Benedikt Etzold, René Richter, Maximilian Eibl, Wolfgang Lehner (editors)

Proceedings of the 10th Joint Workshop of the German Research Training Groups in Computer Science

Benedikt Etzold, René Richter, Maximilian Eibl, Wolfgang Lehner (editors)

Proceedings of the 10th Joint Workshop of the German Research Training Groups in Computer Science

Dagstuhl 2016,
May 22nd - 25th

TECHNISCHE UNIVERSITÄT
CHEMNITZ

Universitätsverlag Chemnitz
2016

Impressum

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Angaben sind im Internet über http://dnb.d-nb.de abrufbar.

Supported by

DFG Deutsche Forschungsgemeinschaft

Coverfoto: Schloss Dagstuhl - Leibniz-Zentrum für Informatik
Satz/Layout: René Richter

Technische Universität Chemnitz/Universitätsbibliothek
Universitätsverlag Chemnitz
09107 Chemnitz
http://www.tu-chemnitz.de/ub/univerlag

Herstellung und Auslieferung
Verlagshaus Monsenstein und Vannerdat OHG
Am Hawerkamp 31
48155 Münster
http://www.mv-verlag.de

ISBN 978-3-944640-88-4

http://nbn-resolving.de/urn:nbn:de:bsz:ch1-qucosa-201990

Preface

Since 2007, PhD students of the DFG Research Training Groups (RTGs) and other doctoral student programs in computer science have been meeting annually for networking and knowledge exchange purposes at Schloss Dagstuhl, one of the world's premier venues for computer science related seminars. The goal of these meetings is to maintain an interchange of opinions and practical knowledge between PhD students and to improve the connection between members of the German computer science community. This meeting, which is organized by the graduate students, invites PhD students in all stages of their work in order to give them the opportunity to present their current research topics, ideas, and scientific results.

This year's meeting is organized in cooperation by RTG 1907 RoSI - Role-based Software Infrastructures for continuous-context-sensitive Systems and RTG 1780 Crossworlds - Connecting Virtual and Real Social Worlds, and takes place at the Research Center of Schloss Dagstuhl from May 22nd to 25th.

This book includes abstracts of the PhD research areas of all computer science related RTG graduate students and associated doctoral programs and provides an insight into current research trends in Germany.

The Editors

Contents

1 RTG 1480: Programm- und Modell-Analyse (PUMA)

Prof. Dr. Helmut Seidl (seidl@in.tum.de)
The Fakultät für Informatik, Technische Universität München and
the Fakultät für Informatik, Ludwig-Maximilians-Universität München
http://puma.in.tum.de

The research training group PUMA brings together the four fundamental approaches of program and model analysis, namely, type systems, theorem proving, model-checking, and abstract interpretation. The Munich universities hosting the program have expert researchers in all of these areas. Our goal is to stimulate cross-fertilization between these approaches resulting in a better understanding of their common basis and their distinctive properties, and leading to better algorithms and tools. Our vision is the Verifying Compiler, i.e., the development of methods and tools that examine not only whether a program or model is syntactically correct, but also whether it behaves according to its specification.

We are in the second funding period has started where we focus on decision procedures which often are at the heart of combining different approaches and also consider verification questions related to assembly lines and autonomous systems.

1.1 Deciding MSO over ω-Words by Means of Finite Automata

Stephan Barth (stephan.barth@ifi.lmu.de)
Supervisor/s: Prof. Martin Hofmann, PhD

Decidability of monadic second order logic (MSO) over infinite words is long known[1]. In contrast to MSO over finite words it is considered impractical, though. The automata based approch that is used in MONA does not work well on infinite words with the standard models for ω-regular languages, as minimization has show to be crucial in the deciding procedure in MONA. However, minimization of widespread automata models for ω-regular languages does not scale well.

Choosing a more appropriate model for representing these languages with an efficient minimization can therefore dramaticaly enhance the runtime.

Herein the ω-regular language L is represented by the regular language $L' = \{u\$v | uv^\omega \in L\}$ and this by a DFA, for reference call this concept loop language/automaton. While the regularity of this language was already known by Buechi, algorithms for transformation between standard ω-regular automata models and loop automata were developed in 1994[2]. They did not give algorithms to work directly with loop languages.

We succeeded in developing the necessary algorithms to decide MSO over ω-words with finite automata using this representation.

Current research focus on incorporating state compression techniques and finalizing the implementation.

[1] J. R. Büchi, "On a decision method in restricted second order arithmetic," in *Proceedings of the 1960 International Congress on Logic, Methodology and Philosophy of Science (LMPS'60)*, 1962, pp. 1–11.

[2] H. Calbrix, M. Nivat, and A. Podelski, "Ultimately periodic words of rational omega-languages," in *Mathematical foundations of programming semantics*, vol. 802, Springer Berlin / Heidelberg, 1994, pp. 554–566.

1.2 Decidability of Linear Tree Constraints

Sabine Bauer (Sabine.Bauer@ifi.lmu.de)
Supervisor/s: Prof. Martin Hofmann, PhD

We consider satisfiability of linear constraints over infinite trees. These constraints are essentially linear inequalities between infinite lists or trees of nonnegative rational numbers which are added and compared pointwise. We have already proven NP-hardness of the general problem and decidability of a certain, for us relevant, subcase and now we are investigating ways to extract optimal solutions.

We have an attempt to formalize this question in a particular list case, namely when the solution lists are bounded only from below. In this case, the problem is similar to iterated matrix multiplication on a vector—with the difference that one has more than one matrix and one has to decide in each step which matrix to take. We have observed the connection to linear recurrence sequences and we are currently working on open questions concerning the results of these matrix operations.

If there is only one constraint per variable, we can determine the growth rate. We can always say, whether it is polynomial (and give a degree) or exponential. In the subcase of radial matrices, we can determine the asymptotic growth of the minimal solutions also if there are several constraints on one variable and mutual dependencies between the lists.

On a more practical side, we plan to implement the decision procedures.

1.3 Formally Verified Foundations for Complexity Analysis

Manuel Eberl (eberlm@in.tum.de)
Supervisor/s: Tobias Nipkow

I am developing mathematical foundations for time complexity analysis in the theorem prover Isabelle/HOL. I have already formalised the Akra–Bazzi theorem[1], a generalisation of the well-known Master theorem for the analysis of Divide & Conquer algorithms, and I am currently developing a formalisