t. General TBoxes Is Decidable for Concrete Domains with the EHD-Property," *European Conference on Artificial Intelligence*, vol. 285, p. 1440-1448, 2016.

Expressive Power of Combinatory Categorial Grammars

Lena Katharina Schiffer (schiffer@informatik.uni-leipzig.de)
Supervisor: Prof. Dr. Andreas Maletti, Prof. Dr.-Ing. Heiko Vogler

Combinatory Categorial Grammar (CCG)[1] is an efficiently parsable grammar formalism that is well-established in computational linguistics. The basis for CCG is provided by a lexicon and a rule system. Given an input word, each input symbol is assigned a syntactic category taken from the lexicon. The categories behave like functions in that they have a target category and expect a number of argument categories, but each of these arguments is given an additional directionality. Adjoining categories can be combined using application or composition combinators. If repeated use of the combinators results in a derivation tree that involves all input symbols and that is rooted in an initial category, the input is accepted.

CCG is an extension of classical categorial grammar, which only uses the application combinator. While classical categorial grammar can recognize exactly the context-free languages, CCG is a mildy context-sensitive grammar formalism. The their seminal work, Vijay-Shanker and Weir showed weak equivalence of CCG and Tree-Adjoining Grammar (TAG).[2] However, the construction of their classical result depends on the ability to restrict the combination rules and to include entries for the empty word in the lexicon. When rule restrictions are excluded, CCG is strictly less powerful than TAG.[3] On the other hand, CCG with generalized composition rules with no upper bound and entries for the empty word in the lexicon are Turing-complete.[4]

More work is needed to clarify the relation between different variants of CCG and also their relation to other formalisms. Possible variants of CCG differ in the use of rule restrictions, the bound of composition depth, lexicon entries for the empty word, as well as additional combinators, e.g. type raising. As these distinctions can influence the expressiveness of the grammar and the complexity of the parsing problem in ways not well understood, these questions are of great concern for potential applications. The goal of this research project is a characterization of the string languages (weak generative capacity) as well as the tree languages (strong generative capacity) recognized by different variants of CCG.

[1] M. Steedman and J. Baldridge, "Combinatory Categorial Grammar," in *Non-Transformational Syntax: Formal and Explicit Models of Grammar*, pp. 181–224, 2011.

[2] K. Vijay-Shanker and D. J. Weir, "The Equivalence of Four Extensions of Context-Free Grammars," in *Mathematical Systems Theory*, vol. 27, no. 6, pp. 511–546, 1994.

[3] M. Kuhlmann, A. Koller, and G. Satta, "Lexicalization and Generative Power in CCG," in *Computational Linguistics*, vol. 41, no. 2, pp. 215–247, 2015.

[4] M. Kuhlmann, G. Satta, Peter Jonsson, "On the Complexity of CCG Parsing," in *Computational Linguistics*, vol. 44, no. 3, pp. 447–482, 2018.

Non-standard Semantics for Knowledge Representation Formalisms – Computational Properties and Practical Reasoning

Lukas Schweizer (lukas.schweizer@tu-dresden.de)
Supervisor: Prof. Dr. Sebastian Rudolph, PD. Dr.-Ing. Anni-Yasmin Turhan

In many application scenarios certain knowledge representation formalisms are used and embedded in a rather unexpected and unintended manner – but nevertheless for plausible reasons. Accordingly, this presumable misusage comes along with a different understanding of the underlying semantics; or a different semantics is assumed while using the formalisms. For instance, description logics (DLs) are (mis-)used to specify typical constraint-type problems. In consequence, (non-standard) reasoning tasks are expected to be solved – most notably *model enumeration*, asking for one, several or all models of some given knowledge base; i.e. solutions to the encoded constraint problems. It would be rather unjustified to dispose such a scenario simply as wrong technological usage, instead it gives rise to interesting research questions. In this thesis the theoretical foundations for such application scenarios based on description logics shall be elaborated. To this end, semantics shall be proposed that particular suit the inherent intuition, and consequently corresponding computational properties such as expressivity and the resulting complexity of reasoning services need to be determined. Apart from theoretical considerations, the goal is to elaborate efficient reasoning methods as well as to provide an implementation and proof the practical capabilities via extensive evaluations. As yet, the *fixed-domain semantics* has been proposed and examined, whereas in contrast to the standard DL semantics, the domain of interest is a priori fixed and of known size (different from finite model reasoning where one is interested in models of arbitrary but finite cardinality). Beside theoretical results, an implementation of a reasoner applying the fixed-domain semantics has been developed – capable of performing standard DL reasoning tasks as well as model enumeration. For this purpose, a translation of DL knowledge bases to logic programs under the answer-set semantics has been proposed – an approach that suits perfectly to solve the required reasoning tasks. In general it is intended to retain and further improve this translation based approach. These findings have comprehensively been published in the proceedings of ECAI 2016.[1] The tool has been further developed and was presented at the 16th International Semantic Web Conference (ISWC) in October 2017. A deeper complexity analysis has been conducted an published.[2]

[1] Sebastian Rudolph, Lukas Schweizer, "Fixed-Domain Reasoning for Description Logics," ECAI 2016 – 22nd European Conference on Artificial Intelligence, vol. 285, p. 819–827, 2016.

[2] Sarah Alice Gaggl, Sebastian Rudolph, Lukas Schweizer, "Not Too Big, Not Too Small... Complexities of Fixed-Domain Reasoning in First-Order and Description Logics," Progress in Artificial Intelligence – 18th EPIA Conference on Artificial Intelligence, vol. 10423, p. 695–708, 2017.

Complexity of $\mathbf{MMSNP_2}$

Florian Starke (florian.starke@tu-dresden.de)
Supervisor: Prof. Dr. Manuel Bodirsky, Prof. Dr. Andreas Maletti

In my PhD project we study the class MMSNP_2. It is a fragment of second-order logic which has the same expressive power as frontier-guarded disjunctive Datalog (which was introduced by Meghyn Bienvenu, Balder ten Cate, Carsten Lutz, and Frank Wolter[1]). It is also a generalization of MMSNP, which was introduced by Feder and Vardi. They showed that every problem in MMSNP is, under randomized Turing-reductions, equivalent to a CSP with a finite template. They also conjectured that the class of all CSPs over finite templates has a dichotomy, i.e., all problems from this class are either NP-complete or polynomial-time tractable. This conjecture was proven independently by Bulatov and Zhuk in 2017. Later, Kun derandomized the reductions, which shows that also MMSNP has a dichotomy. Recently, Mottet found a new proof for the equivalence of MMSNP and CSPs with finite template. We try to generalize this proof to MMSNP_2 in order to show that also MMSNP_2 has a dichotomy.

Now lets introduce MMSNP and MMSNP_2. MMSNP contains all decision problems of the form: Given a finite structure. Is there a colouring of its elements such that certain coloured finite structures do not occur? The problems in MMSNP_2 have the same form except that we color relations instead of elements. A typical problem in MMSNP_2 is: Can we colour the edges of a given finite graph with two colors such that there is no monochromatic triangle?

[1] Meghyn Bienvenu, Balder ten Cate, Carsten Lutz and Frank Wolter. "Ontology-based data access: A study through disjunctive datalog, CSP, and MMSNP", ACM Transactions on Database Systems 39, 2013

Weighted Tree Substitution

Kevin Stier (stier@informatik.uni-leipzig.de)
Supervisor: Prof. Dr. Andreas Maletti, Prof. Dr.-Ing. Heiko Vogler

The flourishing branch of Natural Language Processing (NLP) is concerned with attaining manlike language processing, for tasks like simultaneous translation. Specifically the term parse tree or derivation tree, most commonly used in computational linguistics plays a big role. In a theoretical sense it is a rooted, ordered tree that is supposed to represent the derivation of a sentence given a grammar. By teaching a computer to use grammars and construct these kind of trees it is able to process language. In particular probabilistic Tree Substitution Grammars (TSG) have proven efficient in managing this challenge and are commonly used in NLP.

These TSGs are grammars consisting of smaller sub-trees that in some sense represent specific grammatical rules found in spoken language that then generate the desired derivation trees of a specific language. TSGs have not yet been approached from a theoretical point of view. In sense of the tree automata theory introduced in the 1960s, Tree Substitution Languages (TSL) form a subset of the well-known Regular Tree Languages (RTL) generated by Regular Tree Grammars (RTG). More classically RTLs are the ones generated by Nondeterministic Finite Tree Automata (NFTA), which have equivalent expressive power as RTGs. The goal is to find a characterization of the expressive power of these TSGs and extend the notion to a weighted setup.

In the course of last year multiple closure properties for TSGs have been investigated [1] giving a fundamental study of the expressive power of tree substitution grammars.

[1] Andreas Maletti and Kevin Stier, On Tree Substitution Grammars, DLT, 2020, *in press*

Valued Constraint Satisfaction Problems over Infinite Domains

Caterina Viola (caterina.viola@tu-dresden.de)
Supervisor: Prof. Dr. Manuel Bodirsky, PD. Dr. Karin Quaas

The object of my doctoral thesis is the computational complexity of certain combinatorial optimisation problems called *valued constraint satisfaction problems*, or *VCSPs* for short. The requirements and optimisation criteria of these problems are expressed by sums of *(valued) constraints* (also called *cost functions*). The input of a VCSP consists of a finite set of cost functions, depending on a given finite set of variables, and a cost u; the task is to find values for the variables such that the sum of the cost functions is at most u.

By restricting the set of possible cost functions in the input, a great variety of computational optimisation problems can be modelled as VCSPs. Recently, the computational complexity of all VCSPs for finite sets of cost functions over a finite domain has been classified. Many natural optimisation problems, however, can be formulated as VCSPs only if the domain is allowed to be infinite.

We started the systematic investigation of the complexity of infinite-domain VCSPs by focusing on piecewise linear (PL) and piecewise linear homogeneous (PLH) cost functions. The VCSP for a finite set of PLH cost functions can be solved in polynomial time if the cost functions are improved by fully symmetric fractional operations of all arities. We show this by (polynomial-time many-one) reducing the problem to a finite-domain VCSP [1] which can be solved using a linear programming relaxation [2]. We apply this result to show the polynomial-time tractability of VCSPs for *submodular* PLH cost functions, for *convex* PLH cost functions, and for *componentwise increasing* PLH cost functions; in fact, we show that submodular PLH functions and componentwise increasing PLH functions form maximally tractable classes of PLH cost functions.

We give a local characterisation of the *expressive power* of a set of cost functions over an arbitrary countable domain in terms of the set of fractional operations improving the cost functions in the set[3].

Finally, we provide a polynomial-time algorithm solving the restriction of the VCSP for *all* PL cost functions to a fixed number of variables[4].

[1] M. Bodirsky and M. Mamino and C. Viola, "Submodular Functions and Valued Constraint Satisfaction Problems over Infinite Domains," Proceedings of the 27th EACSL Annual Conference on Computer Science Logic (CSL), 12:1–12:22, 2018.

[2] M. Bodirsky and M. Mamino and C. Viola, "Piecewise Linear Valued CSPs Solvable by Linear Programming Relaxation," Submitted for journal publication. Preprint available at arxiv.org/abs/1912.09298, 2019.

[3] C. Viola, "Valued Constraint Satisfaction Problems over Infinite Domains," Doctoral Thesis (submitted), 2020.

[4] M. Bodirsky and M. Mamino and C. Viola, "Piecewise Linear Valued Constraint Satisfaction Problems with Fixed Number of Variables," Accepted for presentation at CTW2020 and publication in AIRO Springer Series. Preprint available at arxiv.org/abs/2003.00963, 2020.

Weight Accumulation and Probabilistic Model Checking

Sascha Wunderlich (sascha.wunderlich@tu-dresden.de)
Supervisor: Prof. Dr. Christel Baier, Prof. Dr. Markus Lohrey,
Prof. Dr. Sebastian Rudolph

Model checking is a well-established method for automatic system verification. Besides the extensively studied qualitative case, there is also an increasing interest in the quantitative analysis of system properties. Many important quantities can be formalised as the accumulated values of weight functions. These measures include resource usage such as energy consumption, or performance metrics such as the cost-utility-ratio or reliability guarantees. There are different kinds of accumulation like summation, averaging and ratios, all of which are necessary to cover different kinds of quantities.

The main goal of the thesis is to provide a general framework for the formalisation and verification of system models and property specifications with accumulative values. On the modelling side, we rely on weighted extensions of well-known modelling formalisms. Besides weighted Kripke structures, we investigate weighted probabilistic models such as Markov chains and Markov decision processes. The weights in this sense are functions, mapping each state or transition in the model to a value, e.g., a real vector. For the specification side, we provide a language in the form of an extension of temporal logic with new modalities that impose restrictions on the accumulated weight along path fragments. These fragments are regular and can be characterised by finite automata, so called monitors.

The framework supports both linear and branching time logic and allows variation to weaker formalisms, like non-negative or integral weight functions and bounded accumulation. We study the border of decidability of the model-checking problem for different combinations of these restrictions and give complexity results and algorithms for the decidable fragment.

A subset of the resulting algorithms is implemented as a plugin for the prominent probabilistic model-checking tool PRISM. We evaluate their scalability and performance and propose powerful optimizations for many common usage patterns. Furthermore, we investigate the influence and optimal usage of accumulated resource measures such as energy for heterogeneous tiled architectures and for adaptable energy consumers in a demand-response scenario.

GRK 1765: System Correctness under Adverse Conditions

Prof. Dr. Ernst-Rüdiger Olderog
Email: olderog@informatik.uni-oldenburg.de
Carl von Ossietzky Universität Oldenburg
Internet: www.scare.uni-oldenburg.de

The Research Training Group SCARE, established 2012, addresses computerised systems that are placed in an environment with which they cooperate, i.e., sense, control, and equip with unprecedented functionality. System correctness means that the cooperation between environment and system satisfies desired behavioural properties. This relationship depends on certain assumptions about the environment and the components of the system.

SCARE systematically investigates the problem of system correctness under adverse, only partially predictable conditions which can influence the behaviour of the system, the system context, and the assumptions made for verifying correctness. SCARE considers three aspects of adverse conditions, both individually and in their combination:

A. *Limited knowledge.*
B. *Unpredictable behaviour.*
C. *Changing structure of environment and system.*

These three aspects are studied under the following research themes:

1. *Formal modeling techniques.*
2. *Verification and analysis techniques.*
3. *Constructive techniques.*

The main aim of SCARE is research into notions of system correctness that guarantee robustness of the system behaviour under such adverse conditions.

In its second phase 2017–2021, SCARE continues to pursue this general research agenda, but will extend the scope of both verification and construction techniques by two aspects crucial to recent cyber-physical applications: the handling of complex and possibly irregular search spaces for solutions and the possible loss of functional correctness due to security attacks. To this end, we additionally pursue the following:

- *Embedded Artificial Intelligence, in particular machine learning.*
- *Security analysis within applications.*

Recently completed PhD theses focus on the safety of traffic manoeuvres and applications of machine learning.

Learning an Abstraction of NBTI Aging Models

Stephan Adolf (stephan.adolf@uni-oldenburg.de)
Supervisor: Prof. Dr.-Ing. Wolfgang Nebel

Microelectronic components for ICT-systems experience increasing aging stress due to Negative Bias Temperature Instability (NBTI)[1]. NBTI leads to a threshold voltage degradation which results in larger signal delays after some years of usage. Thus timing constraints, defined by the system specification, may be violated in field, leading to malfunction of ICT-components. NBTI is caused by imperfections in the gate oxide of PMOS-transistors. The state-of-the-art explanation of NBTI is given by the four-state-trap model[2], which describes aging as charge trapping under negative bias stress. With NBTI being recoverable and heavily depending on the stress history, it is very difficult to take aging into account during design time. Currently, NBTI simulation-techniques to obtain the threshold voltage damage try to either cope with variable stress conditions over time[3] or provide a fast and overestimating worst case simulation[4].

The aim of this work is to provide an abstract description of the occupation state of trap-ensembles of a single PMOS-transistor in the first step. The idea is to obtain the collective trap-states of a single transistor under varying stress conditions without the need to simulate all traps over time. The abstraction relies on the ideas CET-Maps[5] and the Phase Space model[6]. At the end of the simulation the occupation state for all traps shall be estimated. Thus, the threshold voltage degradation can be obtained.

The objective of the second step is to provide a machine-learning model for a single PMOS-transistor relying on the abstract model obtained in the previous step.

Finally, a machine-learning model for a single gate shall be developed directly providing the delay under aging.

---

[1] T. Grasser et al., "A Two-Stage Model for Negative Bias Temperature Instability", *Proceedings of IEEE Int. Rel. Phy.*, p. 33-44, 2009.

[2] T. Grasser et al., "The Paradigm Shift in Understanding the Bias Temperature Instability: From Reaction - Diffusion to Switching Oxide Traps", *IEEE Trans. Electron Devices*, 58(11), p. 3652-3666, 2011.

[3] M. C. Metzdorf, "Integration einer Zuverlässigkeitsbewertung und -optimierung in den RT- und Gate-Level Entwurfsfluss", *PhD Thesis, University of Oldenburg*, http://oops.uni-oldenburg.de/3642/, 2018.

[4] Y. Cao et al., "Cross-Layer Modeling and Simulation of Circuit Reliability", *IEEE T. Comput. Aid. D.*, 33(1), p. 8-23, 2014.

[5] T. Reisinger et al., "The statistical analysis of individual defects constituting NBTI and its implications for modeling DC- and AC-stress", *Proceedings of IEEE Int. Rel. Phy.*, p. 7-15, 2010.

[6] R. J. Eilers, "Abstraction of aging models for high level degradation prediction", *PhD Thesis, University of Oldenburg*, http://oops.uni-oldenburg.de/3212/, 2017.

Delayed Hybrid Systems

Erzana Berani Abdelwahab (erzana.berani.abdelwahab@uni-oldenburg.de)
Supervisor: Prof. Dr. Martin Fränzle

Delays in feedback dynamics of coupled dynamical systems arise regularly, especially in embedded control due to communication latencies imposed by digital networks between the plant and the controller. Systems featuring delays are however notoriously difficult to analyse. Consequently, formal analysis often addresses simplified, delay-free substitute models, risking negligence of the adverse impact of delay on control performance. In continuous control it is already well-known that such delays may cause oscillations and thus directly affect the control performance which in turn invalidates both safety and stability guarantees obtained from the delay-free models. This insight has encouraged researchers and engineers to exploit the model of delay differential equations (DDEs), which has already been introduced in the sixties [1], initially for modeling delays arising in natural phenomena like population growth and other biological systems. Beside the developments that have been acquired during the following decades, we have also seen interesting results in the last decade on first automatic verification methods for dynamical properties of DDEs [2] [3]. Surprisingly, despite a large portion of digital control schemes being an integration of discrete and continuous state dynamics, i.e., hybrid state dynamics, there are no similar developments for controlling and verifying hybrid systems subject to delays. To the best of our knowledge, neither an established notion of delayed hybrid system nor corresponding verification methods exist.

Introducing a formal semantic, i.e., mathematical model for rigorously modeling delays arising in hybrid systems thus constitutes the main objective of this PhD project. Aiming at a model of hybrid automata subject to feedback delay, DDEs shall be used for modeling the continuous dynamics while discrete switches shall be replaced with their delayed counterparts as well. First findings indicate that a major part of the delay-induced complexity can be reduced effectively when adding natural constraints to the model of the delayed feedback channel, namely that it transports a band-limited signal and implements a non-punctual, distributed delay. The expectation is that the impact of band limitation and non-punctual delay will be positive, and thus permit the development of automatic verification techniques for the established hybrid automata model featuring feedback delays.

[1] Richard E. Bellman and Kenneth L. Cooke, " Differential-difference equations," Technical Report, 1963.

[2] Zhenqi Huang, Chuchu Fan, and Sayan Mitra, "Bounded invariant verification for time-delayed nonlinear networked dynamical systems," Nonlinear Analysis: Hybrid Systems, vol. 23, p. 211-229, 2017.

[3] Bai Xue, Peter N. Mosaad, Martin Fränzle, Mingshuai Chen, Yangjia Li, and Naijun Zhan, "Safe over- and under-approximation of reachable sets for delay differential equations," FORMATS 2017, vol. 10419, p. 281-299, 2017.

Spatial Observation-Based Decision-Making in Autonomous Traffic

Christopher Bischopink (bischopink@informatik.uni-oldenburg.de)
Supervisor: Prof. Dr. Ernst-Rüdiger Olderog

While (partially) autonomous vehicles begin to enter the market, it is desirable that they behave correct with respect to a specification. A basis for this purpose is the *Multi-Lane Spatial Logic (MLSL)* which, together with its abstract model of traffic, can be used to reason about (highway) traffic. [1] Since then, both model an logic were extended to other traffic scenarios, such as urban traffic [2]. Additionally, there is an automata model that can control the cars in the abstract model (*Automotive-Controlling Timed Automata, ACTA*), which are extended timed automata. It is desired to reuse the abstract model and the logic, as well as the automata model in our own approach.

In MLSL in its pure form, it is not possible to express temporal properties about a system, which is a key feature for complex and realistic requirements. Therefore, an extension towards a timed version of MLSL is our first goal. Based on the specifications formulated in the timed extension, the approach is to synthesize controllers and monitors, so that the system under control satisfies its specifications. The mechanism to achieve this is as follows: First, the monitors that represent the knowledge about the current satisfaction of a specification need to be synthesized. Second, a car that wants to execute an action asks the (online) monitors whether this action will violate some other cars' specifications in the near future. If so, the action is forbidden, otherwise it is allowed. A further step could be to let the cars give more detailed answers, for example that changing lanes now is forbidden, but in x time units a lane change would not cause a violation of a specification.

At this point, communication with other cars is needed, which fits well, as broadcast communication is one key feature of ACTA. It also might be of interest to consider lossy channels for the communication.

Obviously, it is possible to give specifications that are not satisfiable at all, or specifications that only hold on some classes of models. We will investigate in this topic to examine whether the specifications are satisfiable or not. Additionally, a probabilistic satisfaction of the specifications might be considered if the they do not hold in general on certain models.

In the end, it is planned to evaluate all results in a simulation environment such as SUMO [3], with monitors and controllers generated by some (to be implemented) tool.

[1] Hilscher, M., Linker, S., Olderog, E.R., Ravn, A, "An abstract model for proving safety of multi-lane traffic manoeuvres.," Int'l Conf. on Formal Engineering Methods (ICFEM), vol. 6991, p. 404–419, 2011

[2] Schwammberger, M., "An abstract model for proving safety of autonomous urban traffic," Theor. Comput. Sci., vol. 744, p. 143–169, 2018

[3] Lopez, P.A. et al., "Microscopic Traffic Simulation using SUMO," IEEE Intelligent Transportation Systems Conference (ITSC), vol. 21, p. 2575-2582, 2018

Scenario-Based Application-optimized Data Replication Strategies

Syed Mohtashim Abbas Bokhari
(syed.mohtashim.abbas.bokhari@uni-oldenburg.de)
Supervisor: Prof. Dr. Oliver Theel

A distributed system is a paradigm which is indispensable to the current world due to countless requests with every passing second. Therefore, in distributed computing, high availability is very important. In a dynamic environment due to the scalability and complexity of the resources and components, systems are fault-prone because millions of computing devices are connected to each other via communication links. Distributed systems allow many users to access shared computing resources which makes faults inevitable. Replication plays its role in masking failures in order to achieve a fault-tolerant distributed environment. Data replication is an appropriate means to provide highly available data access operations at relatively low operation costs. Although there are several contemporary data replication strategies being used, the question still stands which strategy is the best for a given scenario or application class assuming a certain workload, its distribution across a network, availability of the individual replicas, and cost of the access operations. In this regard, research focuses on analysis, simulation, and machine learning approaches to automatically identify and design such replication strategies that are optimized for a given application scenario based on predefined constraints and properties exploiting a so-called voting structure.

Improving Cartesian Genetic Programming for Atari Games

Tim Cofala (tim.cofala@uni-oldenburg.de)
Supervisor: Prof. Dr. Oliver Kramer

Cartesian Genetic Programming (CGP) is a technique for the generation of computer programs using mechanisms inspired by natural evolution. In contrast to other state-of-the-art machine-learning techniques CGP offers the advantage of representing its problem solutions as human-readable program code. The feature of creating novel and interpretable solutions has lead to applications of CGP in various problem domains, like digital circuit evolution or image processing [1]. Recently, CGP was introduced to the generation agents for Atari games [2]. Atari games offer a challenging environment for AI agents and are a common benchmark in the domain of reinforcement learning. CGP has shown to be capable of generating strategies for many different Atari games. Often these strategies outperform the results of professional human play testers and sometimes even other state-of-the-art reinforcement learning strategies.

The success of CGP in the domain of Atari games demonstrate its potential for reinforcement learning applications. Building up on this, the aim of my research is further investigate and improve CGP for reinforcement learning, with focus on two major aspects. Firstly, the extension of CGP with more advanced evolutionary mechanisms. New genetic operations and evaluation strategies for CGP could improve its performance for reinforcement learning tasks and address the problem of premature stagnation. First experiments have indicated that tournament selection and a more sophisticated evaluation result a generation of better agents [3]. Secondly, complex visual environments like Atari games could require the addition of more advanced visual processing strategies. A separate evolution of the visual/perceptual component and the decision-making policy could enable more complex strategies. A combination with neuronal networks, to utilize their visual processing capabilities, could also yield great benefits. These issues will be addressed in future research.

[1] Miller, J.F.: "An Empirical Study of the Efficiency of Learning Boolean Functions using a Cartesian Genetic Programming Approach." In: Proc. Genetic and Evolutionary Computation Conference, pp. 1135–1142. Morgan Kaufmann (1999)

[2] Dennis G. Wilson, Sylvain Cussat-Blanc, Hervé Luga, Julian F. Miller: "Evolving simple programs for playing Atari games." CoRR abs/1806.05695 (2018)

[3] Tim Cofala, Lars Elend, Oliver Kramer: "Tournament Selection Improves Cartesian Genetic Programming for Atari Games" Submitted to ESANN 2020

Reconciling Formal Methods with Metrology

Paul Kröger (paul.kroeger@informatik.uni-oldenburg.de)
Supervisor: Prof. Dr. Martin Fränzle

A typical mathematical model for safety-critical embedded systems featuring complex behaviour based on possibly inaccurate observations of the environment is the hybrid automaton[1] comprising a finite set of discrete control modes each incorporating differential equations governing a continuous state while predicates on the continuous state control dynamics of the discrete state space. Various flavours of hybrid automata have been suggested, among them probabilistic hybrid automata[2] variants enabling quantitative verification.

Contrary to intuition, the quest for precise formal verification verdicts cannot be satisfied by those automata variants. Deterministic variants suffer from ignoring errors, thus being overly optimistic, while the demonic interpretation of nondeterministic models yields an overly pessimistic perspective. Even stochastic models yield imprecise verdicts due to improperly representing measurement techniques established in practice.

We identify the state spaces underlying traditional hybrid automata models as the source of this deficiency, as they are spanned by a finite-dimensional vector space over $\mathbb{R}$ times a finite set of control modes. Such a state space is finite-dimensional and thus cannot incorporate functions over the $\mathbb{R}^n$ as state components, which would be necessary for representing distributions, as pertinent in metrology for state estimation from uncertain measurements. Thus, the aforementioned models ignore wisdom from metrology and game theory concerning environmental state estimation to be pursued by a rational player, which a control system obviously ought to constitute.

Aiming at enhancing the precision of verdicts of formal verification, we develop a revised formal model, called *Bayesian hybrid automaton*[3] (BHA), that is able to represent state tracking and estimation in hybrid systems based on an extended state space comprising distribution functions representing state estimations of variables observed under uncertainty. The application of probabilistic filter techniques as known, e.g., from metrology in order to improve those estimations combined with discrete dynamics based on the likelihood that predicates over the continuous state hold allows to model "rational" systems making evidence-based decisions even in presence of uncertain mutual observations of entities being part of the system and its ambience.

[1] R. Alur et al., "Hybrid Automata: An Algorithmic Approach to the Specification and Verification of Hybrid Systems", *Hybrid Systems*, LNCS vol. 736, pp. 209–229, Springer, 1992.

[2] J. Sproston, "Decidable Model Checking of Probabilistic Hybrid Automata", *Formal Techniques in Real-Time and Fault-Tolerant Systems (FTRTFT)*, LNCS vol. 1926, pp. 31–45, Springer, 2000.

[3] M. Fränzle and P. Kröger, "The Demon, the Gambler, and the Engineer: Reconciling Hybrid-System Theory with Metrology", *Proc. Symposium on Real-Time and Hybrid Systems*, pp. 165-185, Springer, 2018.

Using Fourier Transformation to improve training of modern convolutional neural networks

Philip Mirbach (philip.mirbach@uni-oldenburg.de)
Supervisor: Prof. Dr. Oliver Kramer

Convolutional Neural Networks (CNNs) have established themselves as a successful architecture in the field of machine learning, among other things for typical image recognition tasks such as classification. However, as the complexity of the tasks increases, the computational effort required to train these networks increases considerably, since both the size of the dataset and the capacity of the network must be sufficiently large.

By using the discrete Fourier transform, the training effort of networks with convolutional layers can be significantly reduced[1]. According to the convolutional theorem, the convolution of two functions can be described as the product of their Fourier transformations. This element-wise multiplication is much less computationally intensive than the original convolution operation. In addition, the Fourier basis offers the possibility to use frequency-dependent methods for dimension reduction (pooling)[2]. Depending on the nature of the data, this procedure can lead to a significantly lower loss of information, for example, the largest amount of information from natural images is concentrated in the low-frequency rates.

Since these investigations, however, the common CNN architectures have evolved. The Inception networks, which analyze data by parallel arranged varied procedures (Multi-Branch)[3] and the Residual networks (ResNet)[4], which can construct particularly deep CNNs, are to be emphasized here.

We want to investigate whether Fourier transformations can also be used in these modern CNN architectures to reduce training effort. For this purpose, a pure residual structure of convolutional layers could be replaced by their Fourier representation. It may also be possible to improve the accuracy of a network by supporting convolution in multi-branches by parallel analyses in Fourier space.

[1] M. Mathieu, M. Henaff, Y. LeCun, "Fast Training of Convolutional Networks through FFTs." *ICLR*, 2014

[2] O. Rippel, J. Snoek, R. P. Adams, "Spectral Representations for Convolutional Neural Networks" *NIPS*, p. 2449–2457, 2015

[3] C. Szegedy et al., "Going Deeper with Convolutions", *IEEE Conference on Computer Vision and Pattern Recognition*, p. 1–9, 2014

[4] K. He, X. Zhang, S. Ren, J. Sun, "Deep Residual Learning for Image Recognition", *IEEE Conference on Computer Vision and Pattern Recognition*, p. 770–778, 2016

Functional Verification of Cyber-Physical Systems Containing Machine-Learning Component

Farzaneh Moradkhani (farzaneh.moradkhani@uni-oldenburg.de)
Supervisor: Prof. Dr. Martin Fränzle

Functional architectures of cyber-physical systems, like autonomous cars, increasingly comprise components that are generated by training and machine learning rather than by more traditional engineering approaches. The validation and functional verification of such systems, as necessary in safety-critical application domains, poses various unsolved challenges. Commonly used computational structures underlying machine-learning, like deep neural networks, lack scalable automatic verification support. Their usually large size, the central role of non-linear functions to the operation of neural networks, and the consequential non-convex, highly disconnected solution spaces render DNN verification difficult. In addition, DNNs Verification is a challenge to state-of-art *linear programming* (LP) solvers and *satisfiability modulo theories* (SMT) solvers leading to scalability issues[1][2][3].

The main focus of my research is to investigate the non-linear side of DNNs with emphasis on all kinds of useful activation functions in DNNs, especially such that are not just piecewise linear with the help of the SMT Solver iSAT [4] with its core based on a tight integration of recent DPLL-style SAT solving techniques with interval constraint propagators and aims at solving Boolean combinations of linear and non-linear constraint formulas over the reals involving polynomial and transcendental functions like sine, cosine, exp).

Our proposed method advances beyond the state-of-the-art in two respects: It will be able to handle activation functions beyond the piece-wise linear type as incorporated in ReLU networks. As more general activation functions defined in terms of transcendental arithmetic functions increase the reasoning power and thus potentially decrease the size of neural networks by their ability to fit non-linear functions more concisely, we expect a gain in the complexity of trained network functions we are able to verify mechanically. In addition, smooth non-linear transfer functions like the sigmoid paired with interval-based constraint propagators tailored to them reduce the need of case splitting and case-based reasoning induced by piecewise defined transfer functions, thus potentially inducing a gain in scalability of the verification procedure.

[1] Katz, G., Barrett, C., Dilland, D., Julian, D., and Kochenderfer.M. "Reluplex: An Ecient SMT Solver for Verifying Deep Neural Networks"Springer International Publishing-, 97–117, (2017).

[2] Bastani, Z., O., Loannou, Y., Lampropoulos, L., Vytiniotis. D., Nori, A., Criminisi, A"Measuring neural net robustness with constraints" Proceedings of the 30th Conference on Neural Information Processing Systems,NIPS, (2016).

[3] Huang, X., Kwiatkowska, M., Wang, S., and Wu, M. " Saftey verication of deep neural networks: Technical report",http://www.arxiv.org/abs/1610.06940, (2016).

[4] Fränzle, M., Herde,C., Teige, T., Ratschan,S and Schubert.T,"Ecient Solving of Large Non-Linear Arithmetic Constraint Systems with Complex Boolean Structure" Journal on Satisability, Boolean Modeling and Computation, (2007).

A hybrid RISC-V architecture supporting mixed timing-critical and high performance workloads

Mehrdad Poorhosseini (mehrdad.poorhosseini@uni-oldenburg.de)
Supervisor: Prof. Dr.-Ing. Wolfgang Nebel

A single processor in a mixed-criticality system must run tasks with different levels of criticality, some of them might be safety critical, others non-safety critical[1]. In such a system, critical tasks are often temporally and spatially isolated from each other and all non-critical tasks.

RISC-V[2] is a new instruction set architecture (ISA) that was originally designed to support computer architecture research and education. Currently the RISC-V ISA is on its way of becoming a standard free and open architecture for industry implementations. RISC-V based processor cores are either optimized for timing predictability (like the RISCY microprocessor) or the processor core is optimized for high-performance computing (like the Ariane)[3]. In the scope of this work, the aim is to investigate how we can get the best from both worlds, which are "timing predictable" and "high performance". For this reason, this work proposes and analyzes a single processor architecture, which is based on a high-performance processor core that can be switched at run-time from the high-performance to a timing predictable mode and back. The reason for designing this kind of system is to have the advantages of the predictable and high-performance in one microarchitecture.

So far, we investigated and implemented different platforms in RISC-V ecosystem in order to analyze their capability for providing a timing predictable computation. In addition, we proposed a benchmark environment for the comparison of compilers in the RISC-V ecosystem and performed a comparison of GCC against LLVM for an embedded software benchmark considering compile time, size of the resulting binary, number of instructions and execution time. In the future, we will have a fundamental software structure including two platforms; a real-time (RT) and high performance (HP) and the idea is to merge them. The software structure allows us to trigger switching between modes from a software model[4]. Finally, we will assess the area overhead of our platform compared to a high performance. Furthermore, we will assess the timing overhead for switching between execution modes (RT, HP) and compare this platform with a heterogeneous RT and HP platform, where the two cores are separated from each other.

[1] Burns, Alan, and Robert Davis. "Mixed criticality systems-a review." Department of Computer Science, University of York, Tech. Rep (2013): 1-69.

[2] Asanović, Krste, and David A. Patterson. "Instruction sets should be free: The case for risc-v." EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2014-146 (2014).

[3] https://github.com/pulp-platform

[4] Ittershagen, Philipp, Kim Grüttner, and Wolfgang Nebel. "An integration flow for mixed-critical embedded systems on a flexible time-triggered platform." ACM Transactions on Design Automation of Electronic Systems (TODAES) 23.4 (2018): 51.

Distributed Synthesis in Symmetric Scenarios

Nick Würdemann (wuerdemann@informatik.uni-oldenburg.de)
Supervisor: Prof. Dr. Ernst-Rüdiger Olderog

Synthesis of distributed systems, also called *distributed synthesis*, describes the attempt to automatically generate local controllers for multiple processes that are *not perfectly informed* of each other's moves at all times, but have a *global goal*. *Petri games*[1] are a model for the distributed synthesis problem providing true concurrency of the processes. They are multi-player games representing causal memory of the involved players. Using *high-level* Petri games, we can describe huge ordinary Petri games that have much symmetric behaviour in a very concise way.

Ordinary Petri games are solved by reducing them to a two-player game on a finite graph that simulates runs of the Petri game, using game situations as nodes. A winning strategy for the Petri game (and therefore controllers for the individual processes) is then extracted from a winning strategy in the two-player game.

In my thesis I exploit the high-level representation of a Petri game, and therefore its *symmetries*, to solve these games in a *more efficient* way; using the symmetries provided by the structure of the high-level Petri game, I reduced the corresponding two-player game in size, which again should lead to faster solving. A winning strategy in the Petri game can then be extracted from a winning strategy in the reduced (called *symbolic*) two-player game.

Since the strategies are only defined for ordinary Petri games, I plan to *define high-level strategies* for Petri games with a high-level representation, and to automatically generate the former directly from the symbolic two player game. These high-level strategies could then be tested for scalability, which will be a step towards *parameterized* distributed synthesis.

[1] Finkbeiner, B. and Olderog, E.R.: Petri games: Synthesis of distributed systems with causal memory. In: Peron, A., Piazza, C. (eds.) Proc. Fifth Intern. Symp. on Games, Automata, Logics and Formal Verification (GandALF). EPTCS, vol. 161, pp. 217–230 (2014).

Host-based Misbehavior Detection System in VANETs

Jithin Zacharias (jithin.zacharias@uni-oldenburg.de)
Supervisor: Prof. Dr. Advisor Name

Cooperative Intelligent transportation systems are used to enhance driving safety and efficiency. Vehicles can communicate with other vehicles and infrastructure through wireless communication. This is possible through the vehicular ad-hoc networks (VANETs). Since there can be insider attackers (who possess valid cryptographic keys) to disrupt the network, main challenge is to protect integrity of the data and guarantee its correctness. One solution to this problem is employing on-board sensors like LIDAR, RADAR, Camera e.t.c which can enhance the perception around the vehicle. This can then be used to verify the data correctness by a plausibility analysis through multi-sensor data fusion[1]. But one limitation of this method is the field of view (FOV) provided by the sensors. This limits the plausibilty check and uncertainty arises outside the FOV.

The goal of the thesis is focusing on this direction, how certain attacks can be identified and detected in the FOV surroundings, in particular specifying the Region of Uncertainty (RoU). i.e, in the neighborhood spanning outside FOV of camera and before the FOV of communication sensor. The research challenge is to identify quantity which can relate both the FOV. Traditionally, the density of vehicles has been employed as a key parameter for evaluating the traffic state. This motivates to investigate the traffic density calculated on the host vehicle, defined as Local Traffic Density (LTD) as the security parameter. Thus, the calculation of LTD is used for identifying the misbehavior.

The author introduced the possibility of an illusion attack[2] in the defined RoU, where the location of ghost vehicle is moving with respect to the host vehicle[3]. An approach is introduced that is measuring LTD from two independent sensors and representing it as evidence for certain traffic situation. Firstly, a statistical approach is considered where the correlation between the LTD from communication and camera sensors is established. A detection mechanism based on the approach is outlined. Secondly, as another approach: Dempster rule of combination is used for fusing together multiple pieces of evidence from camera and communication sensors to detect the misbehavior. These approaches can calculate whether the neighborhood communication is under attack or not. For performance comparison, different evaluation[4]

[1] Obst, Marcus, Laurens Hobert, and Pierre Reisdorf *Multi-sensor data fusion for checking plausibility of V2V communications by vision-based multiple-object tracking.*Vehicular Networking Conference (VNC), 2014 IEEE.

[2] Lo, Nai-Wei, and Hsiao-Chien Tsai. *Illusion attack on vanet applications-a message plausibility problem*

[3] Zacharias, Jithin and Sibylle Fröschle *Misbehavior Detection System in VANETs using Local Traffic Density* Vehicular Networking Conference (VNC), 2018 IEEE.

[4] Van der Heijden, Rens W., and Frank Kargl. *Evaluating Misbehavior Detection for Vehicular Networks.* 5th GI/ITG KuVS Fachgespräch Inter-Vehicle Communication (2017): 5.

strategies are compared considering attacker and honest participant ratios being assigned in the communication.

GRK 1907: Role-based Software Infrastructures for continuous-context-sensitive Systems

Prof. Dr.-Ing. Wolfgang Lehner
Email: wolfgang.lehner[at]tu-dresden.de
Technische Universität Dresden
Internet: https://rosi-project.org

Software with long life cycles is facing continuously changing contexts. New functionality has to be added, new platforms have to be addressed, and existing business rules have to be adjusted. In the available literature, the concept of role modeling has been introduced in different fields and at different times in order to model context-related information, including - above all - the dynamic change of contexts. However, often roles have only been used in an isolated way for context modeling in programming languages, in database modeling, or to specify access control mechanisms. Never have they been used consistently over all levels of abstraction in the software development process, i.e. over the modeling of concepts, languages, applications, and software systems.

The central research goal in this program is to deliver proof of the capability of consistent role modeling and its practical applicability. Consistency means that roles are used systematically for context modeling on all levels of the modeling process. This includes the concept modeling (in meta-languages), the language modeling, and the modeling on the application and software system level. The subsequent scientific elaboration of the role concept, in order to be able to model the change of context on different levels of abstraction, represents another research task in this program. Thus, consistency also means to systematically define relationships between the identified role concepts to allow for model transformations and synchronizations. Such consistency offers significant advantages in the field of software systems engineering because context changes are interrelated on different levels of abstraction; plus, they can be synchronously developed and maintained. Potential application fields are the future smart grid, natural energy based computing, cyber-physical systems in home, traffic, and factories, enterprise resource planning software, or context-sensitive search engines.

Currently, the research training group is being financed by DFG in its second phase (01.04.2018 until 30.09.2022). During the first phase of the research training group (01.10.2013 – 31.03.2018) 10 RoSI PhDs completed their doctorate.

By the end of the second funding phase, additionally, 22 RoSI financed PhDs plus a number of non-DFG-financed PhDs are expected to have completed their doctorate.

The research training group is run by ten Principle Investigators from TU Dresden plus a number of associate members. Regular thesis advisory board meetings, off-site workshops, lecture series, seminars, invited talks, long-term stays abroad, and a soft skill program are essential elements of the program.

Role-oriented Particle Methods

Johannes Bamme (johannes.bamme@tu-dresden.de)
Supervisor: Prof. Dr. sc. techn. Ivo F. Sbalzarini, Prof. Dr.-Ing. Wolfgang Lehner

The objective of Systems Biology is to go from the studies of small subunits to a more systems-level understanding. Since it is very hard to study these systems only in experiments, simulations are a key technology in this area. But simulations in the context of Systems Biology require a broad range of expertise, reaching from biology over physics via mathematics to computer science.
Separation of expertise is a solution to circumvent the requirement of a broad range of expertise. Loosely speaking, everybody do what they do best.
Hence, a comprehensive simulation framework with the scope of separation of expertise should incorporate the following five criteria. First, total separation-of-concerns. Each numerical algorithm is independently implemented in building blocks. Second, easy usability. It needs to be as easy as possible to do both, creating an algorithmic building block and stack them together for a simulation. Third, universality. All four categories of models (the four combinations of deterministic or stochastic and discrete or continuous) need to be simulatable. Fourth, ability of steering. During run time it is possible to change the simulation, e.g. the numerical methods or the geometry. Fifth, high performance.
Thus far, most approaches focused on the modular development. Such approaches are MCell, VCell, CoMSES Net, as well as general FEM (Finite Element Method) libraries. But this modularity provides reuse just for models not for algorithms. Also common aims are performance and easy usability. Easy usability is often tackled by DSLs (Domain Specific Languages), not providing easy ways of manipulating or adding algorithms, like in MCell, ChemCell and Smoldyn. Universality is important when it comes to heterogeneous models where continuous and discrete modeling approaches are used. Steering gets more and more popular with the occurring of immersive technologies e.g. VR-Headset and haptic feedback gloves.
Hence, the overall question is: What kind of framework can incorporate all five criteria?
My approach uses two concepts, Particle Methods and roles. Particle Methods is known to be a unifying numerical framework, which provides universality. When it comes to PDEs (Partial Differential Equations) it has the potential of a very fine grained separation-of-concerns. Additionally it can be implemented performant e.g. OpenFPM (Open Framework for Particle and Mesh). But so far there is no formal definition which covers the universality of Particle Methods. Role-orientation can be seen as extension of object orientation. Roles provide the ability of changing the properties and the methods of an object during run time which makes steering directly achievable. Roles can be cluster into so called compartments. Hence, compartments provide a modeling

tool to develop algorithmic building blocks. This supports the aim of a total separation-of-concerns.
Hence, the two remaining questions are: What is a Particle Method formally? What does the CROM (Compartment Role Object Model) for Particle Methods look like which incorporates all five criteria?

Formal Quantitative Analysis of Role-based Systems

Philipp Chrszon (Philipp.Chrszon@tu-dresden.de)
Supervisor: Prof. Dr. rer. nat. Christel Baier

Role-based modeling is a promising approach to cope with the context-dependency and the (self-)adaptivity of modern software systems. However, dynamic role changes at runtime may introduce unforeseen and unwanted side effects, like deadlocks or objects acquiring conflicting roles. As today's society becomes more and more dependent on software systems, reliability, dependability and overall quality are major concerns. Thus, formal methods for modeling, verification and analysis are highly desirable.

Probabilistic Model Checking (PMC) is a formal technique for functional and quantitative analysis. It allows to reason about the probabilities of certain properties, e.g., the probability that an object always plays the same role or the probability that a specific role change leads to a system failure. Furthermore, the quantitative analysis with respect to different utility and cost functions, such as energy consumption, throughput, latency and performance, is also possible. Being able to model stochastic phenomena and environments is especially important for analyzing context-dependent systems. Well known model-checking approaches require a formalization of the system under consideration and the desired requirements. However, to the best of my knowledge, there are currently no formalisms and modeling languages suitable for PMC that incorporate both the context-dependent and collaborative characteristics of role-based systems.

The goal of this thesis is to develop operational models for role-based software infra-structures that allow for quantitative analysis by means of PMC. These models should capture stochastic information about dynamic role changes, their costs and their effects on the system. A major challenge is to find composition operators for the role-based operational models that adequately formalize interactions of role-playing objects. Further steps include the development of suitable modeling languages and model-checking algorithms, as well as the investigation of practical applicability of the developed formalisms and algorithms.

Balanced Database Query Processing Based on Compressed Intermediates

Patrick Damme (patrick.damme@tu-dresden.de)
Supervisor: Prof. Dr.-Ing. Wolfgang Lehner

In-memory column-store databases make extensive use of lightweight data compression to address the increasingly severe bottleneck between main memory and fast multi-core processors. The reduced size of compressed data results in a better utilization of the memory bandwidth and the cache hierarchy. Furthermore, many database operators can process compressed data directly without decompression. Consequently, employing lightweight compression can significantly improve query performance.

In order to leverage lightweight compression optimally, the context of the data to be compressed should be taken into account carefully. First of all, data might be either base data or intermediate results generated during query processing. Interestingly, in in-memory column-stores, accessing intermediates is as expensive as accessing base data, since both reside in main memory. Thus, compression is promising not only for base data, but also for intermediates. However, existing systems do not fully exploit the potential of compressed intermediate results.

Therefore, our vision is a *balanced database query processing based on compressed intermediates* in in-memory column stores. That is, in a query execution plan of compression-aware physical operators, every intermediate result shall be represented using a lightweight compression algorithm suitable in the context of the surrounding operators and data characteristics such that the benefits of compression outweigh its costs. To achieve this goal, we address the following three aspects of the problem:

In the *structural aspect*, we focus on efficient implementations of lightweight compression algorithms and investigate their behavior in the context of different data characteristics and hardware capabilities such as SIMD (Single Instruction Multiple Data) extensions. Furthermore, we explore how data can be adapted to changing contexts by transforming it to another compression format efficiently.

In the *operational aspect*, we extend the considered notion of context to the operators in a query execution plan. Besides the development of physical operators for compressed data, we analyze which compression algorithms are suitable for which operators.

Finally, in the *optimization aspect*, we develop compression-aware strategies for the database query optimizer. These strategies select a suitable compression algorithm for each intermediate in the context of a given query plan. By defining a trade-off between the optimization targets runtime requirement and memory consumption, these strategies are able to adapt to the context of the query execution such as the system's current resource utilization and the user's preferences.

Adaptive Heterogeneous Computation for database systems

Johannes Fett (Johannes.fett@tu-dresden.de)
Supervisor: Prof. Dr-Ing. Wolfgang Lehner

Accelerating Database Operators by Co-processing index- and accelerator structures on SX-Aurora vector engine. A vector intrinsic based Bloom Filter is used on a vector engine to accelerate hashjoin performance compared to CPU and GPU+CPU processing. Bloom filter algorithm is tailored to hardware specifications of SX-Aurora. 8 Processes are used for computation, which request data from a partitioned shared memory buffer.

To maximize hardware utilization Both CPU and VE are processing data in parallel streams. Evaluation is planned as an end to end of Hash-Join execution time against a GPU system.

Context Management in Database Systems with Word Embeddings

Michael Günther (Michael.Guenther@tu-dresden.de)
Supervisor: Prof. Dr-Ing. Wolfgang Lehner

In complex adaptive systems data integration plays an important role. Large organizations usually store data in a lot of different databases with different large schemes. Storing the data in one common scheme is due to the segmentation of such organizations in many loosely connected departments often not possible. However, there are situations in which data from different schemes has to be integrated to solve certain tasks. Since the schemes can change independently it is highly desirable to be able to automatically integrate data from different sources. However, such data integration tasks typically require a lot of manual effort. Since the volume of data which has to be managed growth and software systems evolving more frequently, the demand for more automated data integration solutions increases. Furthermore, data integration has to be supported by tools for data discovery and data exploration which allow the user to observe the coherences in the data.

Word embeddings can be trained on texts of a specific domain. In this way, word embeddings provide a deeper understanding of this domains. They can also be facilitated to gather domain information which is useful to integrate different information sources. Moreover, word embedding operations enable capabilities for semantic comparison. This can be utilized for information retrieval and data exploration. Despite this, word embeddings have been shown to be useful for a variety of machine learning task, especially for data integration purposes (e.g. entity resolution, schema matching, ...).

In this thesis, it should be investigated how word embeddings can be integrated in relational database systems. For this purpose, new operations for unstructured text values should be provided. Furthermore, techniques should be provided to combine the knowledge in the relational database with the information encoded in the word embeddings to enable inference based on combinations of logical and inductive reasoning.

Cardinality Estimation in the Context of Highly Selective Predicates

Axel Hertzschuch (axel.hertzschuch@tu-dresden.de)
Supervisor: Prof. Dr. Wolfgang Lehner

Cardinality estimation is a key input for the query optimizer to generate an optimal query execution plan. Even small estimation errors may lead to highly suboptimal decisions on the used order or implementation of database operators. While many approaches were studied on cardinality estimation, e.g. using histograms, sampling, or machine learning, it is still considered a grand challenge. Various systems use different forms of sampling as primary statistic. The reasons are manifold: Samples can reflect any data distribution without prior knowledge, training or query feedback. Sampling works independently of the underlying data type, predicate type and number of attributes.

Traditionally, we randomly draw a fixed number of tuples from a table and divide the number of qualifying sample tuples by the total number of sample tuples. Given a sufficient number of qualifying tuples, sampling based estimates are precise and give probabilistic error guarantees. However, sample sizes are very limited and evaluating complex predicates often leads to situations where no sample tuple qualifies; we call these *0-Tuple Situations* (0-TS). Although being a corner case, it is a frequent one. In these situations, query optimizers implement different heuristics, e.g. *Attribute Value Independence* (AVI). Relying on AVI results in strong estimation errors and potentially poor execution plans. Nevertheless, good estimates for small selectivities matter. For example, we see industrial strength optimizers where the decision of evaluating queries with precompiled, vectorized code or leveraging just-in-time compilation relies on precise estimates for highly selective predicates.

In this thesis, it should be investigated how query optimizers can adopt different policies depending on the predicate selectivity. Therefore, we develop and study models to improve estimates in the context of highly selective predicates. Further, we integrate these models with plan enumerators and study their effect on the resulting plan quality.

Compressed, Secure and Fault-Tolerant Data Representation in Databases

Juliana Hildebrandt (juliana.hildebrandt@tu-dresden.de)
Supervisor: Prof. Dr. Wolfgang Lehner

Database systems are characterized by two important aspects: (1) consistent and permanent data storage and (2) efficient and isolated data processing. To ensure these two aspects, database systems have to meet three challenges nowadays, which are briefly outlined below.

The **first** challenge is the efficient use of increasing main memory capacity. In order to achieve this, numerous database systems utilize a memory-centric architecture which occupies an important role for data compression. Because of the reduction in data size, the transfer times from CPU and main memory are reduced as well. This leads to decreased processing time. For that, beside basis data also intermediate results are compressed. Different algorithms for compression and decompression are suitable for various data characteristics, query types and hardware capabilities. But all algorithms share the opportunity to process the compressed data.

The **second** challenge is the protection of data misuse. For this, encryption and anonymization can be used. According to data characteristics and query types different property preserving encryptions like order preserving or homomorphic encryptions are suitable. Property preserving encryptions enable an efficient query processing on encrypted data.

A **third** challenge is the fault-tolerance on unreliable hardware. Because of the reduction in circuit line widths more transistors fit on a single chip, but the error rate of these chips increases. This is marked by transient bit flips, that occur in main-memory and CPU as well as during the data transmission. With the focus on data consistency, different kinds of error-detecting and error-correcting codes are suitable to handle this challenge.

In summary one may say that it is necessary to integrate an individual data representation for the storage and processing of data regarding to data characteristics, query types, hardware capabilities and weight of processing efficiency, confidentiality and fault-tolerance. With a view to the GRK *RoSI*, the framework conditions represent a context, so that a role modeling is an adequate approach. This very aspect is intended to be examined. Moreover it shall be analyzed how to use role modeling and a corresponding model-driven approach to integrate the different encoding algorithms. The manual integration of such algorithms is possible, but time-consuming and error-prone. Furthermore a configurability of data representations and adaptivity according to the three challenges is limitedly feasible.

Adaptive Routing in Disruption-Tolerant Network

José Irigon de Irigon (jose.irigon@tu-dresden.de)
Supervisor: Prof. Dr. rer. nat. habil. Dr. h. c. Alexander Schill

The Internet of Things (IoT) seems to be an ever-growing trend able to provide comfort and control in smart homes and improve productivity, performance, and efficiency in industrial processes. Devices connected via Internet generally use TCP/IP protocol suite, which is based on end-to-end connectivity. It is estimated that in 2025, about 50 billion smart devices will be available, able to collect and exchange data. Internet routing strategies are not always suitable to guarantee information exchange despite intermittent connectivity, energy constraints, or localization in isolated areas. Therefore, Disruption Tolerant Networks offer an alternative solution providing communication in the presence of high latency, high bit-to-error rate, or lack of end-to-end connectivity. A typical DTN example is to leverage the mobility of vehicles in public transport systems (buses, trains, or trams) to ship data. Buses and stations embedded with communication devices can provide data offload in smart cities and latency insensitive services for isolated communities.

Within a DTN, each device takes the route decision autonomously. Routing algorithms are classified according to the knowledge used to support the routing decision:

- naive routing replicates messages indistinctly (e.g., flooding);
- predictive routing decides based on past contact or mobility information (e.g., PRoPHET);
- scheduled routing represents contact plans as graphs and calculates the shortest path based on the least expected latency or maximum delivery probability (e.g., Contact Graph Routing).

Intuitively, precise knowledge about future contacts leads to the design of tailored algorithms that have superior performance, as long as the device mobility behaves as expected. However, in the rare event of unplanned mobility changes (disaster, accidents, flooding), the communication can be precluded, when it is needed at most. Therefore, a DTN framework for scheduled and predictive algorithms should be able to adapt to such situations.

This thesis proposes the design of an adaptive framework that adjusts the routing algorithm at run time. Considering that the devices need to exchange not only the data but also additional information to support the routing decision (metadata), the network overhead needs to be critically evaluated. Therefore, we plan to research what, when, and how to exchange metadata during contact opportunities to enable multiple routing algorithms. To evaluate our concept, we plan to assess the computing overhead caused by routing adaptation and simulate metadata exchange in scheduled scenarios to understand the trade-offs between metadata exchange and network overhead.

A role-based architecture for distributed self-adaptive systems

Tim Kluge (Tim.Kluge1@tu-dresden.de)
Supervisor: Prof. Dr. Uwe Aßmann

Today's computing world features a growing number of connected distributed systems that require the cooperation of many physical devices. Examples include cyber-physical systems like autonomous cars and co-working robots, which are expected to appropriately adapt to any possible context they find themselves in (e.g. the presence of a nearby human).

However, the controlling software continues to be developed using established object-oriented modelling techniques like UML, which do not natively possess a notion of context and thus may introduce accidental complexity. With increasing complexity, the probability of the introduction of software errors rises, which can have fatal consequences in cyber-physical systems. To address this, we envision a model-driven architecture for self-adaptive distributed systems that explicitly models structured context using the compartment role object model (CROM)[1] developed in our research training group. Entities are modelled as message-passing parallel processes and can play roles in specific contexts, which dynamically alter their behaviour and relationships with other parts of the system. A possible concurrency model to use is a context-aware refined Hewitt Actor model. Since the planning of complex adaptations can be cumbersome in real-world scenarios, we envision an intuitive declaration of adaptations as graph rewriting rules on the context model. Rule-based graph rewriting on other model types has been proposed for self-adaptation by related work[2]. Therefore, our work approaches the following research questions:

- **RQ1** How can role-based context-models be used to build distributed systems?
- **RQ2** How can decentral adaptations of such a system be planned?

To show that the proposed architecture actually supports the development of self-adaptive cyber-physical systems, it is planned to qualitatively evaluate the system by conducting multiple case studies. Additionally, a quantitative evaluation will be provided. We plan to use the code complexity and adaptation performance as the main measures. As claimed, our approach is expected to reduce the accidental complexity of software by supporting the development of context-adaptive systems with cross-cutting concerns.

[1] Thomas Kühn, Stephan Böhme, Sebastian Götz, and Uwe Aßmann. 2015. A combined formal model for relational context-dependent roles. In Proceedings of the 2015 ACM SIGPLAN International Conference on Software Language Engineering (SLE 2015). Association for Computing Machinery, New York, NY, USA, 113–124.

[2] Basil Becker and Holger Giese. 2008. Modelling of correct self-adaptive systems: a graph transformation system based approach. In Proceedings of the 5th international conference on Soft computing as transdisciplinary science and technology (CSTST '08). Association for Computing Machinery, New York, NY, USA, 508–516.

From Semi-Structured Documents to Relations

Elvis Koci (elvis.koci@tu-dresden.de)
Supervisor: Prof. Dr.-Ing. Wolfgang Lehner

Spreadsheets compose a notably large and valuable data set of documents within the enterprise settings and on the Web. They are extensively used by business professionals, scientists, and everyday common users. In the last years with the advent of the open data movement, an increasing number of government agencies, nonprofit organizations, and other institutions make data available as spreadsheets. However, transforming these data to another format or combining them with other sources (including other spreadsheets) is rather a cumbersome task. It still requires a considerable involvement from the user. The reason is that spreadsheets were primarily designed for human consumption and less for machine consumption. However, following the increase in data availability and the technological advancements, the demand and possibilities for deeper and more accurate analysis (of data) have increased. In the enterprise level new concepts have emerged, such "big data" and "data lakes". It has become more and more apparent that being able to integrate and reuse data from different formats can be very beneficial. These observations motivate the search for better methods to leverage the richness of spreadsheet data.

This PhD thesis aims at tackling this challenge by implementing a system (pipeline) able to understand the characteristics (e.g., structure of the data) of arbitrary spreadsheets and extract their data. This processing pipeline has to automatically perform many consecutive tasks, each dealing with a different aspect of the spreadsheet content, before being able to produce a rich usable output. In addition, the system should take into consideration that not all spreadsheets contain meaningful data. They are also used to create forms, scorecards, graphs, and other not genuine table structures. The intended solution should be able to filter out such cases, and only process genuine tables.

We envision that RDBMSs will be the primary environments to digest the exported data from a spreadsheet. After all, RDBMSs are the most used data management systems. However, it is our aim go beyond the relational model. The output of the processing pipeline will be stored in generic intermediate format that is capable of maintaining not only the exported data, but also its explicit and implicit characteristics. Furthermore, the system should be capable to transform on-demand the output to popular formats, such as JSON, XML, RDF, and relational tables.

Finally, we aim at a solution able to handle various and large volumes of spreadsheets. Therefore, we have considered for our experiments datasets of considerable size from different domains. These provide the settings for building a system that can be utilized at the enterprise level. Furthermore,

it can become an integral component of research projects from related areas, such as information retrieval, data management, and document analysis.

Decision Making using Probabilistic Model Checking in Self-Adaptive Systems

Max Korn (Max.Korn@tu-dresden.de)
Supervisor: Prof. Dr. Christel Baier

The ever growing demand on our software systems creates a lot of difficult demands on software systems. Many of these systems need to properly function in a variety of scenarios, with often completely different outside parameters. This makes software systems that are able to properly function under different contexts a necessity.

Self-adaptive systems are systems with the ability to make context dependent decisions at run-time, depending on internal and external factors. This ability to handle themselves in a multitude of environments makes them a widely studied research topic.

One kind of system that is especially dependent on context information are the role based systems, where certain actors have different behavior depending on the role they play. The goal of this thesis is to utilize formal methods, in particular probabilistic model checking, to create a suitable run-time decider for role based models, allowing these role-based models to become self-adaptive.

For this I first started creating a efficient run-time decider for systems without roles. For this I create a framework for decision making, that takes the formal model of a system to adapt, and creates the decider.

To do this, we use several instances of the formal model, which represent various expected environments, and compute expected consequences of possible decisions using probabilistic model checking. These expectations are then saved in a database. The creation of this database takes place outside of the system run-time, though on of the future goals is to allow the filling of this database at run-time, at least partially.

The decider then uses this database, as well as a specification of its current goals, to decide on the decision with the best expectation regarding this goal.

We check the performance of the decider, by combining certain instances of the formal model with the decider, on using statistical probabilistic model checking to compute performance measures. The instances used can vary from the ones used to create the database, to gather the deciders reaction on unknown environments.

In future, this thesis aims to incorporate role based systems, knowledge creation at least partially in run-time, and the ability to change the objectives of the decider during run-time.

Pattern notation for natural interaction in ubiquitous environments

Mandy Korzetz (mandy.korzetz@tu-dresden.de)
Supervisor: Prof. Dr.-Ing. Thomas Schlegel

Future user interfaces are going to be ubiquitous and seamlessly integrated into the world, offer a large variety of interaction modalities, facilitate situation-dependent adaptation to an increasing diversity of heterogeneous contexts of use and become more tangible, concrete and touchable again through connections with real objects. Interaction designers has to document best practices for such natural interactions appropriately so that other practitioners can use them easily. A common and problem-oriented method for capturing design knowledge is using interaction patterns. Standard pattern formats, e.g. Pattern Language Markup Language (PLML) [1], specify the upper layer with common elements like pattern name, problem and solution. However, interaction patterns are delivered mostly in narrative and unstructured text [2]. And in doing so, they mainly address the presentation of user interfaces. Natural interactions comes along with special characteristics which go far beyond a presentation of user interface elements. Hence, it is a lack of structured and detailed information for supporting tangible, multimodal, and situation-dependent interactions of future user interfaces.

This thesis aims at developing an enhanced pattern format and investigating the aspects of characteristic natural interactions between users and interfaces. An important aspect are parameters for describing natural interaction behavior, for example movements and gestures and their characteristics like speed, duration, start or end postures. Further on, the interaction context like the users situation, social and environmental affects are an decisive factor for applying a pattern. For investigating, three fields are focused:

- Augmented Reality (AR): interactions with virtual objects in the real world
- Device-based interactions: gestures with mobile devices held in the hand
- Wearable interactions: sensors and actuators attached to the body

The findings will lead to a framework for creating more consistent patterns for natural human-computer interactions. It is intended to give assistance

[1] Sally Fincher, Janet Finlay, Sharon Greene, Lauretta Jones, Paul Matchen, John Thomas, and Pedro J. Molina, "Perspectives on HCI Patterns: Concepts and Tools," *CHI '03 Extended Abstracts on Human Factors in Computing Systems, CHI EA '03*, ACM, pp. 1044-1045, 2003.

[2] Ahmed Seffah, "HCI Pattern Capture and Dissemination: Practices, Lifecycle, and Tools," *Pat- terns of HCI Design and HCI Design of Patterns: Bridging HCI Design and Model-Driven Software Engineering*, Springer International Publishing, pp. 219-242, 2015.

in creating and applying patterns with an improved format. In addition, interaction catalogs for each of the interaction fields are developed to show concrete applications.

Adaptable Collaborative Learning Environments

Tommy Kubica (tommy.kubica@tu-dresden.de)
Supervisor: Prof. Dr. rer. nat. habil. Dr. h. c. Alexander Schill

Learning environments, such as *Audience Response* or *Backchannel Systems*, provide a promising opportunity to address issues occurring in traditional higher education, e.g., the lack of interaction, by allowing students to participate anonymously in lectures using their mobile devices. This can promote the students' attention, increase the communication between the lecturer and the students, and foster active thinking during class[1]. Moreover, these systems can be used profitably in novel teaching formats such as *Flipped Classroom*. In order to choose an appropriate learning environment, numerous surveys list and classify these systems according to different criteria, e.g., supported features and platforms[2].

However, the introduction of such systems leads to its own challenges: The lecturers have to adjust their preferred teaching strategy to the chosen system, as this usually relies on a single supported didactic concept and therefore has a limited, fixed functional scope. Moreover, the lecturers have to select and use the system's functionality and interpret the received data by themselves – support or recommendations of a suitable functional scope are rarely provided[3]. Another issue becomes obvious by investigating different didactic concepts: While collaboration with subsequent group discussions is an integral part of various concepts, it is rarely or not at all supported by these systems[4].

Using the means of adaptation, we target to overcome these limitations. The following research question arises: *How can different levels of adaptation support the lecturer in using learning environments in a proper way?* To answer this question, three sub-questions are investigated:

- How will role-based modeling adaptation support the lecturer in creating customized scenarios?
- How will role-based runtime adaptation support the lecturer by providing collaborative functional proposals?
- What are trade-offs of using the concept of roles for learning environments?

[1] Quibeldey-Cirkel, K., "Lehren und Lernen mit Audience Response Systemen," Handbuch Mobile Learning, Springer, 2018.

[2] Kubica, T., Hara, T., Braun, I., Kapp, F., Schill, A., "Choosing the appropriate Audience Response System in different Use Cases," 10th International Conference on Education, Training and Informatics (ICETI), 2019.

[3] Kubica, T., Hara, T., Braun, I., Kapp, F., Schill, A., "Guided selection of IT-based education tools," 47th Frontiers in Education Conference (FIE), 2017.

[4] Shmelkin, I., "Untersuchung der Adaptierbarkeit webbasierter Audience Response Systeme," Main Seminar, Technische Universität Dresden, 2018.

Multimodal Interaction Concepts for Ubiquitous and Social Information Systems

Romina Kühn (romina.kuehn@tu-dresden.de)
Supervisor: Prof. Dr.-Ing. Thomas Schlegel

In collocated collaborative work scenarios analog media, such as paper and pen, are still very common to use. Their usage is intuitive, they are easy to get and very cheap. However, they lack in digitizing, further editing and sharing of content. In contrast, common devices, such as laptops, support digital creating of content but interfere social interactions of group members, since they form a physical barrier between two persons due to their size and form factor. There are also other technologies for digitizing easily in collaborative scenarios, for example, tabletops or display walls. They also provide direct digital creating, editing and sharing content but rely on special surroundings that provide these technologies. Mobile devices can bridge this gap because they are small enough to not hinder people but still can digitize content. Furthermore, nearly everybody nowadays owns such mobile devices, i.e. smartphones. Although mobile devices seem to have a lot of advantages, they still are not often used in collaboration. According to [1], non-intuitive interactions hinder people to use mobile devices collaboratively. By facilitating the interaction with such devices they can become as easy to use as paper and pen and thus support collaboration.

To address this issue I am aiming to investigate device-based interactions on mobile devices and how they can support collocated collaborative work scenarios. Device-based interactions are performed directly with mobile devices using built-in sensors. They depend on devices and their sensors, users and their cognitive abilities and the surrounding and specific situations. In this thesis the mainly addressed parameters for measuring and evaluating efficient collocated collaboration are user experience [2] and social interaction [3] between collaborating people. Different (user) roles and situations will be taken into account to get insights into how such interactions are performed depending on these roles. Several device-based interactions for collaborative scenarios based on specific tasks as well as requirements and challenges in collaboration are presented. Prototypically implemented, they serve as basis to show, compare and revise the efficiency of device-based interactions, to answer the question

[1] Andrés Lucero, Matt Jones, Tero Jokela, and Simon Robinson. 2013. Mobile collocated interactions: taking an offline break together. interactions 20, 2 (March 2013), 26-32.

[2] Sus Lundgren, Joel E. Fischer, Stuart Reeves, and Olof Torgersson. 2015. Designing Mobile Experiences for Collocated Interaction. In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '15). ACM, New York, NY, USA, 496-507.

[3] Gustavo Zurita, Miguel Nussbaum, Computer supported collaborative learning using wirelessly interconnected handheld computers, Computers and Education, Volume 42, Issue 3, April 2004, 289-314.

on the usefulness of such interactions in collaboration and to get measured results on the users' behavior.

Role-based adaptation of protection strategies in mobile environments

Christiane Kuhn (christiane.kuhn@tu-dresden.de)
Supervisor: Prof. Dr. Thorsten Strufe

Various approaches for protection strategies with different properties regarding the performance, cost and strength of protection have been proposed. For example in the privacy enhancing Tor-Network[1] packets are routed over multiple hops and in every hop encryption operations take place. Usually this causes so much delay that it is unsuitable for Voice-over-IP calls.[2] However, with different trust assumptions better performance can be achieved by reducing the number of hops.[3] In general a solution space is built between application requirements, performance and security properties of different approaches.

A role concept can help to cover the user's needs and resources. Our research includes how participants can be dynamically assigned to roles based on their current computational and storage resources, connectivity and requirements of the running applications. Roles of participants might for instance be mobile browsing or mobile video conferencing. Inside the solution space of protection approaches, operating points being beneficial for the participants in different roles shall be defined. Further, it shall be researched which transitions between roles are possible and which reactions are advantageous. For example how the protection strategies should be adapted when a person comes home from work and the person's mobile phone switches from the cellular network to home WLAN.

[1] Dingledine, Roger, Nick Mathewson, and Paul Syverson. "Tor: The second-generation onion router." Naval Research Lab Washington DC, 2004.

[2] Dhungel, Prithula, et al. "Waiting for anonymity: Understanding delays in the Tor overlay." Peer-to-Peer Computing (P2P), 2010 IEEE Tenth International Conference on. IEEE, 2010

[3] Le Blond, Stevens, et al. "Herd: A scalable, traffic analysis resistant anonymity network for VoIP systems." ACM SIGCOMM Computer Communication Review. Vol. 45. No. 4. ACM, 2015.

Towards Robust Decentralized Self-Adaptive Systems

Daniel Matusek (daniel.matusek@tu-dresden.de)
Supervisor: Prof. Dr. rer. nat. habil. Dr. h. c. Alexander Schill

Today's computer networks are largely distributed and therefore require steady maintenance. To tackle this problem, so-called context-aware self-adaptive systems could be used to change the behaviour depending on their environment without human interaction. However, most of the proposed systems use a central instance to control adaptation across multiple devices, which could lead to bottlenecks and reduce scalability.

Solving the problem of adapting systems to changing context and its environment would allow for nearly perpetual running systems. A decentralized solution for coordinating adaptation would increase robustness and allow for improving the scalability of those systems [1].

In the recent years, researchers proposed first approaches for the decentralized coordination of adaptations. By using adaptation managers on each device which are responsible for the administration of the nodes and developing a communication protocol to invoke adaptations decentrally, the need for a central instance was superseded. Nevertheless, those approaches need further investigation regarding the robustness of decentralized adaptation to make them more viable. Problems can still occur when it comes to node failures in big systems and a whole system gets partitioned into several subsystems. The resulting subsystems now perform adaptations by their own, which requires synchronisation of the resulting states afterwards. The same applies for systems of systems, which are partitioned on purpose. When they get aggregated to perform a common task or to dynamically higher performance, decentral adaptations need to get applied on subsystems which are originally in different states.

Another challenge is decentral adaptations in streaming applications. Consider two streaming operators on two different nodes, which perform a common task and one operator depends on the other. Since we have a continuous dataflow in the streaming use-case, it is not trivial to adapt the behaviour of each node. This has to be done in a synchronized way to avoid incorrect states and false transitions. The current protocol[2] does only consider the role lifecycle of a single instance, which could lead to inconsitencies.

[1] Weyns, D., Bencomo, N., Calinescu, R., Camara, J., Ghezzi, C., Grassi, V., Grunske, L., Inverardi, P., Jezequel, J.-M., Malek, S., Mirandola, R., Mori, M., and Tamburrelli, G. (2017). Perpetual Assurances for Self-Adaptive Systems. In R. de Lemos, D. Garlan, C. Ghezzi, and H. Giese (Eds.), Software Engineering for Self-Adaptive Systems III. Assurances (Vol. 9640, pp. 31–63). Springer International Publishing. https://doi.org/10.1007/978-3-319-74183-3_2

[2] Weißbach, M., Chrszon, P., Springer, T., and Schill, A. (2017). Decentrally Coordinated Execution of Adaptations in Distributed Self-Adaptive Software Systems. Proceedings - 11th IEEE International Conference on Self-Adaptive and Self-Organizing Systems, SASO 2017, 111–120. https://doi.org/10.1109/SASO.2017.20

Managing Parallelization and Heterogeneity with Declarative Invasive Software Composition

Johannes Mey (johannes.mey@tu-dresden.de)
Supervisor: Prof. Dr. rer. nat. habil. Uwe Aßmann

Complex code transformations and compositions can be useful in a variety of application domains. One of these is the programming of wildly heterogeneous systems, which introduces new challenges to maintain programmability, because developers do not only have to produce parallel code, but also code for very different and potentially unanticipated target platforms.

Current parallelization and distribution strategies are able to handle those concerns for specific target platforms efficiently, but are both not easily exchangeable and require detailed knowledge of the application code, its performance, and the target platform. A common strategy to create a parallel program is to gradually extend a sequential program with the commands and pragmas, a process called *progressive parallelization*. This process, however, causes an entanglement of concerns that makes testing, benchmarking, and evolving both the core code and the additions difficult.

To overcome these problems, we introduce a novel code composition and transformation approach called Orchestration Style Sheets (OSS). OSS borrow the well-known concept of style sheets and transfer it to annotation and enrichment of source code, in this case for parallelization. Parallelization (and other secondary) concerns are externalized into *styles* that can be defined separately as well as exchanged and reused for multiple programs. This approach is similar to aspect-oriented programming (AOP), but goes further in some respects: e.g., the pragmas used in the Open* languages are heavily parametrized with elements of the core code like lists of private or shared variables. In principle, many of these parameters can be deduced automatically, which requires static analysis of the core program. OSS offer user-defined attributes that can perform this analysis, thus eliminating the error-prone process of deriving the parameters manually and allowing a reuse of styles.

While parallelization is the current main focus, the approach is both language-independent and applicable to different use cases. Currently, there are several systems based on this framework: OSS for Fortran, a language (still) frequently used in parallel programming has been used to evaluate the concept in realistic use cases like simulations used in mechanical engineering. A second, large system is Java-based and uses a complete attribute grammar-based compiler front-end. Additionally, the framework can easily be applied to smaller languages, i.e. domain-specific languages.

Reasoning in Description Logic Ontologies for Privacy Management

Adrian Nuradiansyah (adrian.nuradiansyah@tu-dresden.de)
Supervisor: Prof. Dr. Franz Baader

A rise in the number of ontologies that are integrated and distributed in numerous application systems may provide the users to access the ontologies with different privileges and purposes. Considering this situation, preserving confidential information from possible unauthorized disclosures becomes a critical requirement. For instance, in the medical area, unauthorized disclosures of medical information do not only threaten the system but also, most importantly, the patient data.

Motivated by those circumstances, this thesis initially investigates a new reasoning problem, called the *identity problem*, where the identity of (anonymous) objects stored in Description Logic ontologies can be revealed or not. We further extend the setting of this problem in the context of role-based access control to ontologies before we turn to a problem, which asks if the identity of an anonymous object belongs to a set of known individuals of cardinality smaller than the number k.

If it is the case that some confidential information of persons, such as their identity, their relationships or their other properties, can be deduced from an ontology, which implies that some privacy policy is not fulfilled, then one needs to repair this ontology such that the modified one *complies* with the policies and preserves the information from the original ontology as much as possible. The repair mechanism we provide is called *gentle repair* and is performed via axiom weakening instead of axiom deletion which was commonly used in classical approaches of ontology repair. To realize this repair mechanism, we also introduce formal procedures to weaken ontology axioms by means of *weakening relation*.

However, policy compliance itself is not enough if there is a possible attacker that can obtain relevant information from other sources, which together with the modified ontology still violates the privacy policies. *Safety* property is proposed to alleviate this issue and we investigate this in the setting of privacy-preserving ontology publishing. Within this setting, we additionally require *optimality* property which asks if the modified ontology is safe for the policy and is obtained from the original ontology in a minimal way.

The main contributions of this thesis are inference procedures that are used to solve those privacy problems and additional investigations on the complexity of the procedures, as well as the worst-case complexity of the problems.

Role-Based Smart Contract Development in Multi-Agent Systems

Orçun Oruç (orcun.oruc@tu-dresden.de)
Supervisor: Prof. Dr. Uwe Aßmann

Agents have evolved with roles and enhanced their capability through the dynamicity of roles. Multi-agent systems provide solutions spatially and temporarily distributed using role-based agents. To do that, agents need to be synchronized with each other by using special message exchange protocols. Multi-agent systems do not suffer from single point of failure because of the decentralized deployment. In this study, we will research the development of decentralized blockchain technology whether we can implement the blockchain to agents that reside in the supply chain management or not. The smart contract, which is an application layer of the blockchain, will be chosen to implement a contract-oriented language concept. By realizing the topic from the multi-agent perspective, we will be able to identify the challenges regarding contract-oriented language implementation in the role-based approach.

The importance of the research is based on two key elements. The first one is a role-based language integration to the decentralized database technology called blockchain with its object-oriented language. The second one is increasing the collaborative and autonomous capability of multi-agent systems through smart contracts. To identify the above-mentioned key points, we will answer two fundamental research questions (RQ):

- RQ 1: Can we realize the blockchain smart contracts language for smart contract language for context-aware multi-agent systems?
- RQ 2: How can we build up a role-based context-aware language from object-oriented smart contracts language?

Simulation software will be applied in order to answer this question. Our main point is to develop a model-driven tool that will create Solidity smart contract language from the compartment role-object model (CROM) with a tool such as FRaMED eclipse-based editor [1].
Normally, agent system design is a complex task in terms of collaborative behaviour [2]. We will establish the collaborative level of the multi-agent system. Another uncovered point is how to provide pro-activeness for a multi-agent scenario with blockchain. To this end, smart contracts act as intermediaries in the simulation process with situation awareness that is concerned with anticipating foreseeable situations [3].

[1] https://github.com/Eden-06/FRaMED-2.0
[2] https://www.researchgate.net/publication/228817042_Role-based_multi-agent_systems
[3] https://ieeexplore.ieee.org/document/1342928

We will simulate the application with the JADE framework for multi-agent systems for supply chain simulation. In essence, supply chain management can provide all kinds of agent communication, collaboration, and proactive situations. We are planning to implement a simulation software regarding distributors, retailers, transporters, warehouses, customers, and manufacturing companies in the domain of Industry 4.0.

In future work, we will be researching into the smart contract framework development under uncertainty in distributed domains [4]. In contrast, human communication and collaboration need a lower amount of information than the agent communication. The main research point for future work will be that blockchain-based smart contracts may outperform without increasing data size between agents.

[4] https://usc-isi-i2.github.io/papers/maheswar09-aamas.pdf

Achieving situative privacy protection in a fog environment using situative privacy modeling of a DSPL of role-based pseudonym systems

Frank Rohde (frank.rohde@tu-dresden.de)
Supervisor: Prof. Dr. Uwe Aßmann

Problem The fog computing paradigm was proposed as an extension to the cloud computing paradigm enabling low-latency IoT applications that involve widely distributed nodes. Privacy protection is a challenge for those applications. It can be tackled by the use of pseudonyms [1]. While fog computing mitigates some of the disadvantages of cloud computing it creates a new challenge related to the heterogeneity of the nodes providing the fog service and the presence of highly dynamic client-server relations: situative privacy protection (scientifically described by Mann et al. .[2]), i.e., the challenge to deal with privacy threats that dynamically emerge from the current situation of the client within the fog-based computing environment (e.g., available computing power and hardware security measures of the service-providing fog nodes). Pseudonym systems that implement pseudonym specific behaviour show another problem with respect to their code quality: the respective code is scattered throughout the code base and is tangled with unrelated code as pseudonym specific behaviour is a cross-cutting concern.
Solution This thesis investigates the applicability of feature-oriented software development as an approach to design and implement a pseudonym system that is able to deliver situative privacy protection for fog-based applications. We propose a pseudonym system architecture that allows for the functional variability which is required for situative privacy protection and describe this functional variability by means of a feature model. Decisions with respect to runtime feature adaptation are taken based on a model of the current client situation. We analyze and discuss the applicability of petri nets for client situation modelling in fog computing. Moreover, we analyze and discuss the suitability of the Role-concept to mitigate scattering and tangling in implementations of pseudonym-specific behaviour.
Contributions The contributions of this thesis are threefold: (1) The suitability of feature oriented software development, more specifically software product line engineering, to achieve situative privacy protection for fog computing is analyzed and discussed by means of an exemplary privacy technology: pseudonym systems (2) The applicability of petri nets as a context model for situative privacy protection in fog computing is discussed; (3) The suitability of the role concept to tackle scattering and tangling of code that implements pseudonym-specific behaviour is discussed.

[1] Schaub et al. "Pseudonym schemes in vehicular networks: A survey". IEEE communications surveys and tutorials. 17.1 (2014): 228-255.

[2] Mann et al. "Situativer Datenschutz im Fog-Computing". Informatik Spektrum, 42.4 (2019): 236-243

Role-based Adaptation of Structural Reference Models

Hendrik Schön (hendrik.schoen@tu-dresden.de)
Supervisor: Prof. Dr. Susanne Strahringer

Large software systems are in need of a construction plan to determine and define every concept and element used in order to not end up in complex, unusable and cost-intensive systems. Different modeling languages, like UML, support the development of these construction plans and visualize them for a system's stakeholders. Reference models are a specific kind of construction plan that capture domain knowledge for reuse through adaptation. The actual benefit of reference models is their adaptivity towards a specific use case. They work as a blueprint and the users can apply their own adaptations to fit specific demands. In order to perform these adaptations, the user can rely on various tools and mechanisms.[1][2] Our approach is to combine these reference model adaptations with the concept of roles[3] to model the more dynamic parts and to separate the core elements (provided via the reference model) from user made adaptations. This leads to a strict separation of the two aspects – reuse and adaptation – within application model construction. The actual advantage of using roles as the sole adaptation mechanism is twofold: *(a)* the structure from the original reference model and the dynamics from roles can be combined to model the interface between structure and behavior, and *(b)* through the strict separation of these aspects it will be easier to react on evolution (new versions) of the reference model and easier to (re)adapt to new requirements and features. As a consequence, the roles enriched final application model can be used to describe systems in more detail, with different perspectives, and, if available, can be implemented with role supporting programming languages. But even without this step, the application model itself will provide valuable insights into the overall construction plan of a system through the combination of structure and behavior and a clear separation of relatively stable domain knowledge from its use case specific adaptation.

We will propose a clearly defined methodological approach to adapt a reference model into a user specified application model via roles. Our aim is to constitute and evaluate such an approach and establish it as a modeling paradigm for applying roles on reference models. This includes the development of a (formal) domain specific modeling language as well as tools to support the actual use of the new approach. Related topics are software development and evolution, software architecture, system and enterprise modeling.

[1] P. Fettke, P. Loos. "Classification of reference models: a methodology and its application". In *Information Systems and e-Business Management*. 2003

[2] B. Hofreiter, C. Huemer, G. Kappel et al. "Inter-organizational reference models - May inter-organizational systems profit from reference modeling?". In *Business System Management and Engineering*. 2012

[3] J. Almeida, G. Guizzardi and P. Santos. "Applying and extending a semantic foundation for role-related concepts in enterprise modelling". In *12th IEEE International Enterprise Distributed Object Computing Conference*. 2008

Compilation and Interpretation Techniques for Role-based Programming Languages

Lars Schütz (lars.schuetze@tu-dresden.de)
Supervisor: Prof. Dr.-Ing. Jeronimo Castrillon-Mazo

In recent years many role-based programming languages have been developed. Since there is no common understanding of what roles are, existing role-based programming languages provide different sets of role features.[1] The more role features are supported by a role-based programming language the more complexity is added to the runtime.

In object-oriented programming, the runtime type of objects (i.e., subtype polymorphism) affects the dispatch of method calls on these objects. That is, the method call cannot be resolved statically at compile-time, but has to be resolved dynamically at run-time. In role-based programming, there is another dimension to method dispatching – roles played by the object have to be taken into account. Thus, roles provide an orthogonal polymorphism to the existing subtype polymorphism. Available methods depend on the class type as well as the role types an object is playing. Because of the semantic gap between the role-polymorphic dispatch and the targeted object-oriented machine models the role-polymorphic dispatch is implemented as a verbose description using the object-oriented machine model. Therefore, existing solutions incur in large overhead and suffer from inferior runtime performance.[2]

To succeed in adopting role-based software infrastructures the performance must be on par with current mainstream programming languages. In this dissertation we will study the performance bottlenecks inherent to programming with roles and devise solutions, from the compiler and the language perspective, to circumvent them. If a program does not use specific role features, the runtime performance should not suffer. Profiling the usage of role features during run-time, dynamic compilation could provide performance dependent on the specific use of an application.

[1] T. Kühn, M. Leuthäuser, S. Götz, C. Seidl, and U. Aßmann, "A metamodel family for role-based modeling and programming languages," in *Software language engineering*, vol. 8706, Springer, 2014, pp. 141-160.

[2] L. Schütze and J. Castrillon, "Analyzing State-of-the-Art Role-based Programming Languages," in Proceedings of the International Conference on the Art, Science, and Engineering of Programming - Programming '17, Brussels, Belgium, 2017, pp. 1–6.

Monitoring for Control in Role-oriented Self-Adaptive Systems

Ilja Shmelkin (ilja.shmelkin@tu-dresden.de)
Supervisor: Prof. Dr. Alexander Schill

Self-adaptive Systems (SASs) are one way to address the ever-growing complexity of software systems by allowing the system to react on changes in its operating environment. In today's systems, self-adaptation is typically realized with a control loop, for which the MAPE-K feedback loop is a prominent example. Research uses the notion of patterns to describe the distribution and decentralization of individual control loop components or control loops and their underlying *managed subsystems*. While there are some well-accepted standards about which components a managed subsystem has to implement so that it can interact with the control loop, research still lacks best practices for communication *within* and *across* control loops. The author's thesis aims to find principled solutions to decentralized self-adaptation by defining standardized interfaces and communication protocols for SASs that rely on control loops as well as a standardized monitoring metric representation format.

Role-based adaptation of reference models to application models using business process modeling languages

Tarek Skouti (tarek.skouti@tu-dresden.de)
Supervisor: Prof. Dr. Susanne Strahringer; Prof. Dr. Frank Furrer

Reference process models provide a standardized model that can be adapted to an individual business' requirements. The rise of knowledge workers mandates from one employee to fulfill multiple complex tasks and to take on multiple roles in a business process. A single process can have multiple variations. To model business processes, various Business Process Modeling Languages (BPML) were introduced. The most prominent and de-facto standard BPML being BPMN. Existing BPMN extensions that tackle process modeling challenges are presented. New challenges that have not been solved by these extensions arise from Industry 4.0 and the digitalization. The three main challenges are:

- **Performer**
  A knowledge-worker takes on multiple Roles and performs complex tasks.
- **Adaptation**
  Increasingly demanding customers require constant adaptation of processes
- **Context**
  The context of a process can change during the execution because of new information presented

To solve these challenges a role-based BPMN extension (RBPMN) is introduced. Roles as the main concept of RBPMN allow the expression of the Performers duties, the adaptation of the process during execution of it, and the modeling of context and changes of it. The applicability of RBPMN is validated on various processes from the financial industry. An empirical comparison of RBPMN to the standard BPMN and other BPMN-Extensions is made to showcase the strength of the approach. An experiment is conducted to compare the information richness of RBPMN in combination with BROS and BPMN in combination with UML Class Diagram. It is proven that RBPMN allows for an easier adaptation and richer process models.

Context-Sensitive Description Logics in a Dynamic Setting

Satyadharma Tirtarasa (satyadharma.tirtarasa@tu-dresden.de)
Supervisor: Prof. Dr.-Ing. Franz Baader, Prof. Dr. Ivo F. Sbalzarini

Description Logics (DLs) are a family of knowledge representation formalism that cover a large number of application domains by choosing an instance with appropriate expressivity and complexity. However, the picture changes when the capability to represent meta-concepts, such as contextual knowledge is needed. It is not possible, or at least in an intuitive way, to describe context-sensitive information using classical DLs. This leads to the investigation of DL extensions with a context facet. One result of the research in this direction are *contextualized DLs* (ConDLs)[1], a family of two-dimensional DLs tailored for reasoning on a context-sensitive domain. By imposing the restriction that a signature in the object level can not access the meta level, the decidability is maintained even with the presence of rigid concept and role.

Unfortunately, the problems under consideration so far are static in some senses. We take a look at some common reasoning problems in a dynamic domain with considering context-sensitive DLs and investigate how they are intertwined. The expressiveness and computational complexity results will be very important, especially considering both formalisms are prone to undecidability.While the interaction between ConDLs and dynamic domains is relatively unexplored, the interaction between classical DLs and dynamic domain, such as *action formalisms*, has been studied[2]. Our study yields a ConDL-based action languages[3] which the projection problem with a basic ConDL is well-behaved, i.e., has the same complexity with the consistency problem of the underlying ConDL.

Furthermore, we inspect how to use such formalized framework as an underlying knowledge base for the application domain, and naturally in the means of context-sensitive languages and systems. Specifically, we will consider *role-based* modeling languages and formalize the problems that arise there to our framework. It has been shown that the aforementioned ConDLs are capable to represent role-based systems[4]. Some examples of the problems that can be tackled in a dynamic setting are building run-time system monitor or verifying temporal properties over the system.

---

[1] S. Böhme and M. Lippmann, "Decidable Description Logics of Context with Rigid Roles," *Proceedings of the FroCoS 2015*, p. 17–32, 2015.

[2] F. Baader, C. Lutz, M. Milicic, U. Sattler, and F. Wolter, "Integrating Description Logics and Action Formalisms: First Results," *Proceedings of the AAAI 2005*, p. 572–577, 2005.

[3] S. Tirtarasa and B. Zarrieß, "Projection in a Description Logic of Context with Actions," *Proceedings of the GCAI 2019*, p. 81–93, 2019.

[4] S. Böhme and T. Kühn, "Reasoning on Context-Dependent Domain Models," *Proceedings of the JIST 2017*, p. 69–85, 2017.

Role-Modeling in Round-Trip Engineering for Megamodels

Christopher Werner (christopher.werner@hbsc-werner.de)
Supervisor: Prof. Dr. rer. nat. habil. Uwe Aßmann

In the software development process, different kinds of models are used to describe each development step. Therefore, software development with role models has to manage requirement models, role-based design models (platform-independent and platform-dependent), implementation models, test models, as well as the code. Usually, this ensemble of models, also called a megamodel, must be kept consistent using round-trip engineering for editing such an ensemble of models. There are different approaches which use single underlying models or modular single underlying models to create dynamic views for software developers and only look on the synchronization of these views to the underlying model. The main problems of these approaches are the consistency and the manual interventions, when problems come up. With the integration of roles in models and metamodels, it is easy to form views on models, because roles compartmentalize objects so that these can be projected naturally into slices. For round-trip engineering, this means that edits can be restricted to a view on the megamodel, and the synchronization operations become much simpler. For singular models, this has been assured by Seifert [1] and for megamodels, it is done in this thesis. In particular, for a RoSI megamodel, which supports developers with a consistent set of related models from requirements engineering to testing, this will be done by investigating different role-based model synchronization strategies. As an evaluation, the implementation of a test-case scenario will be created.

[1] M. Seifert, "Designing Round-Trip Systems by Model Partitioning and Change Propagation," *Qucosa*, Technische Universität Dresden, Fakultät Informatik, June 2011.

GRK 2050: Privacy and Trust for Mobile Users

Prof. Dr. Max Mühlhäuser
Email: muehlhaeuser@privacy-trust.tu-darmstadt.de
Technical University Darmstadt
Internet: https://www.privacy-trust.tu-darmstadt.de

The RTG 2050 *Privacy and Trust for Mobile Users* is a highly interdisciplinary collaboration between Computer Science and the fields of Law, Sociology, Information Systems (in Economics), and Usability (in Psychology). We aim at improving the position of mobile users – think of smartphone users – vis-a-vis digital service networks, social networks in form of digital collectives, and sensor-augmented environments, i.e., "IoT" environments (all summarized in the follwing as 'networks').

In the mobile users' experience, these networks and the players therein are becoming increasingly opaque while the users themselves are becoming increasingly transparent. The term 'players' here refers to all kinds of digital 'counterparts' of mobile users and to the responsible people and organizations, such as service providers, social network providers and peers, smart environment operators, network operators, hard- and software vendors. In a multi-disciplinary effort, our RTG counters these 'paired trends' – transparent users and opaque networks – with the 'paired goals' privacy & trust: *privacy* is considered as the main instrument for limiting user transparency, while assessing the expected *trust*worthiness of players in the network is considered as the main instrument for countering the opaqueness of the network players.

Privacy and trust are not yet commonly perceived as paired, i.e., tightly interwoven necessities for making the Internet (and networks in general) a liveable digital habitat. This is in part due to a somewhat misleading use of the term trust in cybersecurity research: fields like trusted computing, trustworthy ICT, and trust management refer to issues of reliability-plus-security, tamper-free hard- and software, and digital identities, respectively – all quite remote from the primary meaning of the term trust. Our RTG fosters research into trust in its primary meaning: justified readiness to engage in a risky engagement, with risks including privacy violations and other negative experience with service provision. An important area of our trust research is *computational trust*, where trust is formalized as the probability of a trustee acting as expected; expectations in turn are justified from two categories of evidence: experience (own prior experience, reputation) and indicators (certified audit results, attestations, etc.). Since trust assessment relies on evidence, i.e., information about the trustee, there is a potential conflict: trust aims at revealing what privacy aims at concealing: information about an entity.

This is relevant if trusters and trustees do not form two distinct sets (cf. social network participants and agents in peer-to-peer economies). In the RTG, privacy related research is (at least) as prominent as research on trust. Due to their interweaving, we are addressing both aspects jointly in our research areas, structuring our RTG according to the above-mentioned network categories: (social) collectives, service networks, and sensor networks in form of the 'IoT' – with an additional focus area emphasizing novel mobile user support.

Outside the digial world, both trust and privacy were concerns since millenia. This mandates our interdisciplinary approach that involves Sociology, Psychology, Laws and Economics. Our experts from these fields contribute long standing experience in linking their disciplines to issues from the digital world, which greatly facilitates their cooperation with our computer scientists.

Effects of Transparency on Trust in AI Applications

Mariska Fecho (fecho@is.tu-darmstadt.de)
Supervisor: Prof. Dr. Peter Buxmann

Artificial intelligence and machine learning methods are already used in many areas of our lives (e.g. medical diagnosis, autonomous driving, digital voice assistants) and are also becoming increasingly important in the digital economy. A key concern, which is often discussed in the context of intelligent systems, is their black-box behaviour. Due to their complexity, the results and functions of the algorithms are often not transparent for the user. Some users are even completely unaware of the intelligence of a system. This is particularly critical with regard to automated decision processes, where decisions are delegated completely or partially to a machine or system.

Trust is an important factor for the design of a technology, as it has a significant influence on the initial acceptance and further use of technologies.[1] Transparency may promote trust in a technology, for example by providing explanations that enable the user to understand how the technology works.[2] However, the extent to which transparency can contribute to build trust and in what context transparency is particularly important is still under investigation.

This project aims to investigate the extent to which transparency can influence the trust of users in AI applications. Users' requirements of AI applications shall be analysed and measures for the development of trustworthy intelligent systems shall be investigated. Furthermore, different contexts with various levels of transparency shall be considered. In addition, the use of intermediaries and central authorities for the assessment of trustworthy AI systems shall be investigated.

[1] Benbasat, Izak; Wang, Weiquan. Trust in and adoption of online recommendation agents. Journal of the association for information systems,vol.,no. 3, p. 4., 2005.

[2] Adadi, Amina; Berrada, Mohammed. Peeking inside the black-box: A survey on Explainable Artificial Intelligence (XAI). IEEE Access, vol. 6., p. 52138-52160., 2018.

Analysis of Privacy and Security Impacts Through Side-Channel Attacks

Matthias Gazzari (mgazzari@seemoo.tu-darmstadt.de)
Supervisor: Prof. Dr. Matthias Hollick

In our world of ever increasing complex computing systems it becomes increasingly difficult to stay in control of the information flow between devices. An ever increasing number of more accurate sensors creates a lot of opportunities but also possibilities to violate the privacy and identity of users. In my current work I am focusing on analysing data from mobile sensors and input devices in respect to private information retrieval and user identification.

In the first part of my work, I am focusing on the analysis of side-channel attacks for reconstructing user inputs on keyboards, for example. For doing so, I investigate device-targeted attacks and user-targeted attacks by observing sensor values from devices measuring human actions.

Similarly, I use sensor measurements for the second part of my work in the context of user identification. I am currently investigating how reliable specific measurements are, for example in case of a desired identification.

As part of my side-channel analysis related work, I am leveraging EMG and IMU data from the forearms to reconstruct whether and what has been typed on a keyboard. To do so, we have collected a data corpus containing about 318000 keystrokes from 38 participants typing predefined texts and passwords. Using end-to-end machine learning we have already shown during our master thesis that keystroke detection is feasible. We are now in the process to combine these results with a keystroke identification system in order to reconstruct passwords from sensor data. In doing so, we will be able to quantify the information gain for reducing the search space of a brute force attack on passwords.

Leveraging the same type of sensor data, we are currently working on doing a user-targeted side-channel attack to reconstruct handwriting. Similarly, we are in the process of conducting a keyboard-targeted temporal side-channel analysis by observing the wireless network traffic. For both of these projects data studies with multiple participants are planned in order to study whether such attacks could be applicable between subjects or only for a single target.

As part of the second part of my work, we are trying to implement a PPG based inter-sensor impersonation attack on an ECG based authentication system. In essence, we use generative adversarial machine learning to transform PPG data and thereby generate valid samples to fool an ECG identification. For creating the final authentication system and the transformation network we are currently in the process of collecting a data corpus in another data study.

In the future, we will be looking into incorporating these findings from the studies above in order to develop techniques for circumventing or reducing the impact of such attacks.

AlterEgo as Trustworthy Device Collective

Dr. Tim Grube (grube@tk.tu-darmstadt.de)
Supervisor: Prof. Dr. Max Mühlhäuser

Smartphones have become a commond and ubiquitous device for handling our poersonal data as well as for interacting with services and devices—mobile devices are becoming our digital counterpart, i.e., are becoming our AlterEgo. Rather than protecting our privacy, today's mobile devices on the contrary distribute personal data. More worrying, our options to assess their trustworthiness are slim to non-existing. Finally, today's mobile devices lack the ability to prove our trustworthiness to others, and, in return, allow us to quantify the trust in services, OSNs, and devices. The goal of this project is to evolve mobile devices into a true digital counterpart—an AlterEgo. Users should be able to assess the trustworthiness of their digital counterpoarts and to control their personal data. Further, users, services, OSNs, and devices quantify the trust in each other. Ultimately, AlterEgo should not only be capable of supporting the user but also of acting autonomously on the user's behalf.

To achieve this goal, D.4 follows a layered approach: (1) federated and recursive AlterEgo architecture, (2) socio-technically based middleware, (3) proactive user assistance, and (4) mechanisms to protect privacy and assess trust according to dynamic constraints.

Layer 1 provides the basis for the middleware AlterEgo of layer 2. AlterEgo is a recursive concept on (at least) three levels. On the middle level, the devices of a user, e.g., smartphone, smartwatch, and PC, cooperate to establish privacy protection and trust assessment using, e.g., majority-based decisions. The lower level distributes the AlterEgo-functionality among the components of a single device; the higher level establishes the functionality of AlterEgo among the social connections of a user.

On layer 2, the focus is on leveling the interests of *all* involved parties. In order for AlterEgo to be trustworthy, i.e., trusted by the user, and accepted by all stakeholders, it is conceptualized on a socio-technical basis. That means, hard- and software is specified within a multi-stakeholder process to ensure that the expectations of all stakeholders are reflected and that the specification of AlterEgo is communicated in an *understandable* form to them.

Layer 3 extends AlterEgo with proactive assistance functionality. This functionality intends to increase the users' understanding of their actions' implications on privacy and trust and even aims at interacting on the users' behalf. AlterEgo derives the preferences by learning from both the user's actions and occasional queries. Psychologically backed nudges should enable the users to finally achieve their very personal privacy and trust demands.

Layer 4 links this research project to the other research areas of the RTG 2050 by combining their research into a holistic AlterEgo with additional measures

to flexibly assess privacy and trust, and enabling respective enforcement measurements.

Building and Using Social Capital in Digital Collectives

Hendrik Jöntgen (joentgen@wiwi.uni-frankfurt.de)
Supervisor: Prof. Dr. Oliver Hinz

Digital Collectives are temporary unions of social media users who cooperate and share their resources and knowledge with each other in order to achieve a shared goal. Due to the ever-increasing usage of social media, these Digital Collectives are becoming progressively common and important. These collectives can be very short-lived or sustain themselves over a longer period of time. Furthermore, they can be uncoordinated or have a single or multiple leaders. And finally, these collectives can result in positive or negative outcomes. For example, although companies can use social media platforms as an effective channel to promote their products and services, they also become vulnerable to online firestorms where their community turns against them[1] and consequently suffer damages to brand value or boycotts[2]. As another example, Open Source Software Communities allow the independent creation of software. The fundamental question here is how users are being motivated to participate in these projects.

Regarding online firestorms, previous literature is mainly focused on giving overviews about the phenomenon and advice on how companies should react to them while previous literature on Open Source Software Communities has already addressed the motivation to participate in those communities but neglected the motivation to join a specific Open Source project. The goal of my research is therefore the examination of motivations to join a specific Digital Collective and the role of Social Capital in these decisions.

In order to do so I am using crawled data from Twitter and GitHub users and their social networks. In addition to statistical tests on real-word data, I am conducting surveys to further test the effects of Social Capital on the motivation to join a Digital Collective.

Finally, the results will contribute to a better understanding of Digital Collectives and their formation and can also be used to allow a better usage of these collectives.

[1] Pfeffer, J., Zorbach, T., and Carley, K. M. (2014). Understanding online firestorms: Negative word-of-mouth dynamics in social media networks. Journal of Marketing Communications, 20(1–2), 117–128.

[2] Mochalova, A., and Nanopoulos, A. (2014). Restricting the spread of firestorms in social networks. Proceedings of the 22nd European Conference on Information Systems (ECIS)

Trust Valuation in Decentralized Digital Infrastructures

Suzette Kahlert (kahlert@privacy-trust.tu-darmstadt.de)
Supervisor: Prof. Dr. Jörn Lamla

One of the main goals in the research area B1 "Trust and Trust Assessment in Social Networks" is to establish complex socio-technical trust infrastructures that are being used and valued for their protection of privacy and enable people to use and trust trust infrastructures. Therefore, it is required to research trust valuation as complex social practices that oscillate between expertise about technical infrastructures, technological amateurs, values of privacy, usability, and actual usage.

The key concept for the empirical approach is on trust valuation and needs to be defined further since it varies among research perspectives. The term trust is used here to refer to systems of normative beliefs about control and responsibility that are mainly held implicit and therefore only become visible when trust is being violated.[1] This definition also implies that trust is (re-)produced in complex interplays between collective actors,technical infrastructures, subjects, etc. and cannot be reduced to a responsibility on an individual level. Valuation on the other hand is definied as a basic social process and practice of valuating actions and thereby (de-)stabilising systems of values.[2] In contrast to the term evaluation, valuation focuses on the implicit production process of values.Taken both definitions as a whole, trust valuation can be specified as a set of social practices that constructs implicit systems of values, which are in a perpetual negotiation process within themselves and are also transferred into and (de-)stabilized as technical infrastructures.

One concept to establish trust and work against the centralization of data is to develop decentralized networks. It is important to note that even in decentralized networks a lot of issues around trust and privacy remain or are simply relocated, e.g. which serve in a decentralized network can be trusted by users. One example for a decentralized network and starting point of my research is the open standard matrix.org, which aims to provide ways to connect different chat clients in a 'privacy aware' and decentralized setting. I conducted a online ethnography of matrix.org, studying the riot client in particular. One of my first findings is the importance that valuation and therefore implicit ideas about encryption as a default setting play. These expectations are loosely structured around trusting in encrypted data and doubts about ever being able to securly protect data.

---

[1] Uhlmann, Markus; Pittroff, Fabian; Lamla, Jörn, "Vertrauensinfrastruktur der digitalen Gesellschaft. Vertrauen als Schlüsselkategorie zur Weiterentwicklung des Datenschutzes", in: Bala, Christian; Schuldzinski, Wolfgang: *Der vertrauende Verbraucher: Zwischen Regulation und Information*, Verbraucherzentrale, p. 18-42, 2019.

[2] Kropf, Jonathan; Laser, Stefan, "Eine Bewertungssoziologie des Digitalen", in: ibid.: *Digitale Bewertungspraktiken. Soziologie des Wertens und Bewertens*, Springer, p. 1-16, 2019.

The effect of the GDPR on the working environment of the Industrie 4.0

Helmut Lurtz (helmut.lurtz@uni-kassel.de)
Supervisor: Prof. Dr. Gerrit Hornung, LL.M.

The thesis's research subject is the effect of the GDPR and the national data protection legislation on employee data protection in general and especially with regards to the 'Industrie 4.0' (Industrial-IoT). The challenges in connection with new legislation on emerging technologies are assessed on the basis of seven use cases of Industrial-IoT, which are taken from a former research project (MyCPS). These use cases are related to mobile applications which are interacting with sensors, therefore posing a significant risk to the employee's privacy. New technologies and organisational methods in the 'Industrie 4.0', like BYOD and several tracking systems for various purposes, are eroding the privacy and the trust of employees. This effect is further reinforced by the employees' relationship of dependence. Not least because of this, calls for separate employee data protection legislation have become louder. Employee data protection is a special field of data protection and consists of two inseparable elements, which are influencing each other: data protection and labour law.

Therefore, the thesis consists of three parts. The first part defines the ambiguous term 'Industrie 4.0' based on theoretical and empirical findings and builds the foundation for the rest of the thesis. Only an extensive knowledge of the technical foundation enables to balance the interests of employers and employees through data protection legislation.

The second part examines labour law implications of 'Industrie 4.0' that are related to employee data protection. The employer's right to direction is reevaluated for instance with regards to directions given by robotic systems. Furthermore, intermediaries can be a highly effective method to secure privacy. With its' rights of co-determination, the working council is one of the most important intermediaries in the working environment. However, this body was established long before the advent of new technologies, making changes to the law regarding its role and competences necessary.

The third part focuses on data protection. The much discussed questions of the admissibility of the opening clause in Art. 88 GDPR and its the German implementation in § 26 BDSG is addressed. Furthermore the risk-based approach is examined and applied on data processing in the 'Industrie 4.0'. Based on this, universal criteria for the assessment data processing in the working environment are derived in form of a 'privacy-criticality-model'.

The result of this thesis is two models to facilitate employee data protection with regards to present and future data processing operations by employers. The first model strengthens privacy by intermediaries, whilst the second 'privacy-criticality-model' takes a risk-based approach. Furthermore, proposals for new employee data protection and works constitution laws are developed.

Limits of Commercial Profiling in the European Law

Dirk Müllmann (muellmann@jur.uni-frankfurt.de)
Supervisor: Prof. Dr. Spiecker gen. Döhmann, LL.M. (Georgetown)

Due to the extensive inclusion of networked technologies into our daily routines it is possible to acquire a comprehensive picture of our activities, attitudes and interests by processing usage data. Users' information, which is often very sensitive, is collected and intertwined with other personal details in profiles allowing the analysis of the collected data, the deduction of metadata and the monetarization of both.

Profiles can hold whole daily routines, movement- or activity- profiles with the result that almost every operation in the real world finds a virtual equivalent. This situation can create an enormous "surveillance pressure" under which citizens might refrain from actions deviating from those of the majority population as they fear possible negative impacts of being different. Furthermore, such algorithm-based analysis of behavior can lead to a determination of human conduct. The algorithmic method, specifically, assumes that a person doesn't change and will always act in a similar way. Based on this premise the algorithm won't recommend action alternatives which don't conform to former decisions.

The fundamental dangers of the technological advances have already been legally addressed in the 80s and have been adapted on the European level. The scientific investigation at hand aims to apply the findings of European data protection law on the technology of profiling in commercial contexts. In this regard, it attempts to reach a legal balance between economic chances of profiling and its dangers for democratic societies. Therefore, the thesis strives to answer two questions: Is there a quali- or quantitative limit for the acquisition, compilation, analysis and use of personal data in commercial profiles? And if so, is it possible to reproduce this limit in a practical system to ensure the protection of fundamental rights and to provide legal security for companies?

In order to answer these questions it is necessary to analyze the technological aspects of profiling by examining how data for profiles is collected and exploited. Moreover, the methods depicted have to be legally classified in order to gain a legal understanding and definition of 'Profiling'. Starting with the European primary legislation it has to be examined if a quali- or quantitative limit for commercial profiling exists. For this purpose, it is crucial to find out if profiling is reconsilable with the essence of the conflicting fundamental rights. As those are predominantly defence rights against the state it is, furthermore, necessary to evaluate, if they develop a 'third-party-effect' under European Law. The legal consideration of secondary European legislation will, in addition, require to assess the impact of a granted consent on the creation of profiles. Finally, it is necessary to determine basic legal, sociological and psychological aspects for a quali- and quantitative scale to indicate the legality of a profile.

Privacy Protection in Educational Internet of Things Settings

Prof. Dr. Stephanie Pieschl

The Internet of Things (IoT) - a network of sensors and devices, often supported by artificially intelligent algorithms - is becoming more relevant for educational settings. Potential long-term advantages include student-centered individualized and adaptive instruction. However, collecting detailed information about learning processes and outcomes also poses new challenges. Data about learning processes and outcomes could be collected via personal IoT technologies such as eye tracking glasses, EDA bracelets, or EEG headbands, or by outfitting smart learning spaces with built-in microphones, cameras, smart furniture, smartboards, and assistant systems. Resulting data could be used by students to self-optimize their learning, but also by instructors or organizations to evaluate learning outcomes. The potential consequences of large-scale use of such IoT technologies cannot be forseen. It might impact student motivation, salaries or foster discrimination.

So far, research in this new field of educational IoT technology has been dominated by proposing technically sophisticated ideas and pointing out ethical and legal concerns. However, a psychological perspective on cognitive and affective responses of different stakeholders (e.g., students, parents, teachers, educational leaders, and software and hardware developers) is missing. This project will investigate how stakeholders in educational settings perceive and evaluate the tension between intransparent educational IoT technologies and transparent learners, especially regarding the key variables of privacy and trust. We assume that laypersons may not fully understand complex and intransparent IoT systems, so that their judgments will not only be based on objective challenges but rather on their subjective beliefs and motives.

We will explore potentially relevant factors for trust in educational IoT settings by literature reviews and interviews with stakeholders, including IoT experts. Variables such as the age of the learners, the kind of IoT sensors, the data protection methods, or user control should emerge as relevant factors for trust and privacy evaluations. Subsequently, we will determine the comparative relevance of the most important factors via empirical studies (experiments, adaptive conjoint analyses) with fictitious but realistic educational IoT case descriptions. These results will also be used to identify trustworthy intermediaries for educational IoT settings. For example, privacy protection could be delegated to a commission for voluntary self-control of educational IoT technologies (similar to USK or FSK in Germany) or digital collectives. In all project stages, interdisciplinary cooperation within the RTG 2050 is warranted, especially with colleagues from the computer sciences (e.g., C.1) and law (e.g., C.2).

Privacy and Trust in Digital Collectives in Value-related Areas of Tension

Prof. Dr. Christian Reuter

Both state security forces and citizens use mobile Online Social Networks (OSN's) in security relevant situations such as emergencies, crises or disasters to provide, receive and analyze information. Using IT tools, the thereby evolved digital collectives can be comparatively well identified and analyzed. Research has already thoroughly evaluated those networks in empirical-analytical and engineering-oriented ways [1]. However, the inherent tension between privacy protection for users and conflicting goals, especially regarding public safety, are addressed only to a very small extent so far. While existing works mostly focus on very specific scenarios of digital collectives in emergency and crisis management, thorough consideration is sensible and crucial as privacy in the context of (life-) threatening situations is necessarily classified as a value of lower relevance. Thus, a considerable need for research remains for the key question of how privacy as well as the provision and processing of potentially personal data in security-critical situations can be guaranteed. Further, the interaction between privacy and trust is relevant regarding the cooperation of the population with state security forces and needs in-depth analyses.

The project B.4 will especially add significant research on Privacy Enhancing Technologies (PET's) and complement the graduate college with the area of specific user perspectives of digital collectives in emergency and crisis management. PET's are suitable as they resolve the area of tension between privacy and security as much as possible [2] to make data in OSN's usable, for example for emergency services in the event of a disaster. B.4 should lead to approaches that balances both the requirements of a functioning emergency and crisis management as well as the needs of users and their privacy protection while focusing on user interaction and user perspectives. Therefore, building on empirical findings, the project develops new interaction mechanisms.

In summary, goals and methods planned for project B.4 are (1) empirical evidence regarding perception of privacy and consideration of its relevance for users, (2) conception of PET's for data-driven safety-critical contexts and (3) abstraction on the development process of PET's using *Value Sensitive Design*.

---

[1] e.g. Reuter, C.; Ludwig, T.; Kaufhold, M.-A.; Pipek, V., "XHELP: Design of a Cross-Platform Social-Media Application to Support Volunteer Moderators in Disasters," *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, p. 4093-4102,2015

[2] van Blarkom, G.W.; Borking, J.J.; Olk, J.G.E., "Handbook of Privacy and Privacy-Enhancing Technologies. The case of Intelligent Software Agents," *Privacy Incorporated Software*, 2003

Privacy in user-based Bluetooth Protocols

Olga Sanina (sanina@privacy-trust.tu-darmstadt.de)
Supervisor: Prof. Dr. Marc Fischlin

The main goal of Research Area D is to develop a system, AlterEgo, that can be trusted in representing a user and his interests in digital networks. However, this is not possible without having the system being verified to be trustworthy enough by the means of identification, certification, and, if required, some others including new ways. Before deploying the infrastructure, it is important to analyse it in a theoretical sense, therefore, D2 project specifically supports Research Area D on the mathematical level.

Bluetooth is one of the PANs where AlterEgo can be used. Due to its short range for data transmission, application of Bluetooth is limited. However, developing of wearables and IoT has put Bluetooth back to be a popular solution for the need of communication between devices.

Bluetooth is being studied for a long time by researchers from different areas. Whereas some attacks and vulnerabilities of devices with Bluetooth are dependent on the manufacturers, proving security guarantees on the level of standard used as a building block to create devices is essential. For instance, Numeric Comparison pairing mode in Core Specification[1] requires involving human into authentication process to confirm digits displayed on the screens. Manufacturers hence implies this approach when designing devices with Bluetooth. In this regard, the project aims to find the answers to the following questions:

- Is key exchange in Bluetooth protocol secured? Does it provide security guarantees?
- Is authentication sufficient? Does it rely on human being involved? What consequences can lead trust-on-the-first use approach to? Does it provide authentication of parties involved into communication at all?
- How security guarantees are dependent on the modes of device pairing? Is it possible to maliciously change the mode to the one with lower guarantees? Do some modes indeed protect from man-in-the-middle attack?
- Does Bluetooth provide privacy for users? What actions can be taken to protect user's privacy from invading when user's device comes within the range of other Bluetooth device?

Since privacy is a focus of the research, it is important to understand whether Bluetooth devices may disclosure data of users and in a what way. Project implementation will allow users to make sure the Bluetooth is trustworthy and standard developers to improve it if it is applicable.

[1] Bluetooth SIG Proprietary "Bluetooth Core Specification Version 5.2," P. 3256, 2019

Towards Efficient Communication in Secure Computation

Kris Shrishak (kris.shrishak@sit.tu-darmstadt.de)
Supervisor: Prof. Dr. Michael Waidner, Dr. Haya Shulman

Secure multiparty computation (MPC) is an important tool designed to maintain user privacy during computations and transactions performed over the internet with remote parties. Concisely, MPC allows parties to perform a computation and obtain the output without revealing their inputs to the other parties. As mobile devices penetrate every aspect of our daily lives, utilizing MPC tools for mobile applications is critical for maintaining privacy of users in everyday life. Currently, mobile applications collect large amounts of personal information about users and store this information in cloud servers for the purpose of providing service to the users. Often sensitive information is also sold to third parties for profit. In addition, devices such as activity trackers are synced to mobile phones and send personal data to servers for the purpose of health monitoring and sports training. Misuse of user data, especially in the context of medical transactions, can be prevented by using MPC without blocking the functionality of the intended application. In our project, we aim to improve the efficiency of MPC both cryptographically and through non-cryptographic aspects when cryptographic protocols reach their theoretical optimal.

In the last decade, the performances of secure two-party computation (2PC) protocols based on garbled circuits have greatly improved and, thanks also to hardware support for cryptographic operations, it is now widely believed that the main bottleneck for 2PC is communication, not computation. In particular, network bandwidth is presumed to be the main hindrance. We show that the usage of network bandwidth rather than the bandwidth itself hinders the efficiency of 2PC protocols based on garbled circuits. We design and implement the first transport layer framework for secure computation. The framework supports a number of transport layer protocols, and selects a suitable one for the given computation task, depending on the circuit size of the function to be securely evaluated and network conditions. The goal of our framework is to help developers of 2PC protocol to choose, replace and use the appropriate transport layer protocol for the given application. Furthermore, we identify that evaluations of 2PC implementations do not reflect performance in real networks since they are typically performed on simulated environments and even more often on a single host. We address this issue by providing a testbed platform for evaluation of 2PC implementations in real life settings on the Internet.

Measurement and communication of users' intentions regarding privacy

Alina Stöver (stoever@privacy-trust.tu-darmstadt.de)
Supervisor: Prof. Dr. Joachim Vogt

Recent studies prove again, that people still have privacy concerns[1]. At the same time, they are confused regarding privacy policies and express a lack of control over their personal information[2]. This leads to the question: How can we support users in protecting their privacy? This question is addressed in two parts. Part I deals with the measurement of users' intentions regarding privacy, using a persona approach. Part II aims to investigate the communication of the users' intentions to a so-called privacy assistant.

If we design privacy support solutions for users, we face two issues: (1) Users differ in terms of privacy issues (e.g. privacy concerns, motivation, knowledge)[3] and (2) we can find evidence that one solution might not fit all users[4]. One approach that addresses these issues, is to cluster users into privacy personas. Already existing clustering approaches, cluster users in terms of concerns [5] or their knowledge and motivation to protect their privacy [6]. But the existing instruments that assign users to a cluster lack quality (e.g. Westins 3-item-scale shows low validity). The goal of part I is to develop an instrument (questionnaire) that meets quality criteria such as objectivity, reliability, and validity and allows to cluster people into privacy personas. Therefore first cluster criteria will be identified, second, the instrument will be developed and validated.

Part II applies the results from part I in the context of a so called privacy assistant that supports users by enforcing their privacy intentions. The idea here is to develop a prototype of a privacy assistant that uses the privacy personas and to investigate the communication of users intentions to privacy assistants.

[1] Braun, M. and Trepte, S. (2017). Privatheit und informationelle Selbstbestimmung: Trendmonitor zu den Einstellungen, Meinungen und Perspektiven der Deutschen. Stuttgart: Universität Hohenheim.

[2] Pew Research Center. (2019, December 31). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Pew Research Center: Internet, Science and Tech.

[3] Baruh, L., and Cemalcılar, Z. (2014). It is more than personal: Development and validation of a multidimensional privacy orientation scale. Personality and Individual Differences, 70, 165-170.

[4] Rudolph, M., Polst, S., and Doerr, J. (2019, March). Enabling Users to Specify Correct Privacy Requirements. In International Working Conference on Requirements Engineering: Foundation for Software Quality (pp. 39-54). Springer, Cham.

[5] Westin, A., and Harris Louis and Associates (1991). Harris-Equifax Consumer Privacy Survey. Tech. rep., Conducted for Equifax Inc. 1,255 adults of the U.S. public.

[6] Dupree, J. L., Devries, R., Berry, D. M., and Lank, E. (2016, May). Privacy personas: Clustering users via attitudes and behaviors toward security practices. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (pp. 5228-5239). ACM.

Mechanisms for Protecting Privacy in Applications

Amos Treiber (treiber@privacy-trust.tu-darmstadt.de)
Supervisor: Prof. Dr.–Ing. Thomas Schneider

Today, a broad range of mobile applications are central to our lives. Driven by the goal of personalized user experience through machine learning (ML) techniques, operators collect large quantities of individual user data. As a result, user data has become essential to digital applications. This raises the necessity to effectively protect privacy, which has been prominently addressed by legislation like the General Data Protection Regulation (GDPR).

The usage of *privacy-enhancing technologies* from applied cryptography such as secure computation (SC) has been shown to be a promising approach to preserve privacy while still allowing an application to process user data. Recently, research has been focused on making machine learning techniques privacy-preserving. However, using these techniques usually requires large-scale computations even without privacy in mind. Existing solutions with optimal leakage do not scale well and require expert knowledge for deployment, which disincentivizes privacy protection in real-world applications. While some privacy-preserving solutions gain efficiency by leaking some information, this approach leaves open the real-world impact on privacy, partly because attacks exploiting leakage have only been studied in artificial environments.

In this work, we build and evaluate mechanisms for protecting privacy, focused on large-scale applications from the domain of machine learning. Our goal is for these mechanisms to enable practical ways for effectively preserving privacy in real-world applications that can even be used by non-experts.

To achieve this, we develop methods from SC for efficient, privacy-preserving machine learning applications at large scale. Building on existing work that was solely focused on privacy-preserving neural networks and decision trees, we show how to practically protect privacy in crucial upcoming variants from machine learning. As an important use case that requires the protection of biometric information due to international standardization efforts, we demonstrate how to apply SC techniques to allow for highly efficient, privacy-preserving speaker recognition. The focus of this work lays on improving efficiency with the aim that our mechanisms can even be practically executed on devices with limited resources, such as smartphones. Our developed tools are published as open source and are targeted to be usable by non-experts.

Additionally, we examine the practical security of existing solutions. We prove the insecurity of a protocol central to a line of prior privacy-preserving ML research and show how to learn private inputs. We also provide a first understanding of the practical impact of information leakage by searchable encryption schemes, an SC mechanism for querying databases used in private ML. For this, we evaluate existing attacks in scenarios surveyed by real-world data, laying out in which use cases common leakage profiles violate privacy.

Distributed Private Analytics in Online Social Networks

Aidmar Wainakh (wainakh@tk.tu-darmstadt.de)
Supervisor: Prof. Dr. Max Mühlhäuser

Online Social Networks (OSNs) became essential means of communication in our modern society. People increasingly use the services provided by OSNs in their daily life. Currently, the dominant OSNs (e.g., Facebook and Twitter) are functioning in a centralized fashion. The service providers have full control of the user data. They collect and process the data to make revenue in several ways. Unfortunately, the providers show consistently insufficient commitment to the privacy of the users. The user data oftentimes is used without informed consent or even misused in different ways. It is disclosed to third parties (e.g., data miners companies). The data is prone to hacking activities (e.g., Facebook tokens hack 2018). In addition, some parties violate the usage policy of the OSNs and harvest the user data for suspicious purposes (e.g., Cambridge Analytica). That is, the users' privacy under the centralized OSN scheme is seriously and continuously violated.

Within the subproject B.2 of RTG 2050, we focus on enhancing the privacy aspect in OSNs by giving the users the ability to control their own data. For that, we propose the concept of hybrid OSN (HOSN), where users can still use the centralized OSNs but with additional means of privacy control. The HOSN is based on three objectives. First, providing users with techniques for distributed anonymous communication. Hence, users are able to communicate and exchange data privately and efficiently. Second, increasing the users privacy awareness by providing users with measures to quantify their privacy level. Third, putting the data access control in the hands of users. Thus, users control what data and in which accuracy is accessible by the providers.

Realizing the concept of HOSN requires to consider the financial sustainability of provider companies. The main source of these companies' revenue is the targeted advertisements. Thus, in order to keep their business model functioning, the providers need to obtain sufficient data to run advertisements. Therefore, I focus in my research on the data exchange between users and the providers, i.e., the data access control objective. Users can deliver data models to the providers instead of the raw data. These models can be built by the users collaboratively in a privacy-preserving manner. To achieve that, I investigate several methods, e.g., federated machine learning.

GRK 2193: Anpassungsintelligenz von Fabriken im dynamischen und komplexen Umfeld

Prof. Dr. Jakob Rehof
Email: jakob.rehof@cs.tu-dortmund.de
Technische Universität Dortmund
Internet: https://www.grk2193.tu-dortmund.de/

The Research Training Group "Adaption Intelligence of Factories in a Dynamic and Complex Environment" addresses highly qualified doctoral researchers of several disciplines. It offers the opportunity to conduct joint research and to compose doctoral theses about adaption planning and realisation of factory systems. In view of increasingly dynamic and intensive transformation processes within corporate environments, the ability of factories to adapt to these changes becomes increasingly necessary. In this context, the time necessary for this adaption as well as the efficiency and effectiveness involved in this process are key factors for success.

Current research programs in the field of factory planning are not characterised by an adequate consideration of multidisciplinary procedures. These, however, are indispensable in order to grasp the complexity of factories, to consider their interdependencies, and to achieve shorter reaction time and

adaption efficiency. The primary intention of the Research Training Group is to strengthen an interdisciplinary education in integrated factory planning of doctoral researchers in order to reach a higher performance of collaborative planning in practice. The Research Training group is thus set up to promote cooperation. It enables the doctoral researchers to reach their interdisciplinary research aims by considering the interfaces of research fields.

Dynamic Job Shop Scheduling Using AlphaZero

Alexandru Rinciog (rinciog@lfo.tu-dortmund.de)
Supervisor: Jun.-Prof. Dr. Ing. Anne Meyer

This work investigates the applicability of AlphaGo Zero (AZ), one of the most prominent advances in reinforcement learning (RL) today, for optimizing large scale (e.g. twenty machines and fifty jobs) dynamic Job Shop Scheduling Problems (dJSSP) with respect to tardiness. Tardiness is chosen as an optimization target given its central importance for industry today.

The well researched static JSSP (sJSSP) model fails to capture the dynamic nature of modern production systems. Jobs arrive in a continuous often stochastic fashion, where the underlying distribution is unknown. Due dates may change due to unforeseen events in the supply chain and the availability of production resources may change because of machine breakdowns, for instance. Any unforeseen change in the production setting would require the re-computation of a sJSSP solution. The dJSSP, research is mainly focused on dispatching rules and dispatching rule ensembles. Such rules are either handcrafted or automatically generated using meta-heuristics and are often domain-specific. For automatically generating dispatching rule ensembles, which was shown to outperform other approaches, rule components (features) still have to be created by hand. Thereby information loss can incur, since the production state is captured only partially through these features. Furthermore, these approaches are mostly myopic, failing to consider future production states.

AZ combines Monte Carlo Tree Search and RL thereby promising to alleviate the two aforementioned caveats. Instead of modeling rules explicitly, AZ only requires a view of the JSSP state for decision making which can be richer than encoded features. Using search together with a simulation, future system states can be taken into consideration when making a scheduling decision. In addition to this, we can train the AZ on a simulation modeling the different productions system dynamics. We thereby enable the scheduler to adapt quickly when unforeseen events occur.

The domain-agnostic nature of RL approaches coupled with the increase in computational power of today's hardware has sparked an interest for RL applications to (d)JSSPs in recent years. RL approaches can be used to schedule different variations of JSSPs without any change to the underlying algorithm's components. AZ applied to dJSSP in particular has yet to be studied. Our contribution will be threefold: First, we develop a parameterizable RL model covering different variations of JSSPs. Secondly we modify AZ to an online setting and tweak it to better suit the dJSSP. Finally we compare AZ with the state of the art and evaluate it on a real-world case study.

Component-based Synthesis of Simulation Models

Fadil Kallat (fadil.kallat@tu-dortmund.de)
Supervisor: Prof. Dr. Jakob Rehof

The planning and the adaption process of a factory comprise the draft of various concepts, which differ in processes, system structures, and control strategies. Often the result is a large number of concepts. Simulation allows to reproduce systems and processes of a Digital Factory in discrete event simulation models for examining the system behavior over time. By using simulation, the planning and adaption concepts can be evaluated regarding specific key performance indicators such as throughput time or total costs.[1]

However, executing simulation studies is a time-consuming and complex task. The modeling of a simulation model demands 30 to 35 percent of the time of a study.[2,3] Especially when multiple concepts are considered, it becomes difficult to model all off them by hand. Automatic Simulation Model Generation (ASMG) is a possible solution, but current approaches are designed for highly standardized systems and do not adapt control strategies. Moreover, the solutions can not assure that the optimal variant is generated.[1]

In this dissertation project, component-based software synthesis is used to generate a set of simulations model variants. The simulation models are not built from scratch but are composed from building blocks, which are held in a repository. The synthesis is performed by using the framework Combinatory Logic Synthesizer (CL)S, which is an implementation of an inhabitation algorithm based on combinatory logic with intersection types. Given a target type, (CL)S generates all possible variants that meet the target type.[4] Although all solutions are valid simulation models, not all of them are quite reasonable. Therefore, in addition constraint solving is used for considering domain-specific constraints to filter not proper models.

During the dissertation project the following research questions will be investigated: First, how well suited is combinatory synthesis for the domain of simulation models? Second, which components are necessary for the synthesis of manufacturing simulation models? Furthermore, how are the components typed and the coherences between the components described in a taxonomy? Third, which (manufacturing) simulation model standards are proper for generating models independent of any simulation tools? Last, how can constraint solving be integrated as a filtering technique?

[1] S. Wenzel, J. Rehof, J. Stolipin and J. Winkels, "Trends In Automatic Composition Of Structures For Simulation Models In Production And Logistics", Winter Simulation Conference, 2019

[2] W.B. Nordgreen, "Steps for proper simulation project management", Winter Simulation Conference, pp. 68-73, 1995

[3] L. Huber and S. Wenzel, "Trends und Handlungsbedarfe der Ablaufsimulation in der Automobilindustrie", Industrie Management 5, 2011

[4] J. Bessai, A. Dudenhefner, B. Düdder, M. Martens and J. Rehof, "Combinatory Logic Synthesizer", 6th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation, pp. 26–40, 2014

Autonomously organized block stacking warehouses - Major challenges and solution approaches

Jakob Pfrommer (jakob.pfrommer@tu-dortmund.de)
Supervisor: Prof. Dr. Michael Henke

Changes on the demand and supply side of companies are often accompanied by adjustments of the material flows. A type of warehouse, which is particularly suitable for continuous adaptation of storage capacities are block stacking warehouses. In block stacking warehouses unit loads are placed on the floor and stacked on top of each other. This does not require any infrastructure and therefore comes with low investment costs. Today, the efficiency of block stacking warehouses still depends on the skills of human operators. In autonomous block stacking warehouses, Automated Guided Vehicles (AGVs) carry out material handling and take over human decision-making.
In this dissertation project, as a first step, major system-inherent decisions of an autonomously organized block stacking warehouse are determined, described and mapped to existing decision problems in research. The following subproblems have been identified: the internal layout design problem, the dock assignment problem, the storage location assignment problem, the routing, and scheduling problem, the vehicle positioning problem, the unit load selection problem, and the unit load relocation problem. All subproblems are strongly interrelated. However, in literature the problems have mainly been considered separately. In a next step, we investigate state of the art in research and major challenges associated with an integrated consideration of the subproblems as well as the aligned practical requirements.

The major challenges include, first, dynamic and stochastic external influences on warehouse operations. Second, evolving product portfolios and alternating filling levels of the warehouse requires to reconsider storage strategies constantly. Third, when assigning goods to storage locations, it's also questionable whether aisles and bays should be defined as part of the internal layout design problem in advance. Internal layouts could also be the result of a sequence of storage location assignment decisions. Forth, varying internal layouts and storage locations cause frequently changing input parameters for routing decisions. Fifth, a large and exponentially growing state space makes it very challenging to look far ahead, in order to better assess current decisions. Sixth, important objetives like minimizing tardiness can only be measured after retrieving the goods from storage, which leads to the problem of delayed rewards for storage location assignment.

Given the known complexity of all subproblems, optimal methods are usually not suitable. Therefore, most promising are heuristic and learning-based approaches, which can be trained based on simulation. A solution for the described problems is developed by applying suitable learning-based methods as well as online and stochastic optimization algorithms.

Control of decentralized systems under uncertainty

Alexander Puzicha (alexander.puzicha@cs.tu-dortmund.de)
Supervisor: Prof. Dr. Peter Buchholz

Swarms of autonomous robots are used for a wide variety of missions for example during disasters or in industries. Typical tasks are the exploration of an area, the escorting of convoys, the set up of MANETs if infrastructure broke down or the transportation of objects. The autonomous control of robots is a challenging task in particular under tough environmental conditions that limit the possibilities of the robots to communicate. This implies that each robot only has a local view with limited information. Before the robot swarm can be deployed in disaster areas or on running production areas, the control software has to be tested carefully. Unfortunately, field tests are expensive and sometimes almost impossible. Thus, the only viable alternative are simulations. However, the test of software with real-time requirements has to be done in a real-time environment which puts very strict demands on the simulation software. The control software has to be part of the simulator, the dynamics of the robots has to be simulated realistically and environment conditions have to be described. The focus here is on the question how to control the agents with respect to the presented conditions and constraints. Model based control seems to be a promising starting point[1]. This leads to the question which methods and optimization strategies shall be used. Thereby sample based model predictive controller are robust against mathematical problems like unsteadiness and undifferentiability. Thus another question is how to choose the sample points. The literature presents some methods like markov random fields, Kriging, machine learning or different probability distributions. Another topic is how to model the dynamic unknown environment to cover on the one hand as much entities and influences as possible and to guarantee real time behavior on the other hand. As a result the handling of the unreliable network is important. There are two types of present related work. The first type of approaches for swarm control simplifies the environment, assumes reliable networks and uses simpler control methods with lower control quality[2]. Whereas the second type uses global optimization, which is not suitable for distributed decentralized autonomous systems and does not work in real time for complex environments[3]. Hence a real time simulation has to be implemented. This can be used to develop and verify different theoretical swarm algorithms. The results will point out how to control swarms of autonomous systems.

[1] Hämäläinen, P., J. Rajamäki und C. K. Liu (2015): „Online Control of Simulated Humanoids Using Particle Belief Propagation“. In: Proc. SIGGRAPH '15. New York, NY, USA: ACM

[2] Amiryan, J. und M. Jamzad, Hrsg. (2015): Adaptive motion planning with artificial potential fields using a prior path: 2015 3rd RSI International Conference on Robotics and Mechatronics (ICROM). Hrsg. von J. Amiryan und M. Jamzad.

[3] Strobel, A. (2016): „Verteilte nichtlineare modellprädiktive Regelung von unbemannten Luftfahrzeug-Schwärmen“. Dissertation. Darmstadt: Technische Universität Darmstadt.

Online modeling and analysis of high-dimensional data from production

Clara Scherbaum (clara.scherbaum@cs.tu-dortmund.de)
Supervisor: Prof. Dr. Peter Buchholz

The availability of inexpensive and flexible sensors and wireless communication networks means that larger amounts of data are available for production planning and control [1]. This data often needs to be analyzed in real time and is increasingly used for modeling and model-based control. Often the collected data is highly dimensional and arrives as a continuous stream. A direct complete analysis and aggregation of the incoming data often does not make sense, because important information is lost through aggregation, and is not feasible for reasons of effort. At the same time, however, complete storage of all incoming data is not possible if it is a continuous stream. Tensor-based approaches for data streams have been further developed [2]. Here, different approaches to decompose tensor structures were presented in order to achieve a compact representation of the data. However, the mentioned approaches for modeling high-dimensional data streams have not been used in production control or stochastic modeling so far. The existing approaches to model input data of stochastic models are mainly based on the adaptation of distributions and stochastic processes on the basis of an existing sample. The model parameters are estimated from the sample [3]. Most methods are only suitable for one-dimensional or dimensionally independent data. In the literature there are already approaches to estimate distribution parameters on the basis of data available in tensor structures [4].

Furthermore, offline analysis and input modeling based on individual samples is not practical. Instead, online algorithms should be used that work directly on the data stream. Within the scope of the PhD project, new online algorithms for parameter estimation for stochastic models are to be developed based on the data structures for compact storage of multidimensional data streams and on preliminary work for online parameter estimation as well as for stochastic modeling of multidimensional data [5]. The work complements previous work on the creation of simulation models by providing new models for load description and the possibility to use large amounts of data for modeling.

[1] O'Donovan, Peter; Leahy, Kevin; Bruton, Ken; O'Sullivan, Dominic T. J., "Big data in manufacturing: a systematic mapping study", Journal of Big Data 2, 2015

[2] Sun, Yiming; Guo, Yang; Luo, Charlene; Tropp, Joel, A.; Udell, Madeleine , "Low-rank Tucker approximation of a Tensor from streaming data", CoRR abs/1904.10951, 2019

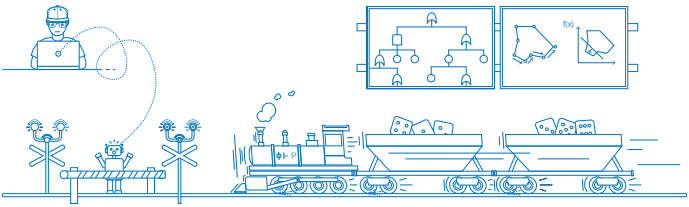
[3] Cheng, Russell , "History of input modeling", Proc. Winter Simulation Conference, 2017

[4] Rabanser, Stephan; Shchur, Oleksandr and Günnemann, Stephan, "Introduction to Tensor Decompositions and their Applications in Machine Learning", 2017

[5] Buchholz, Peter; Dohndorf, Iryna; Kriege, Jan, "An online approach to estimate parameters of phase-type distributions", Int. Conference on Dependable Systems and Networks, 2019

GRK 2236: UnRAVeL

Prof. Dr. Ir. Dr. h. c. Joost-Pieter Katoen
Email: katoen@cs.rwth-aachen.de
Rheinisch-Westfälische Technische Hochschule Aachen
Internet: www.unravel.rwth-aachen.de



Uncertainty is nowadays more and more pervasive in computer science. It is important both in big data and at the level of events and control. Applications have to treat lots of data, often from unreliable sources such as noisy sensors and untrusted web pages. Data may also be subject to continuous changes, may come in different formats, and is often incomplete. Systems have to deal with unpredictable and sometimes hostile environments. A different, also inevitable, kind of uncertainty arises from abstractions in system models focusing on the control of events. Probabilistic modelling and randomization are key techniques for dealing with uncertainty. Many trends witness this. Real-world modelling in planning is advancing by probabilistic programs describing complex Bayesian networks. In security, hostile environments are often captured by probabilistic adversaries. Probabilistic databases deal with uncertain data by associating probabilities to the possible worlds. In systems verification, probabilistic model checking has emerged as a key technique allowing for correctness checking and performance analysis. Similar developments take place in logic and game theory. The pervasiveness of uncertainty urges to make substantial enhancements in probabilistic modelling and reasoning so as to understand, reason about, and master uncertainty. The focus of the interdisciplinary RTG UNRAVEL is to significantly advance probabilistic modelling and analysis for uncertainty by developing new theories, algorithms, and tool-supported verification techniques, and to apply them to core problems from security (e.g., probabilistic protocols), planning (robotics and railway engineering), and safety and performance analysis (railway systems). To tackle

these research challenges, theoretical computer scientists from computer-aided verification, logic and games, algorithms and complexity, together with experts from management science (robust optimization), applied computer science (robotics and security), and railway engineering form the core of this RTG. The qualification and supervision concept aims at offering the Ph.D. students an optimal environment to carry out their research. Every Ph.D. student has two supervisors; the rights and duties of the supervisors and students are laid down in a written supervision agreement. The curriculum consists of bi-weekly research seminars, soft-skill courses, reading groups, annual workshops, a summer school in the first Ph.D. year, and advanced (guest) lectures.

Stable and Robust Management in Health Care Services

Martin Comis (comis@math2.rwth-aachen.de)
Supervisor: Prof. Dr. Christina Büsing

Health is one of the most important factors for the prosperity and well-being of a society. Therefore in 2005, all member states of the World Health Organization (WHO) made the commitment to ensure that everyone is granted access to health services[1]. Expenses of health services are usually covered by insurance schemes, either state-funded such as the National Health Service (NHS) in the United Kingdom or individually selected and co-financed by employer and employee, such as in the German health care system[2]. Demographic change introduces serious challenges to such systems: In Germany, for example, medical and technological progress paired with improved living conditions and reduced birth rates lead to an increased share of elderly citizens (age 65 and older) in the population which is predicted to exceed 30% of the overall population by 2034[3]. This results in an increasing demand for health services, especially due to chronical illnesses[4]. At the same time, the population share constituting the workforce is constantly decreasing[5], endangering the financial foundation of health insurance schemes. Even worse, this simultaneously reduces the availability of trained medical staff which is urgently needed since, e.g., 34.1% of all GPs in Germany were 60 years or older by the end of 2017[6] and thus about to retire. The resulting need for adjustment of health care systems is massive[7] and various new health care concepts to maintain the standard of healthcare provision are discussed by the Statutory health insurance, the German government, and the Associations of Statutory Health Insurance Physicians[8]. One of these concepts aiming at improving ambulatory care in rural areas, is the setup and promotion of mobile medical units. Combining mobile medical units with a centralized appointment scheduling for patients and a transportation system will efficiently increase the medical care in rural

[1] Dye, C., Reeder, J.C., Terry, R.F., "Research for universal health coverage", Science Translational Medicine, vol. 5, p. 199, 2013

[2] Mossialos, E., Dixon, A., Figueras, J., Kutzin, S., "Funding Health Care: Options for Europe", Open University Press, 2002

[3] Pötzsch, O., Rößger, F., "Bevölkerung Deutschlands bis 2060, 13. koordinierte Bevölkerungsvorausberechnung", Statistisches Bundesamt, 2015

[4] Grobe, T., Dörning, H., Schwartz, F., "BARMER GEK Arztreport 2011", Asgard-Verlag, 2011

[5] Pötzsch, O., Rößger, F., "Bevölkerung Deutschlands bis 2060, 13. koordinierte Bevölkerungsvorausberechnung", Statistisches Bundesamt, 2015

[6] "Statistische Informationen aus dem Bundesarztregister", Kassenärztliche Bundesvereinigung, 2017

[7] Pfaff, H., Neugebauer, E., Glaeske, G., Schrappe, M., Rothmund, M., Schwartz, W., "Lehrbuch Versorgungsforschung: Systematik - Methodik - Anwendung", Schattauer, 2017

[8] Gerlinger, T., "Gesundheitspolitik. Eine systematische Einführung", Bern: Verlag Hans Huber (mit Rolf Rosenbrock), 2014

areas. In this project we investigate how such a mobile medical care system can be implemented by investigating the following three subproblems:

- 1. the determination of the best locations of the mobile medical units,
- 2. the setup of a transportation system from the patient to the treatment location, and
- 3. the organization of a centralized appointment scheduling.

Finally, we implement a prototype agent-based simulation tool for the ambulatory health care service in rural areas. The main actors are the patients, which are characterized by their location, treatment requirement and mobility, and the general practitioners, which are characterized by their location and opening hours. This tool displays the current situation of a test region and will enable us to capture and to evaluate the effects of using optimization for the different subproblems.

Provenance Analysis for Logic and Games

Katrin Dannert (dannert@logic.rwth-aachen.de)
Supervisor: Prof. Dr. Erich Grädel

The focus of this dissertation project is to apply the concept of provenance analysis which was originally developed for database theory to logic. Provenance analysis aims at determining properties of a database query or in our case a logical formula beyond its truth value. For instance one might be interested in the number of distinct ways one could prove it or maybe we are not convinced of the truth of some input data and would like to know how sure we can be of the result. This can be achieved by interpreting queries or formulae not just as 'true' or 'false' but over a commutative semiring tailored to the additional information we are interested in. If we would like to know the number of distinct proofs, we evaluate over the natural numbers. If we would like to consider different levels of confidence, we will use the so-called Viterbi semiring. This approach has been successfully developed by Green, Karvounarakis and Tannen[1] for different types of positive database languages. When trying to define provenance analysis for logical formulae using semirings one encounters a problem however. In logic there is negation which is not obviously reproducible in the algebraic context of a semiring. There are several possibilities for treating negation with semiring operations but all have very unintuitive consequences. This unsatisfactory situation was resolved when Grädel and Tannen[2] proposed to treat negation not with a semiring operation but rather by considering the negation normal form of logical formulae and giving semiring values to the literals, not just the positive atoms. These semiring values should be compatible in the sense that the product of the value for a positive atomic formula and the value for its negation should always be zero, corresponding to their conjunction always being false, and their sum should be non-negative, corresponding to their disjunction being (some degree of) true. The values of the literals can then be extended to values for the entire formula by interpreting conjunction and universal quantification as semiring-multiplication and disjunction and existential quantification as semiring-addition. In this way it is possible to evaluate any first-order formula over any commutative semiring. By evaluating formulae over the semiring N[X] of polynomials with variables in the set X, representing the values of the literals, with coefficients in the natural numbers we obtain the most general provenance analysis possible for positive first-order logic. By this we mean that we obtain a polynomial which allows us to evaluate the formula over any semiring by substituting the semiring-values of the literals for the corresponding variables in the polynomial. This does not account for negation however and therefore only applies to positive first-order logic. To

[1] T.J. Green, G. Karvounarakis, V. Tannen, "Provenance Semirings", Proceedings of the Twenty-sixth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, p. 31-40, 2007

[2] E. Grädel, V. Tannen, "Semiring Provenance for First-Order Model Checking", 2007

account for negation and to retain the properties for the pairs of atoms and their negations described above, we have to introduce pairs of variables p,p' for atoms and their negations, respectively. If X is the set of these variables we do not consider N[X] but instead we factor out all of the terms p*p', q*q',... meaning that in the factor semiring all these products are zero. This gives us the most general semiring for all of first-order logic. The aim of this project is to develop similar notions of provenance analysis for logics other than first-order logics, for instance fixed-point logics, guarded logics and verification logics. Similarily we are considering the model-checking games for these logics in order to define a notion of provenance on these games as well as on infinite games in general. Additionally we study the properties of semiring valuations and compare them with the known results for the usual evaluation of formulae as 'true' or 'false'.

Optimization under Uncertainty

Dennis Fischer (fischer@algo.rwth-aachen.de)
Supervisor: Prof. Dr. Gerhard Woeginger

The focus of my research as a member of the UnRAVeL research training group is to study algorithms and complexity of robust optimization problems.

Traditional methods for optimization have the problem that they find solutions that are optimal for one specific scenario, but which are very susceptible to variations in the input. This is a problem because in real world optimization problems often decisions have to be made before all parameters of the instance are completely known. Real world parameters might be uncertain in the planing and optimization process and their real value only becomes apparent later. This leads to the problem of finding robust solutions that optimize the worst case performance considering all possible realizations i.e. solutions that minimize the worst possible regret.

Because of this additional quantor in the problem definition finding those solutions is usually a lot harder than the original optimization problem. They often lie in complexity classes beyond NP and are hard for those classes. I try to pinpoint the complexity of those robust optimization problems.
Another area of my research is the approximation of robust optimization problems. I either try to find algorithms that find solutions which are provably close to the optimal solution but have polynomial running time or I prove that existence of such an approximation algorithm would have complexity theoretic consequences which are generally believed to be false.

Another way of looking at robust optimization problem is as a two step process. First an agent chooses a solution and then the scenario is picked by an adversary. Other things I am interested in other than determining the difficulty of finding a strategy for the agent is finding a strategy for the adversary. Symmetrically we can ask questions about approximability of the adversary.

Robust Infrastructure

Nadine Friesen (friesen@via.rwth-aachen.de)
Supervisor: Prof. Dr. Nils Nießen

The rail infrastructure is recording high levels of capacity utilization and is already reaching its capacity limits in some cases, which could be further exacerbated in the future, in particular by the forecasted growth in European rail freight traffic. Without appropriate measures, this increase in capacity utilisation will lead to a decline in punctuality and an increased number of train path rejections. In order to meet these challenges, suitable new construction and expansion projects must be planned and a timetable must be drawn up that is as performance-optimised as possible. To achieve this, it is essential to know the capacity of the railway network. According to the current state of railway operation research, analytical capacity determinations are carried out separately for railway lines and nodes. Therefore, there is no concatenation over several lines for one (sub)network. Taking into account the relationships between the individual sub-segments, this capacity calculation could be adapted to determine the capacity for contiguous areas. This gives a more realistic picture of the capacity of networks and the relevant bottlenecks that limit the capacity can be identified. In the NeLE project, the analysis of the capacity of railway networks is to be carried out by examining connected lines using Max-Plus algebras and Petri networks. By linking these two models, it will be possible to gain more precise insights into the interrelationships within the framework of the performance analysis.

Special Online Problems with Advice

Janosch Fuchs (fuchs@algo.rwth-aachen.de)
Supervisor: Prof. Dr. Woeginger

Online algorithms compute solutions for problems without knowing the future input. The lack of information prohibits to compute optimal solutions. To measure the quality of an online algorithm the competitive ratio, e.g., the ratio between the optimal solution and the computed solution, was introduced. The best possible competitive ratios for different online problems can be used to compare the difficulty of online problems. But some problems have no constant competitive ratio, which makes a comparison impossible. Therefore, advice complexity was introduced to extend the online setting. Here, the algorithm has access to an advice tape which was written by a helpful oracle. Reading information from the tape generates costs but also provides information to help computing a solution. The number of needed bits until the computation is finished is called the advice complexity of an algorithm. It represents the amount of missing crucial information for an online problem. This parameter allows to compare different online problems by their number of needed advice bits. There are two different approaches for using the advice. The advice can be used to compute an optimal solution in an online scenario or it can be used to achieve a constant competitive ratio. In the latter case, a trade off between advice bits and the best achievable competitive ratio with advice is studied. The aim of my work is to find new lower and upper bounds for the advice complexity for graph theoretical problems, like Graph Exploration. In the graph exploration problem, an algorithm has to decide how the agent, also called explorer, moves through a network such that every point of interest is visited at least once. The best known upper bound to compute an optimal solution is n log(n) bits of advice. The idea of this approach is to enumerate the vertices in the order in which the explorer will visit them for the first time. In my thesis I show that there is an online algorithm with an advice complexity linear in the number of edges of the graph. For graphs with an outgoing degree of at most two, the advice complexity is linear in the number of vertices.

Satisfiability Checking for Optimization of Timetables in Railway

Rebecca Haehn (haehn@cs.rwth-aachen.de)
Supervisor: Prof. Dr. Erika Ábrahám

In many application areas of logic in computer science the aspect of uncertainty plays an increasingly important role. For example in planning in the railway industry the travel times of trains in shortest-path problems do not only depend on the distance, but also on external influences like weather conditions and traffic of other network users. An additional uncertainty results from unreliable railway networks, some of the edges, i.e. tracks, might even fail completely, for example due to construction work. Especially for long forecast periods the models of railway traffic include various uncertainties. Despite the uncertainty in the available data long-term decisions on the design of railway networks, train-schedules, and construction periods have to be made. These decisions are required to be robust that is to deliver (almost) optimal solutions even for uncertain input data or at least allow for efficient re-scheduling and re-routing. Inconveniently even small changes in the input data can lead to arbitrarily bad and even infeasible solutions. The aim of this project is to create an efficient system that can cope with uncertainty in railway traffic while making reliable statements about the network capacity. In conventional models of railway networks capacities are determined for individual infrastructure elements. This does neither answer how much additional traffic the infrastructure can handle in the future nor which railway expansion projects are the most useful. These questions were dealt with before by Christian Meirich in his dissertation project. His approach, however, does not take uncertainty into account, which leaves room for further investigations. The main objectives of this dissertation project in order to estimate railway network capacities under consideration of uncertainties are:

- Mathematically model railway systems under consideration of random events.
- Develop a mathematical formulation of the problem to optimize train schedules using the models mentioned above.
- Solve this optimization problem using linear programming and / or SMT solving.
- Examining the impact of the problem formulation on the running times of the optimization.

Automated run-time analysis of probabilistic programs

Marcel Hark (marcel.hark@cs.rwth-aachen.de)
Supervisor: Prof. Dr. Jürgen Giesl

Analyzing the correctness of a program has become one of the most important steps in program development. For deriving total correctness reasoning about the termination behavior of a program is crucial. Usually, termination is not the only property of interest but one would like to know bounds on the asymptotic complexity to exclude inefficient use of resources and security leaks like possible denial of service attacks. Therefore tools to infer the asymptotic runtime complexity of programs fully automatically, such as AProVE[1], have been developed and shown good results in practice. Probabilistic programs have become more and more popular over the years. While in deterministic programs the simulation of nondeterministic behavior is limited, introducing probabilistic behavior enables a more fine-grained approximation of real world systems and has shown great results in improving the efficiency of existing algorithms such as primality testing and sorting data. Nevertheless, when introducing probabilistic actions, the concept of runtime changes from ordinary functions to random processes and random variables. To ease analysis, the exact behavior of a program is approximated by its expected behavior, such as the expected runtime of a program, yielding different concepts of termination known as positive almost sure termination (expected runtime is finite) and almost sure termination (termination with probability one). Whereas these concepts coincide in deterministic systems, there are probabilistic programs terminating almost surely with infinite expected runtime[2]. Furthermore, deciding termination with respect to these concepts becomes even more involved in the sense of the arithmetic hierarchy than in the deterministic case[3], limiting the chance of techniques for inferring the exact expected runtime of a probabilistic program. However, in applications it is usually enough to know the asymptotic behavior of the expected runtime, e.g. linear, polynomial or even exponential. Thus, developing techniques for reasoning about bounds on the expected runtime is sufficient for real world scenarios. So far, the only existing fully automatic technique is presented in[4] which uses ideas similar to Dijkstra's predicate transformer but is only able to infer upper bounds. The objective of this project is to develop effective algorithms for reasoning about the different termination concepts fully automatically. Therefore, we will use the already

[1] J. Giesl et al., "Analyzing Program Termination and Complexity Automatically with AproVE", Journal of Automated Reasoning, p. 58(1), 2017

[2] O. Bournez and F.Garnier, "Proving Positive Almost-Sure Termination", Proc. of RTA, 2005

[3] B. Kaminski, J.P. Katoen, "On th Hardness of Almost Sure Termination", Proc. of the 40th International Symposium on Mathematical Foundations of Computer Science , vol. 9234 of LNCS, p. 307-318, 2015

[4] J.Hoffmann, V.C.Ngo, Q.Carbonneaux, "Bounded Expectations: Resource Analysis for Probabilistic Program", Proc. Of PLDI, 2017

existing generalization of ranking functions to the probabilistic setting, called ranking supermartingales[5] [6]. In non-probabilistic program verification it has proven itself useful to decompose the program into smaller programs and then combine the so derived partial runtime bounds with size bounds of the program variables. We will develop a concept of expected size for probabilistic systems. Existing theory on expected outcomes of probabilistic programs will be investigated. Afterwards we will focus on connecting this concept with runtime analysis in an alternating way to get a powerful fully automatic technique for the complexity analysis of probabilistic programs. Whereas a few techniques for obtaining upper bounds exist and we are working on combining and improving them, there are no algorithms for inferring lower bounds on the runtime of probabilistic programs yet. But having an upper bound is only an advantage if the upper bound already excludes inefficient effects such as memory usage or runtime. However, having an exponential upper bound is not useful because it means that the measured effect is at most very bad whereas an exponential lower runtime bound would express that a possible adversary could make the system run very long by choosing an appropriate input. So, being able to infer lower bounds is crucial for a thorough program verification. In the analysis of deterministic systems it turned out that by using only a slight modification of ranking functions called metering functions and recurrence solving good lower bounds can be achieved. Unfortunately, lower bounds for probabilistic programs are more involved than upper bounds as was proven in[7]. This is due to the fact that in probabilistic systems the expected runtime or the expected outcome can be described as the minimum of a certain set of values. For finding an upper bound it is then enough to give an upper bound for any of the values. For inferring a lower bound one has to bound every value from below. Hence, the straight forward generalization of the related deterministic concept (metering functions) is not sound for analyzing probabilistic runtimes. Therefore, we will enrich metering functions with concepts from probability theory to obtain a sound technique for inferring lower bounds. Furthermore, the processors to simplify a deterministic program, which are crucial for the performance of this approach, have to be adapted to probabilistic concepts as well to ensure a good performance of the technique on large programs. So far, only basic probabilistic programs have been considered, i.e. only the most basic datatypes (numbers ad boolean values) are used. But all favorite examples showing the gain of randomizing an algorithm contain more involved data structures, e.g. randomized quick sort uses lists. If programs with these structures have to be studied, translating them into a term rewrite system has

[5] O. Bournez and F.Garnier, "Proving Positive Almost-Sure Termination", Proc. of RTA, 2005

[6] S.Agrawal, K.Chatterjee, P. Novotný, "Lexicographic Ranking Supermartingales: An Efficient Approach to Termination of Probabilistc Programs", Proc. Of POPL, 2018

[7] B. Kaminski, J.P. Katoen, "On th Hardness of Almost Sure Termination", Proc. of the 40th International Symposium on Mathematical Foundations of Computer Science , vol. 9234 of LNCS, p. 307-318, 2015

shown good results for deterministic program analysis. Even the termination and complexity analysis of a Java program can be abstracted to the complexity analysis of a term rewrite system[8]. Basic work on probabilistic term rewriting systems has been done in[9] [10]. Still, only positive almost sure termination is considered and none of these techniques are strong enough to handle more involved term rewriting systems resulting from real world applications. The missing ingredient which has improved the analysis of classical term rewriting systems is compositionality, the possibility of combining results of separate analyses. But not all properties that are compositional in the deterministic case are also compositional when analyzing the probabilistic equivalent. For example, there exist term rewrite systems terminating in expected finite time but their composition does not. On the other hand, termination is compositional.

[8] F.Frohn, J.Giesl, "Complexity Analysis for JAVA with AproVE", Proc. Of iFM , 2017

[9] O. Bournez and F.Garnier, "Proving Positive Almost-Sure Termination", Proc. of RTA, 2005

[10] M.Avanzini, U.Dal Lago, A.Yamada, "On Probabilistic Term Rewriting", Proc. Of FLOPS, 2018

Robust Execution of Abstract Task Plans on Mobile Robots

Till Hofmann (hofmann@kbsg.rwth-aachen.de)
Supervisor: Prof. Dr. Gerhard Lakemeyer

Solving a planning problem is itself not sufficient to use a planning system on an actual robotic system. Instead, additional platform requirements need to be taken into account, the execution of the plan needs to be monitored, and abstract plans must be transformed into an action sequence that is executable on the particular robot. One of the goals of my thesis is to provide declarative platform models of robotic system components. Based on these models, we can formulate platform constraints that need to be satisfied during execution. The proposed framework transforms a given abstract task plan into an executable action sequence that takes the additional constraints into account. Additionally, the model can be used during execution to detect and recover from any component failures and unexpected changes in the environment. As foundation for this execution framework, we will provide a temporal extension of the situation calculus that allows formulating quantitative temporal constraints. The task plan and the additional constraints are then translated into a constraint satisfaction problem, whose solution is used to generate the executable action sequence. The framework will be able to execute an abstract task plan (i.e., a plan that was generated without a specific robotic system in mind) on a particular robotic system, given the system‘s platform model and constraints.

Parameter Synthesis for Markov Models

Sebastian Junges (sebastian.junges@cs.rwth-aachen.de)
Supervisor: Prof. Dr. Joost-Pieter Katoen

We consider variants of probabilistic model checking. Traditionally, model checking asks whether a given model fulfils a given specification. A model in this context describes possible system states, and the effect that an event has on the state space. A typical specification is: „A dangerous state cannot be reached“ Probabilistic model checking considers models which contain probabilistic uncertainties, where, e.g., the outcome of some action or event is given by a distribution over the state space. Typical specifications now are: „The probability of reaching a bad state is below 1%“ or „The expected time until reaching some goal is less than an hour.“

The probabilities in probabilistic models can be categorised into two groups: Often, the distributions in these models are approximations of the actual system behaviour, typically obtained by a series of experiments: the (transition) probabilities are then uncontrollable and uncertain. Or, the randomisation is an integral part of the system design, as common in randomised algorithms: the probabilities are then controllable. For both types of models, we are interested in the effect of changing parameters. Thus, we answer questions like “Do transition probabilities exist such that the probability of reaching a bad state is below 1%”, “Is the probability of reaching a bad state below 1% for all transition probabilities”, etc.

Privacy Preserving Online Algorithms

Andreas Klinger (klinger@itsec.rwth-aachen.de)
Supervisor: Prof. Dr. Ulrike Meyer

In secure multi-party computation a number of parties wants to compute a function over their inputs such that their inputs are kept private. The participating parties shall only learn their prescribed output without learning anything beyond that. The output can be either the same for all parties or each party obtains a different output. A trusted third party can be used to perform these computations. However, in some settings the parties want to keep their inputs private, e.g., if it is confidential or private information the parties are not willing to share with anyone. In order to keep the inputs private the parties avoid the trusted third party by computing the function in a distributed fashion, i.e., they jointly execute a secure protocol to simulate the trusted third party. In addition, such a protocol shall provide privacy and security in the presence of adversaries, i.e., a malicious party that wants to learn more than intended or deviates from the protocol specification arbitrarily. For the most common secure multi-party computation settings it is assumed that everything is known prior to the protocol execution, i.e., the parties know their personal input and the set of parties participating in the protocol execution is somehow known. For such a determined setting there exist already a variety of protocols for different requirements. However, there are cases where the scenario is more uncertain and might change over time. The aim of this dissertation project is to analyze these scenarios in more detail and provide a framework to define security and privacy in these settings. We will focus our research on online algorithms and develop protocols that can deal with different types of uncertainty introduced through parties joining at different times. The main research questions are: How to provide privacy and security for online matching algorithms? What are the limitations? To what degree can privacy be provided?

Robust Hospital Management

Tabea Krabs (krabs@math2.rwth-aachen.de)
Supervisor: Prof. Dr. Christina Büsing

Hospitals are under tremendous cost pressure and must achieve a balance between economic efficiency and a treatment that focuses on the patient. To improve clinical operations and patient safety, methods from economics, mathematical optimization and IT-driven management systems are imported into the operational management of hospitals. The goal is to maintain the high quality in medical care while lowering the costs. A major challenge in this optimization process is the changing demand arising from emergencies or patients without appointments, which are difficult to forecast, and thus are, in general, not integrated into the planning process. In this part of the project we will focus on the integration of such uncertainties into three main areas of hospital management:

- the capacity planning and utilization of hospital beds,
- the patient appointment scheduling, and
- the transportation from patients to their appointments.

In the next subsection we will give a rough overview of existing scientific work to the mentioned subproblems. We will finally describe our approach to these problems in detail. In 2012, Hulshof et al.[1] published a detailed bibliography and taxonomic classification on methods from operations research applied to problems in health care. Uncertainties are part of most decision problems in planning and controlling in health care. Mainly methods from queuing theory, Markov processes, and stochastic programming are used to include them into the optimization process, e.g.,[2] [3] [4] [5] [6]. Next to dealing with uncertainties, Hulshof et al.[7] identify the challenge for researchers to develop integral models

[1] P. Hulshof, N. Kortbeek, R. Boucherie, E. Hans, and P. Bakker. "Taxonomic classification of planning decisions in health care: a structured review of the state of the art in or/ms". Health Systems, 1:129 175, 2012

[2] R. Akkerman and M. Knip. Reallocation of beds to reduce waiting time for cardiac surgery. Health Care Management Science, 7:119 126, 2004

[3] M. Asaduzzaman, T.J. Chaussalet, and N.J. Robertson. A loss network model with overflow for capacity planning of a neonatal unit. Annals of Operations Research, 178:67 76, 2010

[4] S. Batun, B.T. Denton, T.R. Huschka, and A.J. Schaefer. Operating room pooling and parallel surgery processing under uncertainty. INFORMS Journal on Computing, 23:220 237, 2011.

[5] G. Dobson, H.H. Lee, and E. Pinker. A model of icu bumping. Operations Research, 58:1564 1576, 2010

[6] P.R. Harper, A.K. Shahani, J.E. Gallagher, and C. Bowie. Planning health services with explicit geographical considerations: a stochastic location-allocation approach. Omega, 33:141 152, 2005

[7] P. Hulshof, N. Kortbeek, R. Boucherie, E. Hans, and P. Bakker. "Taxonomic classification of planning decisions in health care: a structured review of the state of the art in or/ms". Health Systems, 1:129 175, 2012

of different hierarchical planning levels and services in health care. The location of beds and the assignment of patients to these beds in a hospital is studied in operations research at the strategical, tactical and operational level. To support the strategic planning queuing techniques, simulation and models from mathematical programming are already used. Traditionally these planning decisions are based on target occupancy levels. However, Green[8] points out that due to the high fluctuations different measurements as patient waiting time[9] or patient refusal rate[10] need to be integrated into the optimization process. In[11], Ma and Demeulemeester combine the allocation of beds with the appointment of elective patients. In order to integrate emergencies, they reserve a fixed capacity. The Patient-to-Bed Assignment Problem on an operational level has been formalized in 2010 by Demeester et al.[12]. They use a combination of a patient-bed-suitability rating, the number of inpatient transfers and the number of mixed-gender-occupied rooms as the objective function and propose a hybrid tabu search algorithm for this problem. Later, the problem is reformulated to patient-to-room assignment, as it is generally assumed that all beds, located in the same room, are equal. Also more practical variants and other exact and heuristic approaches for patient-to-room assignment have been published, e.g.,[13] [14] [15]. The scheduling of surgeries and the corresponding hospital's operations theater are well studied[16]. Only a limited number of papers take into account multiple resources[17]. They mainly aggregate the scheduling decisions to half-day base or limit the scheduling horizon to one

[8] L.V. Green. Capacity planning and management in hospitals. In Operations Research and Health Care: A Handbook of Methods and Applications, pages 15 41. Kluwer Academic Publishers, Boston, 2004

[9] P. Van Berkel and J. Blake. A comprehensive simulation for wait time reduction and capacity planning applied in general surgery. Health Care Management Science, 7:373 385, 2007

[10] A.K. Shahani P.R. Harper. Modelling for the planning and management of bed capacities in hospitals. Journal of the Operational Research Society, 53:11 18, 2002

[11] G. Ma and E. Demeulemeester. A multilevel integrative approach to hospital case mix and capacity planning. Computers and Operations Research, 40:2198 2207, 2013

[12] P. Demeester, W. Souffriau, P. D. Causmaecker, and G. V. Berghe. A hybrid tabu search algorithm for automatically assigning patients to beds. Artificial Intelligence in Medicine, 48(1):61 70, 2010

[13] Ceschia and A. Schaerf. Local search and lower bounds for the patient admission scheduling problem. Computers and Operations Research, 38(10):1452 1463, 2011

[14] S. Ceschia and A. Schaerf. Modeling and solving the dynamic patient admission scheduling problem under uncertainty. Artificial Intelligence in Medicine, 56(3):199 205, 2012

[15] R. M. Lusby, M. Schwierz, T. M. Range, and J. Larsen. An adaptive large neighborhood search procedure applied to the dynamic patient admission scheduling problem. Artificial Intelligence in Medicine, 74:21 31, 2016

[16] P. Hulshof, N. Kortbeek, R. Boucherie, E. Hans, and P. Bakker. "Taxonomic classification of planning decisions in health care: a structured review of the state of the art in or/ms". Health Systems, 1:129 175, 2012

[17] D. Gartner and R. Kolisch. Scheduling the hospital-wide flow of elective patients. European Journal of Operational Research, 233:689–699, 2014

week. In order to incorporate uncertainties, Vissers et al.[18] build a stochastic discrete program and solve it with a sample average approximation method. Vehicle routing problems are well-studied in discrete optimization[19]. In the context of patient routing within the hospital, Hanne et al.[20] designed a computer-based planning system. Johnson et al.[21] introduced a simulation tool, and Bedaury et al.[22] a two-phase heuristic to solve the dynamic problem. Schmid and Doerner[23] solved the combination of operating room scheduling and transportation with a hybrid metaheuristic.

So far, we have concentrated on the operational patient-to-room assignment. Hospital beds are a special resource in a hospital: according to the number of beds the capacity of a hospital is measured; the size of wards and clinics are given by this number; and the corresponding budget on medical and nursing staff is determined by this number. Yet, the number of available beds fluctuates due to capacity changes in the nursing staff, patient demands and special needs of patients[24]. These fluctuations primarily affect the scheduling of elective patients and the daily allocation of emergency patients to different wards and rooms. In case of a mismatch of available beds and admitted patients, a relocation of a bed or even of a patient to a different clinic or ward or the rejection of elective patients is possible. However, such means should only be used in extreme situations and not on a daily base. Contrary to all previously published work we do not regard a weighted combination of the patient-bed-suitability rating, the number of inpatient transfers and the number mixed-gender-occupied rooms as the objective function. Because choosing appropriate weights is very challenging and there also has no procedure yet been proposed to check afterwards if good weights have been chosen. Also, using a weighted combination prevents us from gaining better insights about how the different objectives influence each other. This is why we keep the three different aspects separated and treat them as independent objective functions. We compare and develop exact and heuristic approaches to solve the

[18] J.M.H. Vissers, I.J.B.F. Adan, and J.A. Bekkers. Patient mix optimization in tactical cardiothoracic surgery planning: a case study. Journal of Management Mathematics, 16:281 304, 2005

[19] B.L. Golden, S. Raghavan, and E.A. Wasil, editors. The Vehicle Routing Problem: Latest Advances and New Challenges. Springer, 2008

[20] T. Hanne, T. Melo, and S. Nickel. Bringing robustness to patient flow management through optimized patient transports in hospitals. Interfaces, 39:241 255, 2009

[21] K. Johnson, D. Kalowitz, J. Kellegrew, B. Kubic, J. Lim, J. Silberholz, A. Simpson, E. Sze, E. Taneja, and E. Tao. Emergency department efficiency in an academic hospital: A simulation study. PhD thesis, University of Maryland, College Park, MD, 2010

[22] A. Beaudry, G. Laporte, T. Melo, and S. Nickel. Dynamic transportation of patients in hospitals. OR spectrum, 32:77 107, 2010

[23] V. Schmid and K. Doerner. Examination and operating room scheduling including optimization of intrahospital routing. Transportation Science, 48:59 77, 2013

[24] L.V. Green. Capacity planning and management in hospitals. In Operations Research and Health Care: A Handbook of Methods and Applications, pages 15 41. Kluwer Academic Publishers, Boston, 2004

multi-objective patient-to-room assignment problem with a focus on robust solutions.

Probabilistic Databases under Open World Assumptions

Peter Lindner (lindner@cs.rwth-aachen.de)
Supervisor: Prof. Dr. Martin Grohe

Probabilistic databases (PDBs)[1] are used to store, process and to query large amounts of uncertain (probabilistic) data as may arise, for example, in information extraction, sensory data or by using machine learning methods. Probabilistic databases are modeled using the so-called possible worlds semantics. Instead of a single relational database, a PDB describes a probability distribution over a collection of traditional instances. These individual instances are called the "possible worlds" of the probabilistic database. More formally, a PDB is a probability space over sets of relational structures. Preliminary work on probabilistic databases dates back to the 80s and 90s with (among others) the seminal work of Cavallo and Pittarelli[2], of Barbará et al.[3] and of Fuhr and Röllecke[4]. The topic regained new interest in the mid-2000s with the work of Dalvi and Suciu[5] who showed a notable dichotomy result for the computational complexity of a very natural class of queries. To that point however, the concrete notions that were considered for modeling probabilistic databases mostly comprised the following two properties:

- the domain (resp. the union of all attribute domains) is of fixed, finite size; and
- the stochastic model is quite simple (using various kinds of independence assumptions).

Parallel and subsequent work proposed systems that may handle even continuous distributions (for example [6] [7]) and even introduced a continuous, formal

[1] Dan Suciu, Dan Olteanu, Christopher Ré and Christoph Koch, "Probabilistic Databases", Synthesis Lectures on Data Management, 2011

[2] Roger Cavallo, Michael Pittarelli, "The Theory of Probabilistic Databases", VLDB '87 Proceedings of the 13th International Conference on Very Large Data Bases, p. 71 - 81, 1987

[3] Daniel Barbará, Héctor García-Molina, Daryl Porter, "The Management of Probabilistic Data", IEEE Transactions on Knowledge and Data Engineering, vol. 4(5), p. 487 - 502, 1992

[4] Norbert Fuhr, Thomas Röllecke, "A Probabilistic Relational Algebra for the Integration of Information Retrieval and Database Systems", ACM Transactions on Information Systems, vol. 15(1), p. 32-66, 1997

[5] Nilesh Dalvi, Dan Suciu, "The Dichotomy of Probabilistic Inference for Unions of Conjunctive Queries", Journal of the ACM, vol. 59(6), article no. 30, 2012

[6] Ravi Jampani, Fei Xu, Mingxi Wu, Luis Leopoldo Perez, Chris Jermaine, Peter Haas, "MCDB: A Monte-Carlo Approach to Managing Uncertain Data", SIGMOD '08 Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data, p. 687-700, 2008

[7] Sarvjeet Singh, Chris Mayfield, Sagar Mittal, Sunil Prabhakar, Susanne Hambrusch, Rahul Shah, "Orion 2.0: Native Support for Uncertain Data", SIGMOD '08 Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data, p. 1239-1242, 2008

semantics for tree-databases[8]. Still, the probabilistic data herein initially follows a closed world semantics. That is, every possible database record that has no explicitly specified positive probability, is assumed to be almost surely (i. e. with probability 1) false. However, as Ceylan et al.[9] pointed out, moving towards an open world assumption is more reasonable in a lot of application scenarios. They suggest specifying a probability interval for all "unspecified" facts that can be built using the underlying domain. However, their approach is limited to finite domains and the assumption of stochastic independence of individual tuples. While this is no real restriction in a finite setting, it is unclear, whether and how their method can be extended to support infinite domains. The goal of this research project is to build and sharpen the theoretical foundations for probabilistic databases with infinite universes and rich correlations as well as explore the possibilities of performing (approximate) open-world query evaluation in such a model.

[8] Serge Abiteboul, T.-H. Hubert Chan, Evgeny Kharlamov, Werner Nutt, Pierre Senellart, "Capturing Continuous Data and Answering Aggregate Queries in Probabilistic XML", ACM Transactions on Database Systems (TODS), vol. 36(4), article no. 25, 2011

[9] İsmail İlkan Ceylan, Adnan Darwiche, Guy Van den Broeck, "Open-World Probabilistic Databases", Proceedings of the 15th International Conference on the Principles of Knowledge Representation and Reasoning, p. 339-348, 2016

Probabilistic Action Formulisms with Applications to Robotics

Daxin Liu (liu@kbsg.rwth-aachen.de)
Supervisor: Prof. Dr. Gerhard Lakemeyer

In many robot applications, an important step before deploying a robot program is to verify whether the program satisfies certain properties. There are related works consider the verification problem of robot programs under full-observations. Yet, in practice, the environment is almost never full-observable to the robot, i.e. partial observable. For instance, robot sensors are subjects to noise, physical actions are subject to uncertainty. Before considering verification, one must design a formulation to model partial-observation where noisy sensor, stochastic actions and incomplete knowledge should be incorporated. Perhaps, the most successful work in doing this is BHL's model which combine probability theorem and situation calculus by introducing beliefs to describe the robot's epistemic state. Yet, it fails to modeling incomplete knowledge, which is exactly how humans interact with environment. My work focus on modeling robot's beliefs (particularly, incomplete beliefs) and reasoning in dynamic domain. Afterward, I will explore belief programing and planning, and verifying. So far, a variant formalism of BHL has been proposed and we are investigating verification of belief programs.

Automata-theoretic techniques in probabilistic verification

Anton Pirogov (pirogov@cs.rwth-aachen.de)
Supervisor: Prof. Dr. Christof Löding

Probabilistic verification is concerned with questions as obtaining the probability for the satisfaction of certain correctness properties with respect to the behaviour of software systems. Such properties are represented in a suitable formalism (like Linear Temporal Logic (LTL)) and are verified on some abstraction (e.g. Markov chain) of the system of interest that preserves the properties in question. Linear Temporal Logic was proposed by Pnueli as a suitable language for specifications and can express many classes of useful properties[1]. A useful property of LTL is that every LTL formula can be translated into omega-automata. Omega-automata are finite-state automata that read infinite words, which turn out to be an adequate representation of traces of program executions, which in the case of reactive, non-terminating systems are infinite. The set of possible program executions can be seen as a language of infinite words and a correctness property can be seen as a description of the set of program traces that are admissible, i.e. do not violate the property. From the logical, descriptive formulation in e.g. LTL one can obtain an operational representation as a corresponding omega-automaton that accepts all words that satisfy the property and rejects the others. This allows for the reduction of verification problems to problems based on the graphs that underlie the automata and the abstraction of the system. Automata-based techniques have proven to be a successful approach for solving verification problems due to the existence of algorithmic solutions that are also feasible in practice, hence this is often the approach of choice for tackling verification tasks in various settings. Multiple acceptance mechanisms, most of which are equivalent in expressivity, are known for omega-automata. While in classical model checking a nondeterministic automaton suffices, in the probabilistic setting restrictions on the nondeterminism are necessary and the classical solution is first to obtain a nondeterministic automaton from the specification and then performing a complete determinisation of the automaton in the next step. The omega-automata obtained in the first step are usually Büchi-automata, i.e. use the Büchi acceptance condition[2] by which a word (i.e. program trace) is accepted if there exists an execution of the automaton that visits final states infinitely often. But as such automata are strictly less expressive under determinism, more powerful acceptance mechanisms must be used in the resulting automaton. A breakthrough result by Safra[3] provided the first asymptotically

[1] Amir Pnueli, "The temporal logic of programs", Proceedings of the 18th Annual Symposium on Foundations of Computer Science (FOCS), p. 46-57, 1977

[2] Büchi, J. Richard, "On a Decision Method in Restricted Second Order Arithmetic", Studies in Logic and the Foundations of Mathematics, vol. 44, p. 1-11, 1966

[3] Safra, Shmuel, "On the complexity of omega-automata", 29th Annual Symposium on Foundations of Computer Science, IEEE, 1988

optimal translation from nondeterministic Büchi to deterministic Rabin automata (which use a different definition of acceptance) and today a number of different translations with the same asymptotic bound are known. But the optimality applies only to the worst-case, while in practice often much smaller deterministic automata can be constructed. Hence, in practice, there is much room for heuristic approaches that produce small automata for specific kinds of inputs and in special cases the rather complex construction by Safra can even be avoided. This dissertation project is concerned with the improvement of automata-based techniques in the context of probabilistic verification. The first goal is the improvement of determinisation of omega-automata by development of new algorithms and heuristics that ideally should work well (i.e. produce small automata) on many practically relevant classes of inputs. The second goal is research into other known or novel automata models (and suitable restrictions of those) which can be applied for probabilistic model-checking by adapting existing or developing new techniques for this purpose. The size of the used automata, depending both on the automaton model and the algorithms that produce them, is critical for the feasibility of verification tasks, due to usually limited computational resources. Hence, results of this project will directly benefit the application of verification techniques in practice.

Analysis of Algorithms for Mathematical Optimization Problem under Uncertainty

Vipin Ravindran Vijayalakshmi (vipin.rv@oms.rwth-aachen.de)
Supervisor: Prof. Dr. Britta Peis

The advent of Industrial Revolution saw an increasing demand on road transportation network across the world. Growing population, rapid production of motor vehicles and rising demand for transfer of goods across cities, warranted well planned road networks that were favorable to efficient travel time. However, the efficacy of the road networks were thwarted by the non-cooperative nature of the users, resulting in congestion and non-optimal travel time. Thus, a comprehensive process that is conducive to at least assuage if not preclude the consequences of such user behavior was imperative.

The primary reason for congestion in road networks is due to the non-optimal distribution of traffic flow arising as a result of the selfish nature of the users. A user's rationale while traversing the network in order to reach his destination is to pick routes that have the least travel time from his current location at that point in time. Such a collective conduct by all the users of the road network resulted in a sub-optimal traffic flow along the network. One of the many approaches investigated to alleviate the aforementioned problem in the transportation network is the introduction of tolls or taxes on the roads in the network. The hope is that this persuades users into taking desirable traffic flows with respect to the network.

A transportation network can be succinctly represented using a directed graph. The nodes in the graph constitute the source and destination of the users in the road network and the edges that inter-connect the nodes represent the roads. Such a representation motivates us to investigate the problems arising in a transportation network by considering the game-theoretic aspect of the problem. Congestion games constitute an important class of games to model resource allocation by different users such as in traffic networks. In this joint work with Alexander Skopalik from the University of Twente, we study the approximation ratio of local optima in these games. However, we allow for that the cost functions used during the local search procedure may be different from the overall objective function. Our analysis exhibits an interesting method to choose these cost functions to obtain a number of different results.

As computing an exact or even approximate pure Nash equilibrium is in general PLS-complete, Caragiannis et al. [FOCS 2011] presented a polynomial-time algorithm that computes 2 + epsilon-approximate pure Nash equilibria for games with linear cost functions and further results for polynomial cost functions. We show that this factor can be further improved to 1.6+epsilon by a seemingly simple modification of their algorithm using our technique. Bilo and Vinci [EC 2016] presented an algorithm to compute load depended taxes the improve the price of anarchy (PoA) e.g. for linear game from 2.5 to 2. Their

algorithm is a centralized algorithm and is sensitive to changes of the instance such as e.g. the number of players. Our methods yield slightly weaker results, e.g., 2.012 for linear games. However, our approach is rather robust since, our tax functions are universal, locally computable and independent of the actually instance of the game. Computing an optimal allocation in congestion games is NP-hard. The best known centralized approximation algorithm is due to Makarychev and Srividenko [FOCS14]. Again, our technique does not quite match there bounds but offers a modified local search procedure as a much simpler alternative which can easily be implemented in a distributed fashion.

Our work considers optimizing a cost minimization game that represents various resource allocation problems. We define a slightly more general smoothness condition than Roughgarden and show that it is a sufficient condition to guarantee a certain approximation factor. From this condition we derive a linear program that computes a (convex) cost function for the resources to minimize the smoothness parameter. From its dual, we derive a reduction to a PoA lower bound of selfish scheduling on identical machines. This specific family of instances also implies a lower bound on the achievable approximation factor and hence, the optimality of the original LP. In case of the unweighted problem, we show that the PoA of the optimal modified game is equal to the PoA for scheduling on identical machines, implying that there is a simple local search algorithm that achieves this approximation ratio. Moreover, using approximate local search one can come arbitrarily close to that in polynomial time. For weighted, we show that the PoA with modified cost function is the PoA of the unmodified game. However, if we change the functions in a weight specific manner, we get exactly the bounds for the unweighted version of the problem. As for future work, we look at other variants such as utility maximization and shapley cost sharing games. We would also like to consider adapting our ideas to online learning techniques that converge faster to other local optimum concepts such as coarse correlated equilibrium.

Learning definable relations in Graphs

Martin Ritzert (ritzert@informatik.rwth-aachen.de)
Supervisor: Prof. Dr. Martin Grohe

We study classification problems for elements from simple structures. That is, given an element of a graph we want to estimate, whether it fulfils some property. The property is not given directly, but via the use of examples which consist of such an element from a graph structure and the correct classification. As in other machine learning scenarios from supervised learning, we assume that we can access a given amount of examples but may not ask for the correct classification of a specific node. We only consider learning algorithms, where the output is a logical formula and a number of constants called parameters. In this framework, we accept an element from the graph if and only if the underlying graph satisfies the formula $\phi(x)$. This way, every formula describes a hypothesis that is a function that estimates a given property. It is known that any hypothesis that classifies a training set correctly will also generalize well in the PAC learning model. We therefore aim at finding hypotheses that are consistent with a given training set. We work with formulas from first-order and monadic second-order logic, where the latter extends the former by allowing for additional quantification over unary relations, i.e. over sets of nodes. We also consider restrictions of first-order logic such as quantifier-free and existential or universal formulas which are formulas using only one type quantifiers, or in the quantifier-free case, no quantifiers at all. Those formulas are then evaluated over simple structures, such as strings, trees and structures of bounded degree. The goal is to design learning algorithms that run in time polynomial in the size of the training set, independently of or at least sublinear in the size of the whole data set. In case that this is not possible, we consider algorithms that first create an index structure for the underlying structure in linear (or polynomial) time and then find a consistent hypothesis in polylogarithmic time. We also consider extensions of the above learning problem, especially regarding higher-arity learning problems, where instead of positions in the graph, we instead consider tuples of the graph and try to find hypotheses based on logical formulas which are consistent with the training examples. Since we are learning to predict membership of tuples in a higher arity relation, this means that we learn new relations over the graph.

Monotonicity in parametric Markov Chains

Jip Spel (jip.spel@cs.rwth-aachen.de)
Supervisor: Prof. Dr. Joost-Pieter Katoen

In several kinds of systems probabilistic behaviour occurs. For instance unreliable or unpredictable behaviour in computer networks can be seen as probabilistic behaviour. Also, in a communication protocols, messages might not be received with a given probability, this yields a probabilistic state change. Research has been done on formal methods for the specification and verification of probabilistic systems. Questions like "what is the probability that the file is transferred correctly if messages are lost with a probability 0.05" could be analyzed through formal methods. One way to describe these probabilistic systems is through Markov chains. In a subset of these Markov chains all state changes are probabilistic and in discrete-time. However, the probabilities of these state changes are not always known in advance. Therefore, parametric Markov chains have been developed. They allow you to use parameters in the probabilities. For instance when you have a biochemical reaction network, the rates of reactions might not be exactly known. In the past, they were then estimated. However, parametric Markov chains allow you to analyse them more precisely. Also in the case of transferring a file, the probability that a message is lost might not be known in advance. Instead of estimating this probability, we can now- based on the parametric Markov chain and a requirement, for instance "the probability that the file is transferred correctly should be at least 99%" - obtain parameter values for which the requirement holds. I want to investigate the effect of changing these parameter values on the probability that a requirement holds. In particular, parameters might have a monotone effect on the probability that a given system state is reached. I want to find this monotonicity in parameters and exploit this to improve the analysis on the behaviour of systems. I started with this during my Master's thesis, in which I provided a framework to determine monotonicity based on the probabilistic program describing a system.

The Behavior of Systems with Selfish Users

Björn Tauer (tauer@algo.rwth-aachen.de)
Supervisor: Prof. Dr. Britta Peis

Due to my position at two chairs and my additional work on the Ford Alliance Project my current research is divided into several main topics, that all are related to the "Behavior of systems with selfish users" and "Social Choice" Theory. I will sketch the different topics here.

1. Competitive Packet Routing
With modern communication systems a lot of challenges rise. Consider the Internet, which is a huge network of servers and wires. An amazing amount of data is transported through this network in every second and each packet of data is allowed to freely choose a path through this network. Such a complex scenario leads to a lot of questions:

- What is a good protocol to send information through the Internet? Which rules could speed up the total performance of the network?
- How long does it take to send a packet from location A to location B?
- What is the benefit of a central authority compared to selfish users in the network? What would it cost to install such an authority? Can we decrease the total travel time without regulating the participants too much?

For dealing with this questions we combine concepts of game theory and network optimization. Game theory deals with systems in which selfish and rational agents interact with each other. While in network optimization there is the so called packet routing problem which asks for central solution that coordinates all agents in such a network. We represent the internet as a graph, servers become nodes and the wires between them become arcs. Selfish players (representing the packets) want to traverse a network as fast as possible but the capacities of some arcs are too small to handle all players simultaneously. So some of the data has to wait until it can pass this bottleneck. To analyse this kind of conflict we search for equilibria that arise from the selfish decisions of the players. We try to prove the existence of these equilibria. In case of existence, we compare the performance of such states with those that would result if a central authority optimized the paths of all participants. Due to this we can give bounds or guarantees on how bad a lack of coordination can be. Therefore we are able to classify different networks and mechanisms by their performance. Moreover, we are interested in the behaviour of different network-mechanism as well as different performance measures. So we compare utilitarian as well as egalitarian cost functions and compare the results. We also considered the question of the complexity of computing an optimal priority

list. It turns out that even for very restricted cases, i.e. for routing on a tree, the computation of an optimal priority list is APX-hard.

2. Autonomous Shuttle-Fleets for Cities

The Ford Alliance Project Autonomous Shuttle-Fleets for Cities is a cooperation between Ford Motor Company and RWTH Aachen University. Here, additionally to our chair, the Chair of Operation Research as well as the Chair and Institute of Urban and Transportation Planning are involved. This bright expertise of all participants results in a lot of synergy effects and thus several questions according to autonomous shuttles ca be answered. Such a shuttle fleet has the potential to decease traffic congestion in a city center by substituting individual traffic but simultaneously increasing the mobility of all inhabitants. Operating such a fleet causes several optimization problems in design and management. In this project, we focus on operational tasks as well as strategic tasks. One aim of this project is to develop a transport model for the region of Aachen that integrates this prospective service as an addition to public transport. A first step is to simulate the demand of this new traffic mode in each iteration of the simulation. Afterwards the simulation will perform the tasks of the shuttle fleet according to our algorithms. Afterwards the customer can evaluate the service of the fleet such that we can validate our performance and prices. So this simulation is a great tool to observe the performance of an autonomous shuttle fleet based on real data of Aachen. The conception and analysis of our heuristic approaches is still not finished yet. Moreover, I supervise different Master and Bachelor theses related to this simulation. For example we try to develop advanced dispatching algorithms, do path-calculations with energy constraints or investigate optimal reallocation strategies. On the other side we are interested in the development of pricing mechanism and auctions. For example we will analyse the impact of price reductions on ride sharing to the behaviour of the customer. Which price policy will give incentives to usage of such kind of services?

Dynamic Modelling of Traffic

Laura Vargas Koch (laura.vargas@oms.rwth-aachen.de)
Supervisor: Prof. Dr. Britta Peis

Urban population is rapidly growing worldwide and so is the number of vehicles in metropolitan areas. To get control of this rising traffic volume intelligent traffic planning is of central importance. In particular it is essential to solve many of the major traffic problems in today's cities, e.g., air and noise pollution and long travel times. In other words, a well-planned traffic does not only increase the quality of life for traffic users but also benefits the economy and environment. Improved navigation systems and the availability of massive amounts of traveling data give a huge opportunity to optimize the infrastructure for the growing demand. This draws the attention to more realistic mathematical traffic models and algorithmic approaches for the interplay of individual road users. Unfortunately, on the one hand, realistic models used in simulations are mathemati-cally poorly understood and, on the other hand, theoretically precise models that are mathematically well-analyzed are very simplified. This is where I want to contribute to with my research. In detail: in the traffic simulation programs MATSim, traffic is simulated as flow driving through a network over the time. Given the choices of all travellers, a fraction of the travellers is allowed to reroute. After some time, this converges to an equilibrium state and this is seen as the traffic situation we would get in a city. Since neither the uniqueness of such an equilibria is proven theoretically, nor the convergence of the algo-rithm, there are a lot of interesting open questions. In my work I try to answer some of them. We investigate this questions in discrete (competitive packet rout-ing) and continuous (Nash flows over time) models that take the deterministic queueing model which is used in MATSim as a basis. In these models we try to understand the structure and the quality of equilibria. Further we are also interested in network design questions which is for instance choosing good priority rules.

Logics with Multiteam Semantics

Richard Wilke (richard.wilke@rwth-aachen.de)
Supervisor: Prof. Dr. Erich Grädel

Classical logics model queries on structures such as graphs, groups, databases and so on. They are usually evaluated via so called Tarski-style semantics. That means during the evaluation process we use an assignment, that is a function mapping each free variable of the current subformula to its value, an element of the target structure. There might be multiple assignments one can use in this process, and there is no way of letting these communicate with each other, as the evaluation processes are independent of each other. In the game semantical sense one can think of such an assignment as a play in the model-checking game, that is the path taken by both players when they choose which value a variable should be assigned in order to prove that the formula is satisfied, or not, depending on the player. Classically one is only interested in the question if there exists a winning strategy for one of the players, because this shows whether the given formula is satisfied by the structure at hand. Analysing these games one can find dependencies between variables, that cannot be expressed in classical logics. For example we could find out that one player can only win if she adapts her move depending on the previous move by her opponent. As said before, a move can be thought of as selecting a value for a variable. Historically many attempts to define logics that are able to speak about dependencies between variables have been made. Such logics are sometimes called logics of imperfect information, and (besides others) originated in the work of Henkin, Enderton and Walkoe. Initially the semantics of these logics were defined in a top down manner, meaning that one cannot infer anything about the formula just from looking at its subformulae. One example is independence friendly logic (IF), proposed by Hintikka and Sandu, where quantifiers are restricted in such a way that only the knowledge about certain variables can be used to determine next value. In the model-checking game this means a player must be able to choose a value without knowing which values the other player has picked for certain variables. Another example are Henkin quantifiers, which can be interpreted as parallel classical quantifiers. It was conjectured that the semantics of these logics cannot be defined in a compositional fashion, but 1997 Hodges has disproven this informal conjecture by providing a model-theoretic semantics for IF-logic in terms of what he called trumps. Today this semantics is called team semantics and it enabled Väänänen to propose a new logic called dependence logic. The main idea is that dependencies are treated as atomic properties. Therefore one has to collect all information about the variables, resulting in a set of assignments, in contrast to the classical case. Such a set is called a team. On the atomic level we can evaluate a dependence or independence statement by looking at the team arriving at it, whence giving us a bottom up semantics. A quantifier no longer provides a single value to a variable, but rather induces a set of

values. Grädel and Väänänen introduced independence logic which interestingly corresponds precisely to the complexity class NP in terms of expressive power (over finite structures), that is existential second order logic. There have been many extensions of logics with team semantics, most of which share a single weakness: A team is viewed as a set of assignments, hence ignoring the number of occurrences of each assignment. While this is appealing in many theoretical settings, it fails to give a good description of real-world scenarios. One can easily think of examples where not only the existence, but rather the number of assignments matters, e.g. in voting. The goal of this project is to augment dependence logics with the ability to handle multiplicities. Our approach is to consider multisets instead of set of assignments, resulting in logics with multiteam semantics. These will for example be able to express statistical dependencies between data. One can also think of a multiteam as a way to incorporate uncertainty in logic, since it allows us to make statements on which portion of the (input) multiteam satisfies a certain criterion.

Automatic Verification and Complexity of Systems under Probabilistic Uncertainty

Tobias Winkler (tobias.winkler@cs.rwth-aachen.de)
Supervisor: Prof. Dr. Joost-Pieter Katoen

My research is concerned with the computational complexity (and decidability) of probabilistic systems, in particular Markovian models such as Markov chains, Markov Decision Processes and stochastic games. The prototypical question addressed by the complexity theoretical framework is "How efficient can a given (mathematical) problem be solved by a computer?" Upper bounds on complexity are generally obtained by providing an algorithm for the problem at hand. In turn, lower bounds are proved via efficient reductions – algorithms transforming one problem into another – of previously studied problems. The study of computational complexity is thus intimately linked with the study of algorithms. As an important side product, one obtains ways to reformulate new problems into ones for which there already exist efficiently implemented well-tested algorithms. Hence complexity theory can also be viewed as a study of reusing existing algorithms in an efficient manner. I am particularly interested in the following probabilistic models: Parametric Markov Decision Processes and Multi-Objective Stochastic Games. In parametric Markov models such as Markov chains or MDPs, concrete probabilities may be replaced by real variables – the parameters. Parametric models are key to analyse situations were transition probabilities are unknown but not unrelated across the whole model; or to synthesise such probabilities in a way that a certain property holds. The main theoretical and practical difficulty of these models are the global dependencies between the parameters. One of my research goals is to establish the theoretical complexity of parametric MDPs and to identify expressive tractable subclasses. I have also been working on stochastic two-person games with multiple objectives. In the context of probabilistic model checking, stochastic games are commonly used as a powerful abstraction mechanism to obtain sound bounds on quantitative properties of otherwise huge Markovian models. I have investigated complexity aspects of such games under lexicographic reachability objectives and conjunctions of thresholds on reachability properties. The aim of this dissertation project is to pursue this line of work by studying various other probabilistic models or properties from a complexity point of view.

Robust routing in railway systems

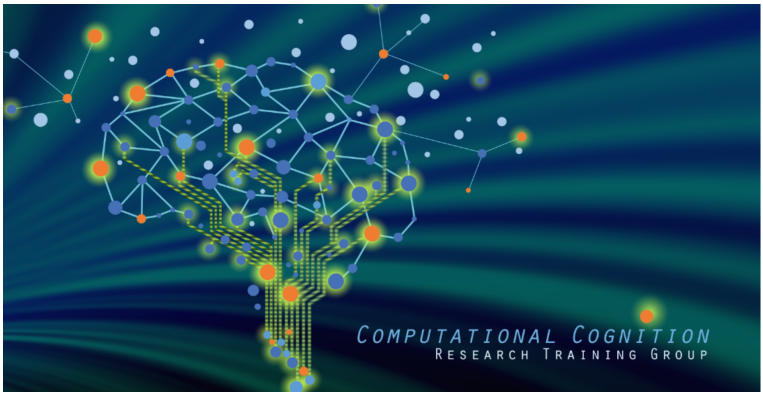
Stephan Zieger (zieger@via.rwth-aachen.de)
Supervisor: Prof. Dr. Nils Nießen

Network flow theory forms the backbone of cost- and time efficient design and analysis of routing algorithms in logistic and communication networks. Various elegant and fast combinatorial network flow algorithms exist, e.g. to maximise the amount of traffic ("flow") that can be sent through a capacitated network—even under the objective to minimise a linear cost function. However, when uncertainties in the capacities come into play, the problem to find a flow that maximises the flow value which actually reaches the sink becomes inherently complex. Already for the simple problem to find a max K-robust flow, i.e., a flow that maximises the guaranteed throughput given that K $>$ 1 arcs may fail, the complexity status is open. (One paper claimed NP-hardness for K=2. The proof, however, only shows that the dual separation is NP-hard.) Complexity results and algorithms for network flow problems under uncertainties are investigated in current research. This doctoral project aims at developing routing algorithms that are robust by minimising the amount of traffic that might be harmed by unforeseen arc failures and/or major disruptions. Developing routing algorithms that are efficient and robust towards changes in the input data belongs to one of the biggest challenges in the design of railway systems. Route- and time-schedules are computed that prescribe which type of train travels along which link of the railway-network in which time period. Certainly, there are numerous different kinds of constraints that need to be satisfied turning the corresponding optimisation problem which asks for a feasible routing protocol of minimum cost and/or time into a highly complex problem, even in the nominal setting, i.e., where there are no uncertainties on the input data. The railway network design algorithms generalise uncertainties in terms of an initial delay distribution function for each train type so far. Other uncertainties like the failure of a link or a major disruption are neglected. Additionally they ignore the temporal dimension of the problem to a large extent. Note that the trains need a certain travel time to traverse each single link of the network. As a consequence, the capacities in the network on tracks and stations limit the amount of flow/trains entering a particular link/station per time-unit. The flow models used so far for route-computations in railway systems work on so-called "static" flow models: the time horizon is split into smaller time periods, and feasible routes are computed using static flow theory for each of those periods separately. Dynamic flows take travel times into account and allow for a more realistic modelling of the underlying routing problem. Dynamic flows were introduced by Ford and Fulkerson. For railway systems, an integral version of dynamic flows, also referred to as packet routing seems to be more appropriate. The goal of this research project is to improve existing routing algorithms in railway systems by either incorporating the theory of dynamic flows and/or by incorporating

the theory of robust optimization, in particular, robust flows. By combining the theory of robust optimization and railway engineering, we are optimistic to develop various new techniques, methods, and structural insights for dynamic routing in railway operations research.

GRK 2340: Computational Cognition

Prof. Dr. Gordon Pipa
Email: gpipa@uos.de
Universität Osnabrück
Internet: www.comco.uni-osnabrueck.de



The Research Training Group in Computational Cognition pursues the re-integration of cognitive science and artificial intelligence. Students in the program will be trained in both fields and will combine insights from both fields to understand intelligence in humans and machines.

First, there is a schism between low- and high-level cognition. We understand a lot about the neural signals underlying basic sensorimotor processes, and we know a fair bit about the cognitive processes involved in reasoning, problem solving, or language. However, explaining how high-level cognition can arise from lowlevel mechanisms is a long-standing open problem in cognitive science. Machine learning has recently made great progress on deep learning methods and recurrent neural networks. At the same time, cognitive scientists have explored similar ideas, such as predictive coding for unified neural theories of learning. PhD projects in the first cluster will tackle problems, such as grammar learning, structured representations, or the production of complex behaviors with neural modeling. Thus, integrating ideas from cognitive science and AI will allow us to finally bridge the gap between low- and high-level cognition.

Second, human intelligence deals with highly structured, yet incomplete knowledge. Thus, the underlying representations and processes are able to

generate new concepts and to take into account uncertainty. Along these lines, analogical reasoning, language, pragmatic inference and concept formation have been proposed as being the key to understand human intelligence. PhD projects in the second cluster will tackle exemplary problems of these domains that are easy for humans, but still hard for AI.

Relationship Extraction using NLP and Image Content

Viviane Clay (vkakerbeck@uos.de)
Supervisor: Prof. Dr. Kai-Uwe Kühnberger, Prof. Dr. Gordon Pipa

How do humans acquire a meaningful understanding of the world with little to no supervision or semantic labels provided by the environment? I investigate embodiment with a closed loop between action and perception as one key component in this process.

Taking the example of object recognition from visual observations, a neural network will be presented with thousands of images of the object in question, each of them accompanied by a class label. A toddler in comparison will also collect many observations of the object of interest, however, will do so by interacting with the object, looking at it from different perspectives by moving the head or even moving the object[1].

This makes it possible to recognize the object as a distinct entity, separate from its surroundings and to learn a general concept of it. It allows the child to robustly recognize the object again even when seen from new perspectives or under different lighting conditions. When the toddler is now told the name of the object, an almost instantaneous association between label and object can be made without the need of thousands of labeled examples[2]. This therefore makes a very efficient strategy for learning stable representations of objects.

I try to apply this idea of embodied learning by training reinforcement learning agents in 3D virtual environments with high dimensional visual observations. This is done with little to no external supervision and learning is sometimes aided by curiosity[3]. I investigate the kind of representations of the sensory input that are learned in the embodied agents, their sparseness, similarity to representations found in animals, their semantic content, robustness, generalizability as well as their similarities to representations found in supervised neural networks.

I further hypothesize that several of the common shortcomings of conventional ANNs such as their vulnerability to adversarial attacks[4] and over-reliance on low-level features[5] originate from the unnatural way in which they are trained. My goal is to show that embodied and curiosity driven exploration of the world leads to more robust and disentangled representations of objects and can even make close to zero-shot object labeling possible.

[1] Bambach, S., Crandall, D.J., Smith, L.B., and Yu, C. (2018). Toddler-Inspired Visual Object Learning. NeurIPS.

[2] Samuelson, L.K., and Smith, L.B. (2005). They call it like they see it: spontaneous naming and attention to shape. Developmental science, 8 2, 182-98 .

[3] Pathak, D., Agrawal, P., Efros, A. A., and Darrell, T. (2017). Curiosity-driven Exploration by Self-supervised Prediction

[4] Goodfellow, I.J., Shlens, J., and Szegedy, C. (2014). Explaining and Harnessing Adversarial Examples. CoRR, abs/1412.6572.

[5] Baker N, Lu H, Erlikhman G, Kellman PJ (2018) Deep convolutional networks do not classify based on global object shape. PLoS Comput Biol 14(12): e1006613. https://doi.org/10.1371/journal.pcbi.1006613

Computational Modeling the Pragmatics of Conditionals

Britta Grusdt (britta.grusdt@uni-osnabrueck.de)
Supervisor: Prof. Dr. Michael Franke & Prof. Dr. Mingya Liu

Introduction. Despite the very long history of research on conditionals, there is no consensus and no prevalent theory that is able to explain the many and varied ways to interpret a conditional utterance. Why does the reply "and what if I don't?" to the conditional "If you want, there are biscuits on the sideboard" appear to be meant as a joke, while it seems totally normal as reply to the conditional "If you mow the lawn, I'll give you $5"?.

Modeling approach. With the aid of computational models, we aim to understand how such diverse interpretations arise for different uses of *if, then*. While most related work on conditionals has focused on qualitative models of their semantics, we investigate their pragmatics with quantitative computational models. As a basis, we use the Rational-Speech-Act (RSA) model,[1] which is a Bayesian formalization of Gricean ideas how speakers choose utterances and listeners are thereby able to infer the speakers' intentions going beyond what is literally said. Besides taking into account the interactivity of the interlocutors, we model the utterance content by explicitly representing the underlying causal structure among world states.[2]

Experimental evaluation With this approach, on the one hand, our model makes predictions for the interpretations of conditionals that align well with theoretical findings from the literature on the acceptability conditions for conditional utterances.[3] Furthermore, first preliminary data from a behavioral online experiment we performed, showed that the model is also able to generate interpretations that correlate with participants' measured intuitions. In the experiment, we exploit peoples' intuitive understanding of physics and causality in order to inject them probabilistic beliefs about world states and their structures — the basis for the predictions of our model.[4][5]

Future work. In the future, we would like to make a step towards a unified theory of peoples' use and interpretation of various sorts of conditionals. To this end, we plan to integrate other theoretical ideas into our model, e.g. how a Question-under-Discussion may lead to a biconditional reading (p *iff* q), making the inference *not p* from *not q* valid, in one context, but not in another.[6]

[1] M. C. Frank and N. D. Goodman, "Predicting pragmatic reasoning in language games", Science, vol. 336 No 6084, p.998, 2012

[2] J. Pearl, "Causality", Cambridge University Press, 2009

[3] R. van Rooij and K. Schulz, "Conditionals, Causality and Conditional Probability", Journal of Logic, Language and Information, vol.28 No 1, p. 55–71, 2019

[4] D. Lassiter, "Probabilistic language in indicative and counterfactual conditionals.", Semantics and Linguistic Theory, vol. 27, p. 525–546, 2017

[5] M. Franke, "The pragmatics of biscuit conditionals", 2007

[6] K. von Fintel, "Conditional strengthening - A Case Study in Implicature", 2000

Self-organised grammar learning with a plastic recurrent network

Sophie Lehfeldt (sophie.lehfeldt@uni-osnabrueck.de)
Supervisor: Prof. Dr. Jutta L. Mueller and Prof. Dr. Gordon Pipa

Preverbal children are equipped with a remarkable ability to detect and learn repeating temporal patterns, and thus the precursors of grammatical structures of natural languages, from the acoustic signal. However, the underlying neural mechanisms of children's grammar learning remain largely unknown. A current working hypothesis assumes that children achieve successful learning in an automatic, associative fashion[1] due to a low level of cognitive control[2] expressed at this age. In order to examine this hypothesis in more detail, it is therefore valuable to ask if state-of-the-art computational models of associative learning, such as spike-timing dependent plasticity (STDP), can reproduce experimental findings about infant grammar learning when applied to recurrent neural network models of cortex. A major goal of this PhD project is thus to train a recurrent neural network[3] to learn grammatical structures as found in natural language in a self-organised fashion. The network will be trained with artificial grammar stimuli ranging from symbolic input sequences up to subsymbolic representations of spoken grammatical samples in form of spatio-temporal spike patterns that incorporate basic neural coding schemes of acoustic stimuli in the brain. In order to learn grammars successfully, the recurrent network will perform several computations ranging from (i) learning the identity of individual linguistic elements, (ii) learning the standard structural composition of grammatical sequences by integrating stimulus identities with their temporal occurrences and (iii) detecting wrong grammatical samples by eliciting a deviant or mismatch response to the rule violating element. Further, an additional sophisticated computation would comprise (iv) a generalisation performance of trained networks in response to unknown samples of learned grammatical structures. Taken together, this PhD project will promote a deeper understanding of infant grammar learning and its underlying mechanisms at the neural level. Specifically, the performance of linguistic operations in a neurobiologically motivated modelling substrate provides a potential link for neural mechanisms and linguistic computations in the human brain.

[1] J. L. Mueller, A. Milne and C. Männel, "Non-adjacent auditory sequence learning across development and primate species," Current Opinion in Behavioral Sciences, vol. 21, p. 112-119, 2018.

[2] S. L. Thompson-Schill, M. Ramscar and E. G. Chrysikou, "Cognition without control: when a little frontal lobe goes a long way," Current Directions in Psychological Science, vol. 18(5), p. 259-263, 2009.

[3] A. Lazar, G. Pipa and J. Triesch, "SORN: a self-organizing recurrent neural network," Frontiers in Computational Neuroscience, vol. 3(23), p. 1-9, 2009.

Incorporating motion into PeriNet - a computational model for central and peripheral vision

Hristofor Lukanov (hlukanov@uni-osnabrueck.de)
Supervisor: Prof. Dr. Gordon Pipa, Prof. Dr. Peter König

The human visual system can be split into two subsystems - central and peripheral vision. Central vision is characterized by recognizing high spatial frequencies (fine details), color and shape, while peripheral vision recognizes low spatial frequencies, flicker and motion better[1]. The peripheral system serves several purposes, such as fast reaction to visual stimuli, spatial orientation and capturing the gist of a scene[2]. The vast majority of the area in the human retina contributes to it, while only a small area (fovea centralis) on the retina contributes to central vision. Despite of this fact, their representation in the human visual cortex is reciprocal. In general peripheral vision is fast and coarse, while central vision is slow and localized but accurate.

The balance of both systems is crucial for human visual capabilities and day to day life. The majority of computational models, however, largely ignore this split reported in biological studies. Convolutional Neural Networks (CNNs) are the state of the art models for image classification and object detection. They are largely used under the model of the central vision. However, with increase in the size of the processed images they become very slow and expensive to train. Typical CNNs are characterized by learning tens or hundreds of millions of parameters and require expensive hardware to train. In order to address this problem we have developed a biologically inspired computational model that accounts for the split in peripheral and central vision (PeriNet). PeriNet is an end-to-end hard-attention classification model, that is supervised on categorical labels only. It takes as input a downscaled, grayscale and blurred counterpart of the images, applies an attention model to determine the locations of interesting regions on the image and produces a small crop of the original high resolution, color image in these coordinates. This crop accounts for central vision and is then processed in the classical way to determine the categorical label of the image.

This work continues previous research on the PeriNet model in order to exploit the continuously transforming nature of the world. By accounting for motion, several saccades and fixations can be made over time, in order to improve the classification accuracy of the model and maintain stable awareness of the presented visual stimuli. The results are important for advancing our understanding of the human visual system and developing efficient, biologically plausible end-to-end computational models for vision.

[1] Strasburger, H., Rentschler, I. and Jüttner, M. "Peripheral vision and pattern recognition: A review". Journal of vision, 11(5), pp.13-13, 2011.

[2] Larson, Adam M., and Lester C. Loschky. "The contributions of central versus peripheral vision to scene gist recognition." Journal of Vision 9.10: 6-6. 2009.

From Point Clouds to Symbols in Mobile Robotics

Michael Marino (mimarino@uos.de)
Supervisor: Prof. Dr. Gunther Heidemann, Prof. Dr. Joachim Hertzberg

When you look around, what do you see? Most responses will vary to some extent based on the type of environment you currently find yourself in, but what will likely be consistent across responses (from humans particularly) is that the answer will take the form of a subset of object classes - *semantic* classes of objects as we would call them. Likely if someone responded to this question by saying "I see a 2D array of colors representing light reflected at various wavelengths spanning the continuum that is my particular instance of human vision" this would seem strange. And yet, such an answer would, in some sense, be a more objective representation of "reality"; perhaps less usefel in ways, but more objective nonetheless.

This notion of perceiving sense data in its raw form, without the addition of a "semantic" interpretation to aid in inference and communication, is what may be called a "bottom-up" view of the world, and is more closely aligned with what machine learning models do. They may encode a particular (semantic) output class as being related to a particular entry in an output vector, which is on some level semantic information. But there is a significant gap between simply mapping vector indices onto semantic classes, and the sort of complex, hierarchical model of semantic relationships at the heart of every human beings' understanding of the world, consciously or subconsciously.

If I asked you what is the relationship between a chair and a sofa, you would likely say they are both pieces of furniture, or they are both things we sit on. Attempting to ask an analogous question to a machine learning model is slightly more challenging, as one must figure out a way to connect particular instances of raw sensor data to something resembling an object class, and then come up with some meaningful way of reasoning about the connection between the two classes. This project seeks to develop methods for relating raw sensor data to semantic level relationships by developing hierarchical analysis techniques as well as ways of enforcing arbitrary hierarchies for bottom-up machine learning models. The final end goal is to use the analysis techniques and training paradigms that were developed, as well as the insights gained in the process, in order to develop robotic learning algorithms that can use feedback from a human user in order to enable robots to generalize more effectively than they could without the extra level of semantic feedback. That is, the resulting approach to learning in robotics should shift the robot's "view" of the world in a direction more readily understandable to a human user.

Learning in Pragmatic (Artificial) Agents

Xenia Ohmer (xenia.ohmer@uni-osnabrueck.de)
Supervisor: Prof. Dr. Michael Franke & Prof. Dr. Peter König

Introduction. We develop computational models of language learning and emergence in pragmatic agents. For one thing, we use these models to gain insights on the role of pragmatic reasoning in human language learning. For another thing, we try to integrate pragmatic reasoning mechanisms into artificial agents designed for language learning or communication.

Pragmatics and mutual exclusivity. Pragmatics studies how humans reason about the context and each other's intentions to enrich the literal meanings of utterances. While pragmatic reasoning is important for flexible and efficient language use it has been argued to also play an important role in early language learning[1]. Amongst others, pragmatics offers a possible explanation for an important word learning bias, the mutual exclusivity (ME) bias. The ME bias describes children's tendency to avoid assigning a second label to an object that already has a label[2]. It allows for fast language learning in humans as it helps to infer new word meanings in ambiguous contexts. Neural networks, if anything, have an anti-ME bias[3]: given a novel object they tend to assign a familiar label. Building neural networks with an ME bias is not only important for word learning but categorization in general.

A computational model of learning in pragmatic agents. So far we have developed a new computational model of *learning* in pragmatic agents. The model extends a prominent model of pragmatics, the Rational Speech Act (RSA) model[4], with a learning mechanism. Our agents learn explicit semantic representations in form of a matrix mapping words to referents. We can show that pragmatic inference influences the learning process such that they develop an ME bias. Importantly, the model's predictions align well with empirical findings on the relation between developmental change and bias strength. In short, we provide a computational account of the ME bias under a pragmatic perspective on word learning.
In future work we would like to transform our agent model into a neural network model. This allows us to: 1) investigate the model's behavior in more complex scenarios, 2) possibly integrate ME into neural networks, and 3) build on top of recent language emergence research working with rather basic forms of pragmatic reasoning[5].

[1] M. Bohn and M. C. Frank, "The pervasive role of pragmatics in early language", Annual Review of Developmental Psychology, vol. 1, p. 223-249, 2019

[2] E. M. Markman and G. F. Wachtel, "Children's use of mutual exclusivity to constrain the meanings of words", Cognitive Psychology, vol. 20 (2), p. 121–157, 1988

[3] K. Gandhi and B. M. Lake, "Mutual exclusivity as a challenge for neural networks", arXiv preprint, arXiv:1906.10197, 2019

[4] M. C. Frank and N. D. Goodman, "Predicting pragmatic reasoning in language games", Science, vol. 336 (6084), p. 998–998, 2012

[5] e.g. E. Choi, A. Lazaridou, and N. de Freitas, "Compositional obverter communication learning from raw visual input", arXiv preprint, arXiv:1804.02341, 2018

Semi-supervised Conceptors and Conceptor Logic

Georg Schroeter (georg.schroeter@uni-osnabrueck.de)
Supervisor: Prof. Dr. Kai-Uwe Kühnberger, Prof. Dr. Gordon Pipa

Conceptors were recently introduced by Herbert Jaeger[1] for the framework of reservoir computing as a mathematical formalism to access the internal representation of concepts by neural networks.

Their application includes but is not restricted to controlling dynamics of reservoirs, denoising and classification of network responses and creating smooth transitions between patterns. On top of this formalism a quasi-Boolean logic is introduced to allow combining conceptors and thus deriving conceptors representing more abstract concepts from other conceptors instead of from data observation.

In general, conceptors are a promising idea to connect the subsymbolic behavior of a dynamical system to a symbolic representation of the high-level concepts represented by the underlying dynamics both in a bottom-up approach of calculating conceptors from neural responses and a top-down approach of applying the conceptors to manipulate the dynamical system.

During this PhD project a number of research questions will be tackled:

1. In the first phase of the project the main goal is to increase the understanding of the behavior of conceptors in general and the range of possible applications. One important detail is the role of the aperture; originally introduced as an additional parameter for controlling the regularization it plays a central role in the formalism, and identifying this role more clearly will most likely help with that.

2. Of special interest is the possibility of a transfer of the conceptor formalism to more commonly used classical architectures like feedforward neural networks. This transfer would enable us to apply theoretical results to a bigger variety of solutions for real world problems and thus on one hand help in developing the formalism and on the other hand making use of analysis mechanisms for more applications.

3. Originally, conceptors are only applied to Echo State Networks (ESNs) where neither the input weights nor the internal connections in the recurrent layers are trained but instead initialized randomly, only the weights connecting to output neurons are learned. Conceptors can identify how well suited the reservoir is for a specific task from a dynamical perspective.

[1] Jaeger, H.: Controlling recurrent neural networks by conceptors. arXiv preprint arXiv:1403.3369 (2014)

Instead of using the randomly connected networks, frameworks like SORN[2] implement local learning rules to train a recurrent network unsupervised, and show that this increases the efficiency and performance of the network for the given task. We aim to combine unsupervised learning of recurrent networks with conceptors, thus making the conceptors semi-supervised.

[2] A. Lazar, G. Pipa, J. Triesch: SORN: a self-organizing recurrent neural network, Frontiers in Computational Neuroscience, Vol. 3, p. 23 (2009)

The semantics, pragmatics, and acquisition of polarity items

Juliane Schwab (jschwab@uni-osnabrueck.de)
Supervisor: Prof. Dr. Mingya Liu, Prof. Dr. Jutta L. Mueller

Polarity items in natural language are an important field of research both for theoretical linguistics and for experimental psycho- and neurolinguistics. Negative and positive polarity items (NPIs and PPIs respectively) are words or phrases that are restricted in their distribution to so-called *licensing contexts*. As they lie at the interface of syntax, semantics, and pragmatics, NPIs (and, to a lesser degree, PPIs) have attracted much attention in theoretical linguistics (see Barker (2018)[1], Giannakidou (1998)[2], Krifka (1995)[3], among many others). Neuro- and psycholinguistic investigations, too, have provided insight into NPI/PPI licensing, for instance via EEG studies investigating the processing of polarity items in licensed and unlicensed contexts (e.g. Liu et al. (2019)[4]).

Despite this rich tradition of research, most work to date (with honorable exceptions) has focused on a relatively small number of NPIs, like English *ever* and *any*. The current project therefore shifts focus to a less well-known class of polarity items: (German) degree modifiers (e.g. 'sonderlich' (NPI), 'so recht' (NPI), 'durchaus' (PPI)).

The aims of this work are three-fold: the first part of this project will provide a formal analysis of degree-modifying NPIs and PPIs. Relying on a scalar approach to polarity sensitivity, it will formalize their licensing mechanism by relating their scalar semantics and subjective meaning.

The second part of this project is directed at the cognitive mechanisms via which degree-modifying NPIs are processed. It will investigate structures wherein an NPI precedes its licensor, as this may induce expectations for the upcoming licensing context. This investigation will contribute new insight into the form and mechanisms underlying semantico-pragmatic expectations in the processing of polarity items.

Finally, the third part of this project approaches polarity sensitivity from a developmental perspective. How the licensing restrictions of polarity items are acquired across early and late childhood is as of yet unknown. Therefore, this work will use on-line methods to investigate children's comprehension of polarity items, thus contributing to our understanding of the learning mechanisms at the interface of syntax, semantics, and pragmatics.

[1] Barker, C., "Negative polarity as scope marking", *Linguistics and Philosophy, 41*, pp. 483-510, 2018

[2] Giannakidou, A., "Polarity sensitivity as (non)veridical dependency", Amsterdam/Philadelphia: John Benjamins, 1998

[3] Krifka, M.,"The semantics and pragmatics of polarity items", *Linguistic Analysis, 25*, pp. 209-257, 1995

[4] Liu, M., König, P., and Mueller, J. L. "Novel ERP Evidence for Processing Differences between Negative and Positive Polarity Items in German". *Frontiers in Psychology, 10*, p. 376, 2019

Studying task-driven situations in visually simulated contexts

Marc Vidal De Palol (mvidaldepalo@uos.de)
Supervisor: Prof. Dr. Gordon Pipa, Prof. Dr. Peter König

By the use of realistic virtual reality environments, the immersion of the subjects is considered to be favorably close when compared to naturalistic ones. In a large number of experimental studies, subjects report two essential components when the immersion happens. On the one hand, the place illusion or sensation of being in a real place. On the other, the illusion that the scenario shown is actually occurring. When both components are noticed, participants tend to react realistically to the VR simulations[1].
Also, the broad possibilities, flexibility and well-controlled experimental habitat that VR technologies offer, immensely facilitate and favor the study of close-to-naturalistic situations in the lab[2].
It is known that humans' location selection in a scene is driven by the stimuli (bottom-up) and by context-dependant (top-down) factors as, for instance, the given task[3]. And these can be precisely defined, manipulated and time-controlled in simulated environments, allowing researchers to study their influence on visual perception dependant aspects such as attention and memory, for example.
In this project, research comparing the influence of the task within the same context is studied. To achieve that, car rides in a full-featured and realistic simulated city are used aiming to get more insights about how and what drives visual attention in humans.
Subjects' gaze points and brain electrophysiological activity is recorded using eye-tracking and EEG methodologies during the experimental tasks. With the analysis of the acquired data, the classification of relevant versus non-relevant targeted visual stimuli combined with their preceding event-related potentials are investigated in order to better understand the involved underlying cognitive processes.

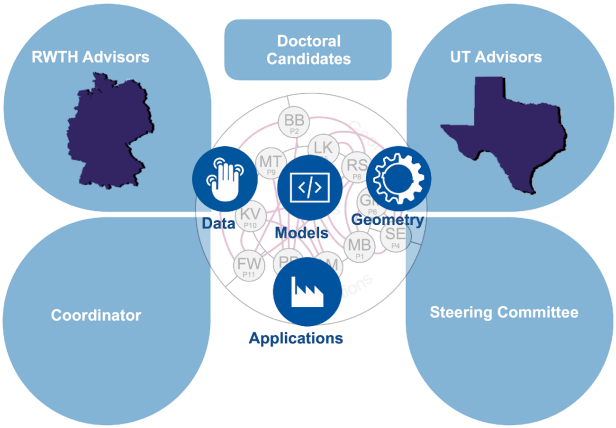
[1] Slater, M. "Place illusion and plausibility can lead to realistic behaviour in immersive virtual environments", Philosophical Transactions of the Royal Society B: Biological Sciences, vol. 364(1535), p. 3549-3557, 2009

[2] Nezami Farbod N., Wächter Maximilian A., Pipa Gordon, König Peter "Project Westdrive: Unity City With Self-Driving Cars and Pedestrians for Virtual Reality Studies", Frontiers in ICT, vol. 7, p. 1, 2020

[3] Jansen, L., Onat, S., König, P. "Influence of disparity on fixation and saccades in free viewing of natural scenes", Journal of Vision, vol. 9(1):29, p. 1-19, 2009

GRK 2379: Modern Inverse Problems: From Geometry and Data to Models and Applications

Ph.D. Prof. Marek Behr
Email: behr@cats.rwth-aachen.de
RWTH Aachen University
Internet: http://www.irtg-mip.rwth-aachen.de/



Computational methods permeate every aspect of engineering and science, from analysis to discovery and optimization. Their evolution continues at a rapid pace, driven not only by ever faster computing hardware, but also by our growing understanding of the true potential of computer-aided methods. Practical simulations transition from single numerical experiments towards robust predictive tools; models of isolated phenomena evolve into model hierarchies representing complex systems; numerical methods expand to deal with sensitivities with respect to parameters, uncertainties in those parameters and in models themselves. The educational system on all levels must keep up with and foster these advances; it is our objective to establish the required framework for doctoral training. The International Research Training Group builds on a unique and complementary consortium, at RWTH Aachen University with its Aachen Institute of Advanced Study in Computational Engineering Science (AICES), and at the University of Texas at Austin with its Institute for Computational Engineering and Sciences (ICES). The projects are embedded in the field of modern inverse problems and introduce a new innovative

perspective into the education of future scientists and engineers. They focusing on the challenges that arise in the interaction of the four specific themes: geometry, data, models, and applications. Within each theme, the expertise at one institution is significantly augmented by that of the other partner. The International Research Training Group provide a worldwide-unique environment for doctoral training in the field of computational engineering. This training group unites experts in Aachen and Austin, providing unparalleled critical mass in computational engineering. Extensive experience with doctoral training on both sides of the partnership are perfected. A joint research training with the right combination of structure and individuality, a tailored academic program of courses and colloquia, and a common supervision concept make this transatlantic cooperation a success and a blueprint for future collaborations.

Boundary Conforming Smooth Spline Spaces for Isogeometric Analysis

Janis Born (born@cs.rwth-aachen.de)
Supervisor: Prof. Dr. Leif Kobbelt

Methods in computer-aided design, mechanical numerical simulation, or geometric optimization use different representations of geometry. Conversion between these representations can be a challenging task, especially when going from polygon meshes (as used in geometry processing or finite-element analysis) to smooth spline representations (as used in CAD or isogeometric analysis). The difficulty lies in determining a suitable base domain for the spline surface and its embedding into the original mesh. Even if we assume a certain domain structure as given, the embedding still has continuous (geometric) and discrete (topological) degrees of freedom.

We study the topological optimization of domain embeddings with regard to embedding quality. We can judge the quality of an embedding for example by the parametric distortion of the embedded domain faces or by measuring the approximation error of a spline surface fitted to the original geometry.

We investigate two alternative approaches: The first is to build an embedding from scratch by successively adding domain elements (vertices, edges, faces) to a partial embedding. By eliminating some of the continuous degrees of freedom (e.g., choosing fixed vertex positions, embedding domain edges as geodesics, etc.), we can pose the embedding optimization as a purely combinatorial problem which can be approached by a branch-and-bound algorithm.

The second approach is to incrementally modify a given full embedding using topological modifications that improve its quality. One candidate for a basic operator is the Dehn twist: This operation cuts a cyclic strip from the embedding surface, twists it by a full cycle along one boundary, and reinserts it. Here, the challenge lies in finding sequences of Dehn twist (and associated twist cycles) that lead to a quality improvement.

For both approaches, a suitable representation of (partial) embeddings is essential. The straightforward approach of embedding domain edges in the 1-skeleton of the underlying polygon mesh gives a simple explicit representation of an embedding. Unfortunately, it requires frequent mesh refinement to accommodate some configurations. Hence, finding a representation that encodes only the topological type of the domain embedding while allowing to easily extract an explicit geometric embedding is another key task.

Computational tools for chemical imaging

Jan-Christopher Cohrs (cohrs@aices.rwth-aachen.de)
Supervisor: Prof. Dr. Benjamin Berkels

The term *chemical imaging* describes digital image acquisition techniques that record at each position of the image domain a spectrum with a very high spectral resolution. In contrast to the typical image types like, e.g., RGB images that are sampled from the regime of visible light with a low spectral resolution, chemical imaging records a full spectral band of data in a broad wavelength interval and yields a very high amount of information about the captured scenery. The resulting images are called *hyperspectral images*. One encounters them, for instance, in remote sensing taken with an airborne visible/infrared imaging spectrometer (AVIRIS) or in medical imaging as Fourier-transform infrared spectroscopy (FTIR) images. The price one has to pay for the high spectral resolution is the huge size and high dimensionality of the data, which is one of the major challenges in the processing of hyperspectral images.

A first goal of our IRTG project is the segmentation of hyperspectral images. *Image segmentation* describes the task of partitioning the image domain into meaningful homogeneous regions, based on a suitable notion of spectral homogeneity. Mathematically, a segment label is assigned to every pixel in the image based on its corresponding spectrum. A main difference to clustering algorithms is that segmentation methods also take into account the spatial relations between the pixels. In this project, segmentation is planned to be done using a Mumford-Shah (MS) type functional. Segmentation techniques are applied for example in cancer treatment where FTIR images showing a human tissue sample shall be partitioned into the segments (or classes) “highly cancerous”, “mildly cancerous” and “normal”.

A second goal of the project is the so-called *unmixing* of hyperspectral images. Unmixing takes a more general perspective on the problem of segmentation. Here, every pixel is considered to be a mixture of a predefined number of different classes instead of belonging to exactly one class (or segment). This is usually modeled with a linear mixing model. The objective is to unmix this mixture by determining the mixing ratio and mathematical representations of its constituents. As an example, one can consider human tissue to be a mixture of different cell types that are the classes represented by unique fingerprint spectra and every pixel to show a mixture of different cell types. An important class of algorithms to tackle unmixing is nonnegative matrix factorization (NMF).

A challenge one has to deal with when doing hyperspectral segmentation or unmixing is the so-called *high intra-class variation*. It describes the phenomenon that pixels belonging to the same class show a non-negligible variation in their recorded spectra. The so-called indicator function in the MS functional is used to evaluate how well a pixel fits into a certain segment and forms one of the main building blocks of the functional. Consequently, the first idea is

to design new indicator functions for the MS functional that can handle this variability since problem-adopted indicator functions are crucial for the success of image segmentation via the MS functional. To make the new indicator functions robust against the intra-class variation, an estimation of the underlying distribution of the spectra can be used. One of the important questions to answer is which models for the distribution are suitable. As a starting point, we use training data to determine and consider the first principal modes of variation and the corresponding variances to obtain an estimation of the distribution.

In the case of hyperspectral unmixing, a way to control the intra-class variation is to consider the problem as an unmixing of mixture of mixtures. For example, one could view the tissue as a mixture of cell types, which are considered as a mixture of fixed molecule types. This approach allows for a higher order (possibly nonlinear) approximation and may enable to find better local minima.

Machine-Learning-Based Performance Modelling

Aravind Sankaran (aravind.sankaran@rwth-aachen.de)
Supervisor: Prof. Paolo Bientinesi, Ph.D.

The efficient computation of mathematical expressions is critical not only for complex simulations but also for solving problems in real-time on resource-constrained hardware. For instance, the resilience of a flying drone to atmospheric conditions depends on the amount of gradients per second that the on-board processor can compute. In practice, mathematical expressions such as the gradient are translated into code through compilers. Typically, one expression can be computed in many alternative ways, which although equivalent from a mathematical perspective, differ in terms of performance. The objective of this research is to aid compilers in selecting a fast implementation by using performance models and machine learning techniques.

Common performance models, like those obtained by accumulating the number of arithmetic operations(FLOPs), are not always direct indicators of the fastest code; almost all high-level languages for matrix computations (e.g., Matlab, Eigen) that map computations internally to optimized kernels such as those provided by BLAS and LAPACK, find programs that are suboptimal in terms of performance [1]. Moreover, the prediction of performance based on FLOPs or memory-stalls, not only requires a deep understanding of the processor architecture but also a detailed analysis of kernel implementations [2] [3], which are not always available. Also, in a program consisting of a sequence of kernel calls, due to cache effects, models of individual calls cannot be directly combined to predict the performance of the whole program[4] [5].

In this research, we do not assume any knowledge of the computing architecture and kernels but treat them as black boxes. We do not attempt to directly predict the execution time of the code but focus on the comparison and ranking of equivalent programs. Machine-Learning techniques are used to model the causal factors from individual kernel arguments and combine them using call sequence information to facilitate comparisons. The performance model will first be evaluated by ranking the multi-threaded versions of automatically generated programs by Linnea[6] and then be expanded to include sparse data operations and heterogeneous architectures.

[1] C. Psarras, H. Barthels and P. Bientinesi, "The Linear Algebra Mapping Problem", arXiv:1912.12924, Nov 2019

[2] R. Iakymchuk and P. Bientinesi, "Modelling performance through memory-stalls", ACM SIGMETRICS Performance Evaluation Review 40(2), Oct 2012

[3] R. Iakymchuk and P. Bientinesi, "Execution-Less Performance Modelling", PMBS11, DOI: 10.1145/2088457.2088465, Nov 2011

[4] E. Peise and P. Bientinesi, "A Study on the Influence of Caching: Sequences of Dense Linear Algebra Kernels", VECPAR 2014, LNCS 8969, Apr 2015

[5] E. Peise and P. Bientinesi, "Performance modelling for Dense Linear Algebra", PMBS12, DOI: 10.1109/SC.Companion.2012.60, Nov 2012

[6] H. Barthels, C. Psarras and P. Bientinesi, "Linnea: Automatic Generation of Efficient Linear Algebra Programs", arXiv:1911.09421, Dec 2019

Automating linear algebra code development, without sacrificing performance

Christos Psarras (psarras@aices.rwth-aachen.de)
Supervisor: Prof. Paolo Bientinesi, Ph.D.

An increasing number of scientists from a variety of fields including robotics, computational chemistry and biology rely on languages such as Matlab, Julia and Eigen. These languages enable users to express their computational problems in a notation that closely resembles their mathematical form, while attempting to deliver high performance. In the early stages of this project, we performed an investigation[1] on how these languages translate user's high-level linear algebra inputs to code. To this end, we designed benchmarks to test both standard compiler optimizations such as common subexpression elimination and loop-invariant code motion, as well as linear algebra specific optimizations, such as optimal parenthesization for a matrix product and kernel selection for matrices with properties. Our results showed that while few optimizations are performed, most of them are not considered, often leading to substantially suboptimal code. Ultimately, the aim of this study is twofold: On the one hand, we introduce the Linear Algebra Mapping Problem (LAMP), which is the problem of mapping a linear algebra expression to a set of fundamental function calls (kernels) while minimizing a cost function. On the other hand, we give concrete guidelines for the development of languages and libraries that support linear algebra computations.

Following up on this investigation, we implemented several of the proposed guidelines in Linnea[2], a linear algebra compiler aimed at solving a subset of LAMPs. Linnea accepts as input linear algebra expressions in a high-level notation which includes operand sizes and properties such as triangular, symmetric etc. Then, it symbolically rewrites the input expressions, while using pattern matching[3] to identify parts which can be computed by one or more BLAS/LAPACK kernels. Finally, a graph is created containing many different sequences of kernels that compute the input expression. As output, Linnea produces the sequence which minimizes the number of floating point operations (FLOPs).

Tests performed with real and artificial datasets indicate that Linnea's generated code outperforms popular languages and libraries[4]. However, there are still opportunities to improve the decision making mechanism. For instance, since FLOPs alone do not characterize well the execution time of parallel

[1] C. Psarras et al., "The Linear Algebra Mapping Problem", arXiv: 1911.09421, 2019

[2] H. Barthels et al., "Automatic Generation of Efficient Linear Algebra Programs", arXiv: 1907.02778, 2019

[3] M. Krebber et al., "MatchPy: A Pattern Matching Library", In *Proceedings of the 16th Python in Science Conference*, Ed. by K. Huff et al., pp. 73-80, 2017

[4] H. Barthels et al., "Linnea: Automatic Generation of Efficient Linear Algebra Programs", arXiv: 1912.12924, 2019

executions, machine-learning-based performance prediction is currently under development.

Furthermore Linnea, like most other high level languages and libraries, supports shared memory parallelism through multi-threaded BLAS/LAPACK kernels[4]. While results show that this method is generally effective, it is only one possible solution for parallelism; alternatives include the "by blocks"[5] methodology, as well as OpenMP concurrent tasks. Further research is required to determine how different parallelization schemes affect performance across a diverse set of applications.

[5] E. Chan et al., "SuperMatrix: A Multithreaded Runtime Scheduling System for Algorithms-by-blocks", In *Proceedings of the ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming, PPOPP*, pp. 123-132, Jan. 2008

GRK 2475: Cybercrime and Forensic Computing

Prof. Dr.-Ing. Felix Freiling
Email: felix.freiling@fau.de
Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)
Internet: https://cybercrime.fau.de

Information technology has caused a new form of crime to emerge: cybercrime. It is incurring an increasing cost on modern society and is arguably threatening the stability of our economic system. Traditional law enforcement approaches appear to struggle with this new development. However, with new technologies also come new forms of criminal investigation, like large-scale data analysis and police trojans for covert surveillance. The effectiveness of such methods routinely raises questions regarding their impact on the constitutional rights of affected citizens. The inherent bounds of national law complicate matters further.

This Research Training Group aims to disentangle the many open ends of this research area arising from the interaction between computer science and criminal law by bringing together established scientists from both areas. Computer science is represented through the areas of cryptography (Dominique Schröder), theoretical computer science (Lutz Schröder, Stefan Milius), multimedia security (Christian Riess), hardware-software-co-design (Jürgen Teich, Stefan Wildermann) and computer security (Felix Freiling). Colleagues from law represent criminal law (Hans Kudlich), criminal procedural law (Christoph Safferling) and criminology (Gabriele Kett-Straub). Our goal is to slowly but systematically work towards establishing new methodological standards in handling digital evidence, intepreting and developing national and international law in the years to come. At the same time, we attempt to (at least partially) remedy the lack of scientifically trained experts in this area.

The individual research and training programme of funded researchers is undertaken in cooperation with an interdisciplinary advisory committee and supported by a joint lecture series, a research seminar and interaction with international guests. During the annual cybercrime workshop, funded researchers interact by solving selected cybercrime cases involving forensic analysis of digital evidence and its presentation in front of an expert panel consisting of computer security professionals, public prosecutors and judges.

Coalgebraic Automata and Learning Algorithms and their Application in Forensics

Hans-Peter Deifel (hans-peter.deifel@fau.de)
Supervisor: Prof. Dr. Stefan Milius

The study of dynamic systems has a long and rich history in computer science, spanning fields such as classical automata theory, concurrency theory, and IT security. Such systems include deterministic automata, (labeled) transition systems, and probabilistic systems. Historically, algorithms developed for one type of system had to be adapted or reinvented for another one. In contrast, the theory of universal coalgebra aims to provide a generic framework for systems that encompasses the instances mentioned above and many others.

The use of coalgebraic techniques has recently facilitated the development of a generic partition refinement algorithm, which we implemented in a tool that can efficiently minimize a wide array of state based systems. In fact, for many of the studied system types, the generic algorithm matches the run-time complexity of the best known specialized algorithm and for some system types even surpasses it. Genericity is achieved by varying the type functor, but the base category is assumed to be Set in the concrete algorithm.

In this thesis we will, as a first step, add support for data automata to this algorithm, by porting it to another base category. Data automata deal with infinite alphabets that are accessible only by a limited API. They arise e.g. when dealing with user data in XML processing. A natural base category for these structures is a suitable category of nominal sets, whose use in computer science goes back to Gabbay and Pitts. They provide an elegant theory for infinite structures that exhibit certain symmetries. We will therefore extend our algorithm and tool to be able to deal with systems over nominal state sets.

Another class of algorithms that has recently seen the introduction of coalgebraic techniques is active automata learning, which allows to infer automata models by querying a black-box system. E.g. Angluin's original learning algorithm reconstructs a deterministic finite automaton by posting a series of questions to an adequate *teacher*. Since this pioneering work, similar learning algorithms have been developed for a variety of different systems, motivating the search for a generic method. Advances in this direction were made in the last few years using coalgebraic methods by Silva et al. with their Coalgebraic Automata Learning Framework (CALF) and recently, by Barlocco et al. The newest development is an algebraic approach by Schröder and Urbat. All of these approaches still have various shortcomings, in particular, they do not yield a concrete ready-to-use generic algorithm. So the search for such an algorithm continues. In this thesis, we will investigate the applicability of those approaches and hope to devise a readily implementable algorithm with a high level of genericitry.

As a case study, we will apply active learning techniques in the field of digital forensics, e.g. by constructing accurate models of black-box systems in digital evidence.

Cryptocurrency Anonymity

Dominic Deuber (dominic.deuber@fau.de)
Supervisor: Prof. Dr. Dominique Schröder

Cryptocurrencies are digital means of payments that are based on the blockchain technology and cryptographic primitives such as digital signatures. In contrast to traditional currencies, cryptocurrencies do neither require a central bank to issue new units nor a central point to monitor transactions. These unique properties are the reason why cryptocurrencies increasingly change how payments are made worldwide.

In most cryptocurrencies, transactions use public keys as part of a digital signature scheme to specify senders and recipients of the payments. A person can generate an arbitrary number of public keys on the fly and the keys themselves do not reveal the identity of the person. Therefore cryptocurrencies working like this are often mistakenly considered anonymous. However, multiple public keys belonging to the same person can be grouped by linking heuristics.[1] For this reason, such cryptocurrencies only achieve pseudonymity and are thus non-privacy-preserving. However, two main techniques have been developed to realize anonymity. On the one hand, there are so-called *overlays*[2] that can be used on top of non-privacy-preserving cryptocurrencies to add anonymity by complicating linkage. On the other hand, there are privacy-preserving cryptocurrencies aiming for anonymity by design. The three largest privacy-preserving cryptocurrencies by market capitalization are Monero, Zcash, and Dash. While the privacy measures of Monero and Zcash have been extensively studied,[3] Dash has not yet been subject to analyses. Therefore the first part of my work is to understand and formalize Dash.

Cryptocurrencies, especially the aforementioned Monero, Zcash and Dash are more and more used by criminals[4] and thus gain the attention of law enforcement agencies. While the results of deanonymization attacks might be sufficient to start investigations, it is not yet clear what their meaning in a criminal trial might be. The reason is that deanonymization attacks are based on heuristics and thus might lead to false positives. This may raise problems given the standard of evidence required to find a defendant guilty. Thus, the second part of my work is to study how results based on those heuristics can be used in criminal procedures, especially how they should be interpreted.

---

[1] D. Ron and A. Shamir. Quantitative analysis of the full Bitcoin transaction graph. In *FC 2013*, pages 6–24, 2013. S. Meiklejohn et al. A fistful of Bitcoins: characterizing payments among men with no names. In *Internet Measurement Conference*, pages 127–140, 2013.

[2] S. Meiklejohn and C. Orlandi. Privacy-enhancing overlays in bitcoin. In *FC 2015 Workshops*, pages 127–141, 2015.

[3] M. Möser et al. An empirical analysis of traceability in the Monero blockchain. *PoPETs*, 2018(3):143–163, 2018. G. Kappos et al. An empirical analysis of anonymity in Zcash. In *USENIX Security 2018*, pages 463–477, 2018.

[4] G. Tziakouris. Cryptocurrencies——a forensic challenge or opportunity for law enforcement? An Interpol perspective. *IEEE Security and Privacy*, 16(4):92–94, 2018.

Viktimologie Cybercrime

Julia Drafz (julia.drafz@fau.de)
Supervisor: Prof. Dr. Gabriele Kett-Straub

Die Digitalisierung schreitet in unserer Gesellschaft immer weiter voran und bringt neue Technologien hervor. Nach der JIM-Studie 2019 des Medienpädagogischen Forschungsverbunds Südwest ist von einer flächendeckenden Vollausstattung sowohl mit dem Internet als auch Smartphone in den deutschen Haushalten auszugehen. Das Internet ist somit nicht mehr aus dem Berufsleben und privaten Alltag wegzudenken. Doch die technischen Errungenschaften gehen jedoch nicht nur mit positiven Aspekten einher, da auch Kriminelle das Potential des Internets zum Missbrauch für ihre eigenen Zwecke entdeckt haben. Während das Schadensausmaß enorm ist, ist das Aufdeckungsrisiko aufgrund der Anonymität des Internets und fortschreitenden technischen Entwicklungen gering. Im Gegensatz zu anderen Kriminalitätsbereichen steht die Forschung im Gebiet der Internetkriminalität noch am Anfang. Insbesondere in der (Cyber-)Viktimologie, einem Teilbereich der Kriminologie, das sich mit verschiedenen Facetten der Kriminalitätsopfer beschäftigt, bestehen Forschungsdesiderate.

Bisherige Studien beliefen sich bisher relativ erfolglos auf die ausschließliche Verwendung von quantitativen Methoden zur Identifizierung von Risikofaktoren bei Opfern von Cyberkriminalität in der allgemeinen Bevölkerung. Im Rahmen der Dissertation steht neben der Aufarbeitung des aktuellen Stand der Opferforschung die Durchführung einer eigenen empirischen Studie im Vordergrund, die darauf abzielt, die Opfererfahrungen im Internet von Student*innen am Campus Erlangen-Nürnberg zu erfassen. Mithilfe eines standardisierten Fragebogens sollen Daten für die statistische Analyse gewonnen und gleichzeitig Studierende mit Opfererfahrungen identifiziert werden, um im Anschluss mit ausgewählten Proband*innen qualitative Interviews durchzuführen. Diese kombinierte Vorgehensweise schafft zum einen die Möglichkeit, statistische Kennwerte einer bestimmten Zielgruppe zu erhalten und zum anderen mithilfe einer qualitativen Inhaltsanalyse nach Mayring nähere Erkenntnisse über Cybercrime-Opfer zu generieren.

Graded Monads and Graded Logics: A Formal Approach to Digital Fingerprinting

Chase Ford (chase.ford@fau.de)
Supervisor: Prof. Dr. Lutz Schröder

This thesis explores formal approaches to digital fingerprinting by modelling user-machine interactions as concurrent systems. To this end, we explore topics arising at the interface of universal (co)algebra, logic, and automata theory, motivated by their rôle in the analysis and verification of such systems: while logical languages and automata work to specify properties of systems, coalgebras[1] serve as a suitable level of generality for the uniform analysis of a variety of system types (e.g. automata and transition systems). In particular, we propose a user-as-coalgebra approach to the digital fingerprinting problem and explore logical, algebraic, and automata-theoretic approaches to distinguishing user behaviour from some (possibly artificial) yardstick behaviour.

Another dimension in the analysis of concurrent systems arises in the variety of notions of process equivalence; we advocate a notion of digitial fingerprint which is flexible in notions of process equivalence situated along the linear time-branching time spectrum[2]. In recent work, a framework based on graded monads was introduced which, for a fixed Set-based coalgebra type T and notion of process equivalence $\equiv$ (induced by a graded monad on Set and subject to minor assumptions), induces a logic over T-coalgebras which is characteristic for $\equiv$ (i.e. $\equiv$-expressive and $\equiv$-invariant)[3]. Motivated by these observations, we explore the possibility of using (chains or directed systems of) graded monads to solve the digital fingerprinting problem.

First, we elaborate on the theory of graded monads, graded theories, and graded algebras over the category Pos of partially ordered sets and monotone functions and show how graded semantics induced by graded monads on Pos give rise to logics which are characteristic for simulation-like equivalences. Next, we will contribute to the learning problem for coalgebras under graded semantics by developing the theory of minimal coalgebras under graded semantics. An interesting further line of research lies in the characterization of graded logics as a class of automata.

[1] J. Rutten, "Universal coalgebra: A theory of systems," *Theor. Comput. Sci.*, p. 249:3–80, 2000

[2] R. van Glabeek, "The linear time–branching time spectrum I; the semantics of concrete sequential processes," J Bergstra, A. Ponse, and S. Smolka, editors, *Handbook of Process Algebra*, p. 3-99, 2001

[3] S. Milius, D. Pattinson, and Lutz Schröder, "Generic trace semantics and graded monads," *Proceedings of the* 6^{th} *Conference on Algebra and Coalgebra in Computer Science* (CALCO 2015), p. 253–269, 2015

Reliable Models for Authenticating Multimedia Content as Forensic Evidence

Benedikt Lorch (benedikt.lorch@fau.de)
Supervisor: Dr. Christian Riess

Criminal investigations often need to handle photo and video recordings that may serve as forensic trace or be probative in a legal setting. Such recordings are found on a seized device or hard disk, or on social media platforms. In most cases, little is known about the origin of the recording, such as its processing history or the camera that captured it. To validate the authenticity and to identify the source of the recording, researchers have developed a broad set of tools, which can be categorized into model-based and learning-based techniques.

Model-based techniques aim to characterize traces of image formation by constructing an analytical model of properties of natural images. Deviations from the model indicate tampering. Many model-based forensic methods, however, are designed for very specific problems and thus are based on restrictive assumptions that limit the applicability of these methods in practice. When no prior knowledge about the image under analysis is available, it is far from clear whether or not that image satisfies the model assumptions, and which forensic methods can safely be employed on that image, leading to arbitrary results.

While rigorous analytic evaluation of the evidence is certainly preferable, many traces are notoriously hard to describe and isolate, given the lack of knowledge about hardware manufacturing and the abundance of possible processing operations that an image may have undergone. When analytical derivations are infeasible, researchers try to estimate those underlying patterns by learning a statistical model from large sets of examples. Due to the unknown origin of the image under analysis, however, it is not trivial to know what training data is representative for the specific task. When the training data is not representative, machine learning models can produce arbitrary predictions.

For use in criminal investigations, forensic methods must meet high requirements for precision and reliability. We argue that the typical lack of knowledge about the exact circumstances of a recording limit the practical applicability of model-based and learning-based approaches. The goal of this thesis is to create reliable forensic techniques by exploring two directions. First, we aim to develop analytical methods to validate whether an image meets the assumptions of model-based approaches. Second, we aim to equip learning-based models with ways to express predictive uncertainty in a Bayesian framework by explicitly modeling its full posterior distribution. Such a framework can then be used to assess the reliability of the method and to anticipate potential failure cases.

Die strafprozessualen Ermittlungs- und Eingriffsmaßnahmen im Lichte der Cyberkriminalität: Grenzen der Anwendung bestehender Normen und Reformvorschläge

Florian Nicolai (florian.nicolai@fau.de)
Supervisor: Prof. Dr. Hans Kudlich

Cyberkriminalität nimmt stetig zu. Im Lichte dieser Entwicklung sind die im Rahmen der Strafprozessordnung (StPO) geregelten Eingriffsbefugnisse der Ermittlungsbehörden überarbeitungs- und reformbedürftig. Bereits bei einem Rückblick auf die letzten zwei Jahrzehnte kann festgestellt werden, dass die StPO zwar stellenweise mit Blick auf neue technische Entwicklungen reformiert worden ist, dass ihre bisherigen Regelungen aber an verschiedenen Stellen nicht hinreichend auf die Verfolgung von Cyberkriminalität ausgerichtet sind.

Die vorhandenen Eingriffsbefugnisse sind sowohl in rechtsdogmatischer Hinsicht als auch unter praktischen Gesichtspunkten nicht auf dem neuesten Stand. Zwar werden — teils unter Billigung höchstrichterlicher Rechtsprechung — bestehende Normen (analog) auf neue, die IT betreffende Sachverhalte angewandt. Jedoch bestehen hiergegen zum Teil (schwerwiegende) rechtsdogmatische Einwände. Damit einher gehen Probleme bei der Rechtsanwendung, insbesondere bei den Ermittlungsbehörden, für die die Unsicherheiten über den Anwendungsbereich der Ermittlungsmaßnahmen im Alltag der Strafverfolgung Schwierigkeiten bereiten. Ferner steht zu befürchten, dass mit weiterem Fortschreiten der Technik die existierenden Normen den neuen Anforderungen, denen sich Staatsanwaltschaft und Polizeibehörden ausgesetzt sehen, nicht gerecht werden. Um Lösungsansätze für die genannten Probleme zu entwickeln, wird die Arbeit sich zunächst mit den grundsätzlichen Anforderungen an solche, für die Gewinnung digitaler Beweise nötigen, Ermittlungsbefugnisse auseinandersetzen. Sodann werden einzelne, ausgewählte Aspekte gesondert betrachtet und mögliche Lösungen, insbes. auch Vorschläge zur Um- oder Neugestaltung entsprechender Normen, erarbeitet.

Beispielhaft genannt sei die Betrachtung des weiten Feldes des „Internet of Things“. In diesem Zusammenhang ist nicht nur von Interesse, inwiefern Daten aus diesem Bereich überhaupt für einen Strafprozess von Relevanz sein können. Vielmehr ist auch begutachtungswürdig, auf welche Weise diese Daten gerichtsfest und für den Strafprozess verwertbar gewonnen werden können.

Diese Betrachtungen können nur unter enger Bezugnahme auf technische Neuerungen und Grundverständnis der technischen Aspekte erfolgen. Unerlässlich ist ebenfalls eine dezidierte Auseinandersetzung mit den technischen Möglichkeiten, auf Grundlage derer den Ermittlungsbehörden neue Befugnisse und Ermittlungsmethoden an die Hand zu geben sind. Es gilt, die Schwierigkeit zu meistern, die dabei besteht, eine möglichst für neue Technik offene Regelungen zu schaffen und diese dennoch hinreichend bestimmt in ihrer Anwendbarkeit zu gestalten.

Understanding Privacy in Cryptocurrencies

Viktoria Ronge (vikoria.ronge@fau.de)
Supervisor: Prof. Dr. Dominique Schröder

Cryptocurrencies are digital currencies normally not issued by a government or other central authority relying on cryptographic tools. They enable users to transfer money all over the world in a secure way, where there is no need for intermediaries like banks or exchange the money into different currency. Thereby, no user can be prevented from transferring money, no one can spend money they do not own or spend it twice and money can only be created under rules everyone agrees to. They further provide different nuances of privacy, where somewhat fully private ones are rare. The largest two are Monero[1] and Zcash[2]. They pursue different approaches, which are, with our current knowledge about privacy, at least partly incomparable.

This research project focusses on the foundations of anonymous cryptocurrencies from different angles. One is to understand the theory behind different anonymous cryptocurrencies and to formalize them. This is necessary as without formalizing no security can be proven and no statements about actual privacy for users can be done. Another one is to extend our knowledge and comprehension of different anonymity measures and to use them for comparison of currencies. This would help us to answer simple questions like which currency offers better anonymity, but this research is also important from a legal perspective, because anonymous cryptocurrencies often are used by criminals. Understanding privacy of different systems might lead to ideas on how to attack a system. This raises the fundamental question if this is proportional in relation to the violation of privacy of honest users. Moreover, when using results from such attacks in prosecution, we need an understanding of the results' quality. For genetic tests we know well about the accuracy based on past experiences. For deanonymising we are lacking such a ground truth that exists in other areas used for evidence. Therefore it is urgent to gain confidence in the accuracy of deanonymisation to make sure no innocent is falsely accused.

We hope to help giving an overview of these issues to provide the community with a better understanding of what privacy means in this subfield and how reliable we can talk about it. A first step was already done in formalizing Monero as a whole[3]. We further currently work on a better understanding of choosing anonymity sets for Monero.

[1] The Monero Project, https://www.getmonero.org/, last visited March, 27^{th}, 2020

[2] Electric Coin Company, https://z.cash/, last visited March, 27^{th}, 2020

[3] *Omniring: Scaling Private Payments Without Trusted Setup*, R. W. F. Lai and V. Ronge and T. Ruffing and D. Schröder and S. A. K. Thyagarajan and J. Wang, *Proceedings of the 2019 ACM SIGSAC CCS 2019*

Digitale Daten als Beweismittel im Strafverfahren

Dr. Christian Rückert (christian.rueckert@fau.de)
Supervisor: Prof. Dr. Christoph Safferling

Durch die Durchdringung der Arbeitswelt und des Privatlebens durch Computertechnik und das Internet werden in zunehmendem Maße Daten über Aktivitäten, Beziehungen und Bewegungen von Personen erzeugt und gespeichert. Die erzeugten und gespeicherten Daten sind auch für das Strafverfahren interessant und relevant. Dies gilt nicht nur für den Bereich des sog. Cybercrime, sondern für alle Deliktsbereiche.

Das deutsche Strafverfahrensrecht bzw. die Auslegung seiner Normen ist derzeit nicht an die sich schnell entwickelnde IT-Technologie angepasst. Das Habilitationsvorhaben adressiert dabei die beiden aus Sicht des Verfassers dringlichsten Problemkreise.

Zunächst stellt sich im Bereich der Datenerhebung im Ermittlungsverfahren das Problem, dass die Regulierung von Eingriffsgrundlagen zur Datenerhebung nicht mit der technischen Entwicklung Schritt halten kann. Dies führt dazu, dass der Gesetzgeber in den letzten Jahren eine Vielzahl von einzelnen Eingriffsgrundlagen für jeweils spezifische Technologien geschaffen hat. Diese Eingriffsgrundlagen sind häufig eng zugeschnitten und lassen sich wegen des Vorbehalts des Gesetzes nicht auf die Anwendung neuer Technologien übertragen. Dennoch werden die Grenzen spezieller Eingriffsbefugnisse überschritten oder es werden neue Eingriffsgrundlagen unter Verstoß gegen den Vorbehalt des Gesetzes und die Wesentlichkeitstheorie des BVerfG durch Kombination verschiedener bestehender Befugnisnormen geschaffen.

Das Habilitationsprojekt möchte diese Problemstellung adressieren, indem aus höherrangigen Normen (Grundgesetz, Europäisches Recht, Völkerrecht) allgemeine Leitlinien zur Auslegung bestehender und Schaffung neuer Eingriffsbefugnisse entwickelt werden. Als Ergebnis sollen Vorschläge zur technikneutralen Reform der Befugnisnormen für Datenerhebungen auf Grundlage der notwendigen Schutzmechanismen in Abhängigkeit von der Eingriffsintensität unterbreitet werden.

Der zweite Problemkreis betrifft die Würdigung von digitalen Daten als Beweismittel in der Hauptverhandlung. Hier geht es vor allem um die Schaffung und Bewahrung eines möglichst großen Beweiswerts. Da Daten flüchtig und leicht manipulierbar sind, müssen Regeln zur Sicherung der Authentizität und Integrität in das Beweisrecht der StPO intergriert werden. Weiterhin stellt sich das Problem, dass das Tatgericht die Daten nicht selbst auswerten kann. Die Richterinnen und Richter müssen sich daher auf die Auswertung durch IT-Forensiker/innen verlassen. Hierfür muss es daher einheitliche Regeln hinsichtlich Methodik und Qualifikation der herangezogenen Sachverständigen geben. Das Vorhaben entwickelt diese Regeln sowohl aus dem Stand der Wissenschaft und Technik der IT-Forensik als durch Auslegung der Normen des Beweisrechts der StPO.

„Der IT-Sachverständige“ — Heuristik und Beweiswürdigung

Nicole Scheler (nicole.scheler@fau.de)
Supervisor: Prof. Dr. Christoph Safferling

Nicht nur viele unserer Lebensinhalte spielen sich nunmehr digital ab, auch die Beweismittel haben längst die analoge Welt verlassen („eEvidence“). Durch die Allgegenwärtigkeit der Informationstechnik in unserem Alltag (Smartphones, Laptops, Wearables, Navigationsgeräte, Sprachassistenten, etc.), können anhand der dabei entstehenden Daten umfassende Persönlichkeits- und Aktivitätsprofile erstellt und digitale Abbilder gespeichert werden. Diese Daten können umfangreiche Spuren enthalten, die auf Sachverhalte aus der körperlichen Welt schließen lassen und menschliches Verhalten nachweisbar machen. Sie zu finden, zu sichern und gerichtsverwertbar auszuwerten ist Gegenstand der IT-Forensik. Diese digitalen Spuren müssen als gerichtsfestes Beweismittel in die Hauptverhandlung eines Strafverfahrens eingeführt werden. Neben den Herausforderungen der Massendatenauswertung, der Heterogenität von Daten sowie der Verschlüsselung der Kommunikation und von Festplatten, stellt sich u.a. auch der „Übersetzungsvorgang“ von digitalen Beweismitteln durch IT-Sachverständige für die anderen Prozessbeteiligten vor Gericht als problematisch dar. Die Gerichte können in vielen Verfahren nicht mehr auf die Hilfe von IT-Sachverständigen verzichten. Aufgrund der steigenden Komplexität informationstechnischer Systeme ist hierfür — neben der reinen Übersetzungstätigkeit in eine menschenlesbare Form durch Software — in zunehmendem Maße auch eine tiefgehende Erläuterung der Ergebnisse von Datenverarbeitungsvorgängen durch menschliche IT-Forensik-Expertinnen und Experten notwendig. Bei mangelnder Kompetenz der Gerichte im Bereich der IT-Forensik besteht die ernstzunehmende Gefahr, dass nicht mehr die Richter (allein) über Schuld oder Unschuld befinden (§261 StPO), sondern die IT-Sachverständigen in weiten Teilen das Ergebnis hinsichtlich der Schuldfrage determinieren. Um dieser Gefahr vorzubeugen, sollen verschiedene Lösungsansätze entwickelt werden. Zum einen soll ein Vergleich zu den Anfängen anderer forensischer Wissenschaften vor Gericht hergestellt (u.a. DNA-Analysen, Rechtsmedizin, Glaubwürdigkeitsgutachten) und ggf. die dabei entwickelten Regeln auf die IT-Forensik übertragen werden. Zum anderen könnte eine präzisere Kommunikation zwischen verfahrensbeteiligten Juristen und IT-Sachverständigen notwendig sein, sowie Grundkenntnisse aller Verfahrensbeteiligter hinsichtlich der Besonderheit der IT-Forensik und Daten als Beweismittel, um die Ergebnisse der Gutachten im Rahmen der Beweiswürdigung auf Plausibilität überprüfen zu können.

Automated Side-Channel Evaluation of Embedded Devices

Jens Schlumberger (jens.schlumberger@fau.de)
Supervisor: Dr. Stefan Wildermann

The always increasing abundance of embedded devices dealing with sensitive or security critical data should incentivize side-channel security evaluations not only for vendors but also forensic investigators. Hereby, side-channels like electromagnetic radiation can compromise mathematically safe cryptography by leaking information about the key. This is of special interest, as smart home devices and the Internet of Things are on the rise and many devices can provide valuable information when their cryptographic key is revealed. To analyze the side-channel information of a specific device, emissions of several cryptographic operations need to be recorded, synchronized, and compared to detect leakage. In order to enable easier and faster ways to evaluate generic embedded devices, new approaches have to be developed.

Forensic investigations have specific requirements for side-channel analysis, as they should not modify or tamper with evidence during the task. Therefore, electromagnetic radiation probes can be used to measure the emissions. However, current side-channel evaluation techniques use highly device-specific training or information which is not feasible due to the diversity of embedded systems. Therefore, expensive experts and a lot of time and effort would be needed to retrieve side-channel information at a crime scene. As this is not feasible for every crime scene, valuable information may be lost.

To tackle these problems, this thesis investigates new approaches which will enable highly automated side-channel evaluation of embedded devices. With a main focus on the Advanced Encryption Standard (AES) as it is widely spread for embedded systems as a symmetric, round based cipher. The goal is a system that automatically evaluates a device which uses AES without preliminary knowledge about the device. Specifically, the following challenges are faced:

First, detecting and characterizing of AES operations on a power trace with multiple recorded AES operations without device-specific knowledge. Second, the approach shall be independent of the measuring setup as well as the concrete implementation of AES. A final goal is to build a framework that can do a live side-channel evaluation of a target device.

Tools and Techniques for Structured Analysis of Digital Evidence

Janine Schneider (janine.schneider@fau.de)
Supervisor: Prof. Dr.-Ing. Felix Freiling

Digital evidence is an increasingly important form of evidence in courts of law today and it comes in many different forms, be it pictures stored on a hard disk, documents in a cloud or passwords stored in a computer's main memory. This form of evidence constantly introduces new challenges, changing with new technologies and applications. For example, because solid-state drives (SSDs) operate in an entirely different way as classical hard discs (HDDs) it is questionable whether classical techniques to recover deleted files (file carving) can still be applied. Furthermore, the increased risk of bit errors could lead to integrity check failures while using cryptographic hashes. Another example is the complex handling of cloud storage and shared documents. Vassil Roussev and Shane McCulley already did some extensive research on API-based data acquisition and analysis and developed a tool called *kumodocs*[1] which is able to extract artifacts of Google documents and slides. Besides, in contrast to other forms of evidence, the sheer quantity of digital evidence is actually a problem. Therefore, it needs new ways to acquire and analyze digital evidence efficiently, to ensure integrity and to combine already existing forensic approaches. Brian Carrier already observed that the task to reconstruct evidence on higher levels of abstraction from low level evidence is non-trivial[2] since it involves decoding the mapping between pieces of data on both layers and to bridge the semantic gap[3]. Within this PhD thesis we will develop a model of storage abstraction layers to formalize the problem of reconstructing evidence on higher levels from lower levels of abstraction. The model will make use of heuristics to formalizes different analysis and reconstruction problems and to create a generalized interface for enabling the combination of different solving approaches. Through the generic combination of various techniques results could be strengthen or the result quantity could be decreased. To demonstrate the applicability of the approach, a forensic analysis and reconstruction tool will be implemented. The tool will be an open-source C++ framework whose architecture will be directly derived from the model.

[1] Vassil Roussev and Shane McCulley, Forensic analysis of cloud-native artifacts, Digital Investigation, 16, S104-S113, 2016

[2] Brian Carrier, Defining digital forensic examination and analysis tools using abstraction layers, International Journal of Digital Evidence, 1, 2003

[3] Jain et al., SoK: Introspections on Trust and the Semantic Gap, IEEE Symposium on Security and Privacy, SP 2014, pp. 605-620, 2014

HPI Research Schools on Data Science and Engineering and Service-Oriented Systems Engineering

Prof. Dr. Felix Naumann, Prof. Dr. Tilmann Rabl,
Prof. Dr. Andreas Polze, and Prof. Dr. Robert Hirschfeld
Email: felix.naumann@hpi.uni-potsdam.de,
tilmann.rabl@hpi.uni-potsdam.de, andreas.polze@hpi.uni-potsdam.de,
robert.hirschfeld@hpi.uni-potsdam.de
Hasso Plattner Institute at the University of Potsdam
Internet: https://hpi.de/forschung/research-schools.html

HPI's research schools explore topics in the fields of data science and IT systems engineering that are of interest to academics and practitioners.

The research school "Data Science and Engineering" unites top PhD students and researchers in all areas of data-driven research and technology, including scalable storage, stream processing, data cleaning, machine learning and deep learning, text processing, data visualization, digital health, and more.

The research school "Service-Oriented Systems Engineering" is active in research areas such as system design, analysis, and modeling; adaptability; component-based development and application integration; business process management; cyber security; software engineering; and programming technology.

Bayesian Causal Inference Models of Software Fault Understanding with an Application to Sequential Decision Models for Optimal Code Inspection Task Allocation

Christian M. Adriano (christian.adriano@hpi.de)
Supervisor: Prof. Dr. Holger Giese

Context. Software programmers spend from 20% to 40% of their time searching for the causes of software failures. To alleviate that, debugging techniques were developed to reduce the search space from the entire program execution to a list of suspicious program statements. However, these debugging techniques assume "perfect fault understanding", i.e., that the programmer will always recognize the software fault among the list of suspicious program statements. Since inaccurate fault understanding inevitably happens, this causes programmers to waste time generating invalid bug fixes, which in turn undermines the programmers' trust on the debugging techniques and tools.

Objective (Goal-Question-Metric). Analyze code inspection tasks for the purpose of understanding which factors can predict if a software fault was correctly identified from the perspective of the programmer in the context of software debugging.

Method. We performed two large experiments with respectively 777 and 654 anonymous programmers who executed small, self-contained, independent code inspection tasks. These tasks consisted of answering automatically generated questions about possible relationship between a suspicious program statement and one out of 18 real software failures from various popular open source software projects. The independent variables were the programming ability of the participant and two types of program statements, faulty (experimental condition) or not faulty (control condition). Participants with different programming abilities were randomly assigned to one of the two conditions.

Results. We uncovered a set of factors that can predict the accuracy of fault understanding. Factors combine both programmers' attributes (coding ability, profession, years of experience) and the outcomes of their code inspection tasks (perceived difficulty, confidence, duration, explanations provided). To confirm and refine the prediction factors, we built two causal models: programmer qualification model and task inspection model. This two-stage causal model guarantees that the inferences about participants programming ability are understood and explained before we use this information as input to the second causal model, which in turn explains the accuracy of the code inspection tasks. We applied these causal models to build an algorithm the minimizes the

number of tasks needed to identify bugs. The algorithm extends the multi-armed bandit approach to make sequential decisions about which tasks to generate next based on the answers of previous tasks. Our results allowed to locate all faults with more than 90% precision while requiring only 20% of total available tasks.

RGB-D Camera and Deep Learning based Human Motion Analysis

Justin Albert (justin.albert@hpi.de)
Supervisor: Prof. Dr. Bert Arnrich

The human gait pattern is an important indicator of neurological and musculoskeletal diseases. Usually, gait is assessed in a specialized laboratory environment using expensive and high-quality multi-camera motion capturing systems, such as the Vicon system (Vicon, UK). However, these systems require active or passive reflective markers to be placed onto the subject to be tracked by the individual cameras. With the release of the Microsoft Kinect RGB-D camera in 2010, low-cost and markerless tracking of human movement has become available to the global market. The recently released new Kinect generation (Azure Kinect) has improved hardware and uses Deep Learning for body tracking. The aim of this work is to investigate how these low-cost cameras can be used for health-related applications.

A first question is how the performance of the Deep Learning based algorithm for tracking human poses has improved over the last Kinect generation, which uses conventional learning algorithms. Similar evaluation studies of the predecessor model have been presented in the literature for use in the physical assessment of healthy or pathological people[1][2]. Therefore, the Azure-Kinect camera is evaluated for treadmill gait assessment in comparison to a 10 camera gold standard Vicon system that provides high quality joint positions. The experiments will be conducted at the Division of Training and Movement Science at the University of Potsdam.

Subsequently, the Azure Kinect camera should be utilized for health related applications such as the fatigue detection based on a person's walking behavior. The defined study protocol provides that healthy participants first walk on a treadmill, followed by an exercise protocol for the synthetic induction of fatigue, and then perform a second walking trial. Kinematic time series data is recorded using the Azure Kinect and later evaluated using supervised or unsupervised machine learning methods. The corresponding ethics proposal for this study has already been accepted by the Ethics Committee.

[1] M. Capecci, M. Ceravolo, F. Ferracuti, S. Iarlori, S. Longhi, L. Romeo, S. Russi, and F. Verdini. "Accuracy evaluation of the Kinect v2 sensor during dynamic movements in a rehabilitation scenario". In: IEEE Engineering in Medicine and Biology Society. Conference 2016 (Aug. 2016), pages 5409–5412.

[2] R. A. Clark, B. F. Mentiplay, E. Hough, and Y. H. Pua. "Three-dimensional cameras and skeleton pose tracking for physical function assessment: A review of uses, validity, current developments and Kinect alternatives". In: Gait and Posture 68 (2019), pages 193–200.

Outlier Records: Syntactic Pattern Matching Using Abstractions

Mazhar Hameed (mazhar.hameed@hpi.uni-potsdam.de)
Supervisor: Prof. Dr. Felix Naumann

Data is produced every second from different sources with different structures for different purposes. As more and more data is produced, the ability of dealing with it accurately and according to user requirements has become more challenging for downstream applications. Among other challenges, the detection of outlier records in files is a unique problem that can be one of the key features in the data preparation pipeline. Outlier records is a problem persistent not only in raw data but also in refined data due to loosely defined schemata, incorrect formatting of values, record structure discrepancy, etc.

Generally, outlier detection implies values or attributes that are anomalies within a dataset. In our research, we are focusing on detecting outlier records in files i.e., to identify rows that are inconsistent with the rest of the data in file. This provides a unique opportunity to detect and resolve issues that can either hinder or completely halt operations, such as loading data to management systems, loading data to structure data driven systems, ingesting data to machine learning algorithms, etc.

To address these issues, we propose a technique that is not reliant on external information, such as field data types, record structure, file dialect, etc. To meet this challenge, we are developing an algorithm that parses input files and generates patterns using abstraction classes with ordered dependencies for individual records based on their syntax. Finally, we group these generated patterns into clusters to identify records that do not belong to them, which helps to identify outliers.

Structure Detection in Verbose CSV Files

Lan Jiang (lan.jiang@hpi.de)
Supervisor: Prof. Dr. Felix Naumann

To enable data-driven applications, such as business decision makings, scientific studies, and health cares, users must analyze data collected from possibly various sources in various shapes and forms. Verbose CSV format is one of such form. A normal CSV file contains a header row and a number of data rows. In addition to these basic information, a verbose CSV file includes metadata such as preamble, aggregation, group headers, and footnotes. These metadata may scatter at any positions in the file, causing it impractical or impossible to extract information from these files with common CSV parsers.

In order to collect useful information from verbose CSV files, one must understand the structure thereof. The research problem can be formalized as *detect the classes of particular elements in a given verbose CSV file*. In this context, an element is either a row or a cell. Previous work addressed a similar problem for either row or cell level element class detection with various classification models, e.g., random forest, conditional random fields, neural networks. However, they were focused on dealing with rich-text files, i.e., files with assorted styles such as element background/font color, border thickness, etc., and therefore adopted a set of styling features. We try to relax this constraint by considering only content and context information, because verbose CSV files do not store styles. We have built our class taxonomy with six various types on top of a previous work[1]. Our approach is grounded on a multi-class random forest classifier. In order to compensate the loss of style features, we have proposed a number of sophisticated features about content and context. Our approach deals with both line-level and cell-level element class detection. Experiment results show that our approach outperforms the related works that exploited styling features in terms of our evaluation metrics F1 score. We feed the result from line class detection task to the cell counterpart, and recognized that a good line-level class discovery helps to improve the overall cell-level element classification.

Our approach is so far only using syntactic content features, such as data type, letter cases, value length, etc. However, we have observed their limitation to deal with semantics, such as country-state relations. A possible follow-up work may introduce semantic understanding techniques such as knowledge base. We have introduced an arithmetic calculation feature to dedicated derived cell detection. The calculation is only considering the adjacent cells for a derived cell candidate. Therefore, another future work is to explore how to use cells that are a few hops away from the candidate.

[1] M. D. Adelfio and H. Samet. Schema extraction fortabular data on the web.Proceedings of the VLDBEndowment, 6(6):421–432, 2013.

Personal Small-batch Production

Shohei katakura (shohei.katakura@hpi.de)
Supervisor: Prof. Dr. Patrick Baudisch

The goal of my research is to enable non-industrial designers or initial hardware startups who don't have mechanical engineering knowledge to produce 500 - 1000 of their products.

Today, we can design using CAD software and prototype our hardware using 3D printers, laser cutters, etc. 3D printers in particular have few restrictions on manufacturing, allowing people without manufacturing knowledge to quickly fabricate objects they have designed. While there are few problems if we only make a one-off prototype, once we try to mass-produce it, non-expert users encounter the following issues during the 3D modeling and design phase.

- Managing material consumption
- Addressing manufacturing processes
- Catering for machine-specific characteristics
- Designing for easy assembly

In the industrial domain, a professional engineer refines the prototype to be mass producible, the process is called design for manufacturing and assembly (DFMA). This process is critical for mass-production from a cost/manufacturing perspective and is considered early in the design process. However, it is difficult for non-experts to carry out this refinement as it requires a lot of domain knowledge.

I address this by developing a design system with a software agent. In this design system, the user has authority over the function and shape of the product while the agent has authority over the cost of the materials and the manufacturing process. Users can collaborate with the software agent to create products and custom-made tools, facilitating small-batch production.

Space Independent Real Walking In Virtual Reality

Sebastian Marwecki (sebastian.marwecki@hpi.de)
Supervisor: Prof. Dr. Patrick Baudisch

The goal of my research is to allow virtual reality experiences to be run in arbitrary tracking volumes and with arbitrary physical objects.

VR experiences today are designed with a specific tracking volume and objects in mind, such as "square 5x5m space with a rubber sword". This prevents experiences from running with different objects or in tracking volumes of smaller size or different shape, making it impossible to share experiences, especially with home users.

I address this by creating an abstraction between VR applications and the space and physical objects they are using. Instead of accessing space and physical objects directly, in my system applications express their needs in an abstract way, which my systems then maps to the actual available physical space and physical objects. This allows VR applications to run on a wide range of installations.

Solving this problem would have substantial commercial impact, as the proliferation of real-walking VR is currently hindered by developers' reluctance to require users to have space and objects.

My work is inspired by operating systems research. Before opening systems, application programs were written for a specific machine. Operating systems allow applications to run on arbitrary computers and architectures by creating an abstraction of the physical hardware, an API, that allows applications from accessing the hardware directly.

Closed-Loop Warning System of Epilepsy Treatment

Sidratul Moontaha (sidratul.moontaha@hpi.uni-potsdam.de)
Supervisor: Prof. Dr. Bert Arnrich

Among the 0.5-1% of the pediatric population suffering from epilepsy, about 25-30% of patients have difficult-to-treat or treatment-resistant epilepsy. Along with the risk of SUDEP (sudden unexpected death in epilepsy), the quality of life (Qol) of these patients highly depends on other comorbidities such as medication side effects, sleep quality, restricted independence, stigmatization, and importantly, the unpredictability of seizure occurrence. To provide a closed-loop warning system for proper management of epilepsy, the most important are continuous monitoring of patient's data, seizure prediction (before seizure onset) and detection (during seizure onset), maintaining electronic seizure diary, providing right dosages of AEDs. Researchers provide a set of several *seizure prediction* algorithms based on the available databases which provide Electroencephalogram (EEG) data for epilepsy patients. However, to predict and detect epileptic seizures, continuous monitoring is necessary. The long term video EEG monitoring, which is the gold standard at present, may limit not only the patients' day to day activities but also is costly in terms of providing in-hospital support, trained nurses, trained EEG analysts, and so on. Therefore, data technologies of predicting or detecting seizures are evolving towards wearable devices. In search of non-EEG seizure prediction bio-markers, we found that the changes in the pre-ictal heart rate are most effective in predicting seizure several minutes before seizure onset. Recent literature of seizure prediction shows a few analysis-oriented approaches of seizure prediction where the main objective is to analyze the statistical properties of pre-seizure states. It was mainly based on analyzing the pre-ictal Electrocardiography (ECG) data of patients who have epilepsy by applying machine learning algorithms. Recently, a study proposed a method of combining the features taken from EEG and ECG with a machine learning approach[1]. We propose to replace for these non-invasive, non-EEG prediction of seizures based on analysis based seizure prediction to provide a real-time solution. We will aim at collecting the pre-ictal and interictal heart rate data with a wearable device and extract features to provide an alarm to the patients or caregivers before seizure onset. The next step after seizure prediction or detection is to apply *behavioral interventions* for a better QoL for epilepsy patients. Researchers have already found evidence of producing physiologic changes such as the improvement in epileptiform activities on EEG of patients who have epilepsy. Since behavioral intervention itself is a broad category, our research will focus on providing bio/neurofeedback based on the collected ECG data.

[1] Billeci et al., "Epileptic seizures prediction based on the combination of EEG and ECG for the application in a wearable device," 2019 IEEE 23rd International Symposium on Consumer Technologies (ISCT), p. 28–33, 2019

Automatic Reinforcement of Lasercut Structures

Muhammad Abdullah (muhammad.abdullah@hpi.de)
Supervisor: Prof. Dr. Patrick Baudisch

My research focuses on developing a software tool that identifies points of potential failure in lasercut structures and automatically reinforces them.

Laser cutting is a fast fabrication technology that is orders of magnitude faster than other prototyping technologies. This allows users to build large objects quickly. While earlier systems used thicker materials to achieve strength and functionality, recently proposed "closed box structures" achieve similar results using considerably thinner materials. However, these structures need to be manually reinforced to allow functional use. This task is quite difficult and tedious for non-expert users.

The proposed software tool called *Infill* performs this task automatically. It first classifies points of potential failure in the structure using a graph based algorithm. Then it identifies a set of lasercut plates that can be placed to reinforce each failure point. *Infill* can be integrated into existing 3D editors for lasercutting. *Infill* is designed to require very little computational resources allowing it to run in the background continuously and automatically reinforcing the user's model during editing.

In our technical evaluation, we found that objects reinforced using *Infill* took up-to 52 times more force to break than without. This allows *Infill* to facilitate non-expert users to build functional objects e.g. furniture that people can sit on from materials as thin as 4mm plywood.

Shortest Path Enumeration

Stefan Neubert (Stefan.Neubert@hpi.de)
Supervisor: Prof. Dr. Tobias Friedrich

Algorithms that solve shortest path problems on graphs are among the most studied algorithms in both theoretical and applied computer science. Besides the obvious application for routing (physical navigation and data routing likewise), many problems can be modeled in terms of a shortest path problem, for example computing string similarity measures, aligning character sequences or efficiently navigating a huge state space in robotic arm movement.

When analyzing such problems, one is usually interested in algorithms that minimize total computation time for large inputs, and in matching lower bounds that rule out faster algorithms. However, most lower bounds are based on conjectures such as the All-Pairs-Shortest-Paths Hypothesis, which claims that there is no ε such that APSP can be solved in $O(n^{3-\varepsilon})$ time.

In current day systems, the input size n tends to be that large, that such an algorithm with cubic theoretical runtime leads to enormous wall-clock waiting time. In addition, systems rarely consist of a single data processing step, but are made of multiple algorithms run in series on potentially many machines. If one of those algorithms takes a lot of time to produce its output, the rest of the pipeline is stalled, and computing power is unused.

We approach this issue by quickly enumerating individual shortest distances. Even though the algorithm's total runtime cannot be better (and might even be worse) than when producing the output in one piece, following steps in the pipeline can already work on partial outputs long before the whole solution is provided and by that cut down on the overall runtime of the pipeline.

From a theory perspective, we want to find the *worst case delay* for such an approach: How long must a subsequent pipeline step wait in the worst case until the next partial solution is provided? By homogeneously distributing an algorithms computing time on the produced partial solutions, this analysis might reveal parts of the final output that are the hardest to compute, leading to new lower bounds or to faster algorithms, that optimize for this sub-problem.

We have been able to proof that a modified breadth first search is optimal for enumerating all single source shortest distances. In a graph with n vertices with a maximum degree of Δ this achieves a delay of $O(\Delta)$. The matching $\Omega(\Delta)$ lower bound on the delay is proven with an unconditional adversary argument. The equivalent construction for positively weighted graphs and Dijkstra's algorithm yields a delay of $O(\Delta + \log(n))$.

For the unweighted APSP we achieve a better delay of $O(\overline{\Delta})$, where $\overline{\Delta}$ is the average degree of the graph. Positive edge weights increase the delay to $O(\overline{\Delta} + \log(n))$. Both algorithms achieve the same total time as repeatedly running BFS or Dijkstra's algorithm (and in their core do exactly that).

Federated Learning Utilising the Tangle Architecture

Bjarne Pfitzner (bjarne.pfitzner@hpi.uni-potsdam.de)
Supervisor: Prof. Dr. Bert Arnrich

Data for training machine learning models is often widely distributed and difficult to share, especially in the medical domain. One approach to still make use of large distributed datasets is *federated learning* which relies on sharing the machine learning model instead of the data directly. In a federated learning system, the server defines and initializes the model and sends it to the clients, who own private data. They can then train for a few epochs on their local data and send the resulting model back to the server, where all updates are averaged into a new improved model. In an iterative fashion, this process is repeated until the model converges.

Sometimes there is no trusted entity available to facilitate the training process, which is why some federated learning research is concerned with using blockchain methods for a decentralized training procedure. We propose going a step further and building a tangle architecture[1] for training machine learning models. Participants own private data and further the training process by selecting two recent model parameter publications (called transactions) from the tangle, averaging them and training locally. If this new model performs better than the current global consensus model, the new parameter values can be published onto the tangle, verifying the two selected transactions.

Our experiments have shown that the tangle learning architecture can reach model performances comparable to the one of federated learning. One benefit of the tangle approach is an inherent resistance against model poisoning attacks, where adversarial participants try to introduce random or malicious weights into the averaging procedure, which reduces the resulting model accuracy. The local validation process for selected transactions before submitting new model parameters entails that (usually) only malicious participants can verify malicious transactions. The initial experimentation has shown that for smaller fractions of malicious participants (< 0.25) introducing random weights into the tangle, the consensus model performance stays the same over time. Also, the popular label-flipping attacks were found to be ineffective against the tangle architecture.

Since federated learning has not been used together with a tangle architecture before, there is a lot of future research to be done. The approach has to be applied to real-world datasets, for example from the healthcare domain, which requires methods to train machine learning models with private data. Moreover, the experimentation in the security and privacy direction only considered model poisoning attacks so far, but there are more, such as reconstruction attacks, that have to be investigated and could show stronger security and privacy needs of the algorithm.

[1] Serguei Popov, The tangle, 2018. [Online]. Available: https://iota.org/IOTA_Whitepaper.pdf.

Learning Disentangled Deep Latent Space Representations

Alexander Rakowski (alexander.rakowski@hpi.de)
Supervisor: Prof. Dr. Christoph Lippert

The sizes of modern datasets tend to grow, allowing to train more complex machine learning models, containing up to billions of parameters, by leveraging the vast quantities of samples. However, the labeling of examples remains a costly process. This instigates the need of developing better unsupervised, self- or semi-supervised algorithms, which are designed to use when no (or only a limited number) of annotations are available. In the field of representation learning one would try to learn transformations which map the data into smaller, more compact spaces. Ideally, these should correspond to more abstract factors of the observed samples. It is believed that disentanglement of dimensions of these representations is one of the crucial qualities to be obtained, making them more interpretable and more useful for further tasks[1].

Current methods are based on the *Variational Autoencoders (VAEs)* framework. However it is shown that none of them yield consistent performance in the unsupervised setting[2]. In particular, increasing the regularization strength of these methods is not correlated with disentanglement scores. Neither are sets of hyperparameters transferable (in terms of achieving the same performance) across different problem settings. It thus still remains an open question how to develop learning methods that lead to disentangled representations, and even to identify aspects of the training process that are related to disentangling.

In my research I decided to investigate other model families capable of learning representations. *Generative Adversarial Networks (GANs)* are able to produce more realistic samples than VAEs. It might be that VAEs are not able to learn correct latent representations of the data because they are not able to reflect some factors of variation in the generative model. *Wasserstein Autoencoders (WAEs)*, while similar to VAEs, allow the choice of different distances to measure divergence from the prior. They have also been shown to yield better sample quality, without the need of an adversarial type of training. The investigated methods of learning disentangled representations with these models include *cycle consistency, robustness to transformations* or *model sparsity*.

[1] Y. Bengio, A. Courville, and P. Vincent, "Representation Learning: A Review and New Perspectives,"IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 35.8, p. 1798–1828, 2013

[2] F. Locatello, S. Bauer, M. Lucic, G. Raetsch, S. Gelly, B. Schoelkopf, and O. Bachem, "Challenging Common Assumptions in the Unsupervised Learning of Disentangled Representations" arXiv preprint arXiv:1811.12359, 2018

Comment Analysis with Deep Learning

Julian Risch (julian.risch@hpi.de)
Supervisor: Prof. Dr. Felix Naumann, Dr. Ralf Krestel

Comment sections of online news platforms are an essential space to express opinions and discuss political topics. However, the misuse by spammers, haters, and trolls raises doubts about whether the benefits of comment sections justify their costs, e.g., the time-consuming content moderation. As a consequence, many platforms limited them or even shut them down completely. With my research, I aim to support news platforms in keeping comment sections open and investigate the research question: "How can we foster respectful and engaging online discussions?". To this end, I analyze large comment datasets and develop deep learning approaches for comment classification, recommendation, and popularity prediction. Research challenges are the generalization across different tasks, the robustness despite sparse training data, and the explainability of black-box deep neural network models.

I focus on two kinds of comments: (1) toxic comments, which make other users leave a discussion, and (2) engaging comments, which make other users join a discussion. On the one hand, the goal is to discourage and remove comments that violate the platform's rules, e.g., by using offensive language. My semi-automatic comment moderation approach is based on binary and on fine-grained text classification.[1] For example, the classes include obscenity, threats, insults, identity hate, misogynistic aggression, and overt or covert aggression. On the other hand, the goal is to encourage and highlight comments that trigger other users to contribute to the discussion. My approach is to rank comments by how engaging and relevant they are instead of their publication time.[2] Further, based on a user's interest, I provide personalized recommendations on discussions that are interesting to join. This approach also considers journalists as users, for whom it is infeasible to keep track of all readers' comments on their articles. To support them in joining a discussion, I recommend the most relevant comments to them, e.g., comments that address the article author.

My experiments show that unsupervised pre-training, data augmentation, and ensemble learning allow training robust classifiers even on small datasets of less than five thousand labeled comments. To establish trust in the semi-automatic moderation process, attribution-based explanation methods reveal which words are decisive for the classifier's output. In future work, I would like to enable readers to explore comment threads with the help of interactive visualizations. Rather than scrolling through hundreds of comments, readers could dive into clustered subtopics of their interest.

[1] Risch, J., Krestel, R., "Delete or not Delete? Semi-Automatic Comment Moderation for the Newsroom", *Proceedings of TRAC@COLING*, p. 166-176, 2018.

[2] Risch, J., Krestel, R., "Top Comment or Flop Comment? Predicting and Explaining User Engagement in Online News Discussions", *Proceedings of ICWSM*, p. 1-11, 2020.

Digital Twins for Indoor Built Environments

Vladeta Stojanovic (vladeta.stojanovic@hpi.de)
Supervisor: Prof. Dr. Jürgen Döllner

One of the key challenges in modern Facility Management (FM) is digitally reflecting the current state of the built environment, referred to *as-is* or *as-built* versus as-designed representation. While the use of Building Information Modeling (BIM) can address the issue of digital representation, generation and maintenance of BIM data requires considerable amount of manual work and domain expertise. Another key challenge is being able to monitor and forecast the current state of the built environment, which is used to provide feedback and enhance decision making. The need for integrated solutions is becoming more pronounced as practices from Industry 4.0 are currently being evaluated and adopted for FM use. This research presents and describes methods and approaches for complete digital representation of indoor environment. The key to solving such a complex issue of digital data integration, processing and representation is with the use of a Digital Twin (DT). A DT is a digital duplicate of the physical environment, states, and processes. A DT representation fuses *as-designed* and *as-is* physical representations, with additional information layers pertaining to the current and predicted states of an indoor environment or complete building. The design, implementation and initial testing of a prototypical DT software platform for indoor environments is presented and described. The DT software platform is implemented using a Service Oriented Architecture (SOA) paradigm, and its feasibility is presented through functioning and tested key software components. The outcome of this research shows that digital data related to FM and Architecture, Construction, Engineering, Owner and Occupant (AECOO) activity can be analyzed and visualized in real-time using a service-oriented approach. This has great potential to benefit decision making related to Operation and Maintenance (Oand M) procedures within the scope of the post-construction lifecycle stages of typical office buildings.

Stojanovic, V., Trapp, M., Richter, R., and Döllner, J. (2018). "A service-oriented approach for classifying 3D points clouds by example of office furniture classification". In: *Proceedings of the 23rd International ACM Conference on 3D Web Technology (Web3D '18)*, p. 9. DOI: https://doi.org/10.1145/3208806.3208810.

Stojanovic, V., Trapp, M., Richter, R., Hagedorn, B., and Döllner, J. (2018). "Towards the Generation of Digital Twins for Facility Management Based on 3D Point Clouds". In: *Gorse, C and Neilson, C J (Eds.), Proceedings 34th Annual ARCOM Conference*, 3-5 September 2018, Queen's University, Belfast, UK. Association of Researchers in Construction Management, pp.270–279.

Stojanovic, V., Trapp, M., Richter, R., and Döllner, J. (2019). "Generation of Approximate 2D and 3D Floor Plans from 3D Point Clouds". In: *Proceedings*

of the 14th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications - Volume 1: GRAPP, pp. 177-184.

Stojanovic, V., Trapp, M., Richter, R., and Döllner, J. (2019). "Classification of Indoor Point Clouds Using Multiviews". In: *Web3D '19: The 24th International Conference on 3D Web Technology (Web3D '19)*, p.9. DOI: `https://doi.org/10.1145/3329714.3338129`

Stojanovic, V., Trapp, M., Richter, R., Hagedorn, B., and Döllner, J. (2019). "Semantic Enrichment of Indoor Point Clouds: An Overview of Progress towards Digital Twinning". In: *37th eCAADe Conference*. Faculty of Architecture, University of Porto, Portugal, 11th - 13th September 2019.

Stojanovic, V., Trapp, M., Richter, R., and Döllner, J. (2019). "Service-Oriented Semantic Enrichment of Indoor Point Clouds using Multiview-Based Classification". In: *Graphical Models*. DOI: `https://doi.org/10.1016/j.gmod.2019.101039`. Elsevier.

Stojanovic, V., Trapp, M., Hagedorn, B., Klimke, J., Richter, R., and Döllner, J. (2019). "Sensor Data Visualization for Indoor Point Clouds". In: *Advances in Cartography and GIScience of the ICA*, 2.

Stojanovic, V., Trapp, M., Richter, R., and Döllner, J. (2019). "A Service-oriented Indoor Point Cloud Processing Pipeline". In: *The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences*, 42, pp.339-346.

Isailović, D., **Stojanovic, V.**, Trapp, M., Richter, R., Hajdin, R., and Döllner, J. (2020). "Bridge Damage: Detection, IFC-Based Semantic Enrichment and Visualization". In: *Automation in Construction*. DOI: `https://doi.org/10.1016/j.autcon.2020.103088`. Elsevier.

Stojanovic, V., Trapp, M., Richter, R., and Döllner, J. (2020). "Comparison of Deep-Learning Classification Approaches for Indoor Point Clouds". In: *Publikationen der DGPF, Band 29, 2020*. pp.437-447.

Splitting Complex Multiregion Files for Data Preparation

Gerardo Vitagliano (gerardo.vitagliano@hpi.uni-potsdam.de)
Supervisor: Prof. Dr. Felix Naumann

The recent growth of data-intensive applications is often hampered by data quality issues, which cause 80% of the time spent on development to be focused on collecting and preparing data. Our research focuses on the pipeline of preparation operations carried on data before its usage in a downstream task, aiming at designing solutions that can either automate or assist the user interactively in solving time consuming data preparation problems.

In our work, we identified multiregion files: spreadsheets characterized by the presence of multiple, independent regions that may be scattered in an arbitrary layout (Cf. Figure 1).

To prepare such spreadsheets end users need to split them according to their visual structure isolating independent regions. We developed an approach, called Mondrian, to automate the region detection and assist users with an interactive file splittin based on the automatically detected regions. We combine a graphical stage, in which a spreadsheet is transformed in a binary image, and a clustering phase, where candidate elements are grouped together to form homogeneous regions. In the first stage, empty cells are represented with white pixels and non-empty cells are represented with black pixels. This operation highlights the structural layout of the spreadsheet data and allows to detect connected components, i.e. connected groups of data cells, which are used as starting elements for region recognition. Then, the connected components are partitioned into finer grained atomic elements using a rectilinear cut, to possibly allow detection of independent regions that are visually non separated. Once atomic elements have been identified, we use a density-based clustering algorithm to obtain candidate regions.

Finally, end-users are able to visualize the automated clustering results, validate them and to carry the final spreadsheet split in a graphical fashion using a web-based interactive interface.

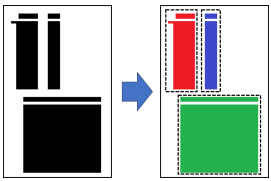


Figure 1: Visually splitting a multiregion spreadsheet

Concepts and Techniques for the Analysis of Large-Scale Geospatial Mobile-Mapping Data of Transport Infrastructure

Johannes Wolf (johannes.wolf@hpi.de)
Supervisor: Prof. Dr. Jürgen Döllner

Geospatial data is of great interest for urban planning, environmental monitoring, risk management, and in emergency situations. Captured datasets are usually large and unstructured and thus not easy to handle in traditional GIS. Efficiently processing the data and presenting use-case specific aggregated information and to gain valuable insights are central requirements for many applications.

3D point clouds are a universal, easy-to-capture, and discrete representation of real world environments. They are used in a multitude of use cases and enable analyses on precise geospatial measurement data. 3D point clouds have proven to be a valuable data source for analyses as they are easy to handle and hold great detail of the captured environment. Technically, they are stored as an unordered collection of measurement points each featuring three-dimensional coordinates and additional attributes, e. g., intensity values when being measured via LIDAR.

Different stakeholders, e. g., municipalities, governmental institutions, and private companies create digital archives of geospatial data by means of 3D point clouds, typically used for analyses, measurements, and preservation purposes. Cadastral data can be combined with point clouds to create interactive visualization tools for analysis and exploration. Mobile carrier platforms like cars or trains are used to capture entire infrastructure networks like roads or railroads. Mobile mapping data created that way serves as a detailed digital representation of the real world, and can be seen as a "digital twin".

Automated capturing technologies practically enable to achieve complete coverage in a given region and create highly detailed data sets in short amounts of time. Immediate uses in related workflows and processing systems and applications are hindered by the large amounts of unstructured data. For that reason, fast and reliable processing techniques are developed to automatically evaluate 3D point clouds and to add additional attributes, particularly enriching it with information about general object categories like "Building", "Vegetation" or "Ground" up to specific object identification like "Curbstone", "Road Marking—Arrow Left" and "Traffic Sign—No Overtaking" for groups of points. This process is called semantic classification.

The classification is done by developing automated processing techniques, using geometric features where fixed thresholds can be applied to detect certain structures as well as neural networks optimized for 3D point clouds, that have been previously trained using manually labeled data to detect the semantic classes of objects.

Towards Joint Design-Time and Run-time Verification of the Complex System

He Xu (He.Xu@hpi.de)
Supervisor: Prof. Dr. Holger Giese

When concerning a complex system that runs in the real world, it is hard to acquire an accurate long-term system model. On the one hand, the system may be too complex to establish a proper model, and it may also change its configuration or behavior during operation to react to the real world. On the other hand, it is infeasible to predict the long-term behavior of other systems that interact with the target system.

In this approach, I will use two checking methods correspond to run-time and design time verification. The backward checking will be used at design time to establish the unsafe areas around the inevitable unsafe states and to help engineers pick the proper countermeasures for each of these failures. This checking process can also help to analyze the uncertain and rare adverse events and conditions that may or may not happen in the operation of the system. For example, when self-driving car systems test or operate on the open street, they may collect failures or adverse events that are unanticipated in development. These unexpected situations can be analyzed offline using backward checking, and build specific unsafe areas that include these unsafe states and related system states. After that, these unsafe areas can be updated to the operating systems, and systems can react to these new threats. The backward checking can also analyze potential hazards and failures of the system, even the accurate system model is unknown, and establish the unsafe areas and specify the countermeasures respectively.

At run-time, the forward checking process only searches to states that are reachable from the current state within a fixed number of transitions. Once it detects the boundary of the unsafe area, it can execute the emergent mechanism to cope with the adverse situation. Combining with results from design time backward checking, the run-time forward checking can hence give the system enough time to prepare for potential failures or hazards. At the same time, it will reduce the time and resource consumption of time and resource at run-time.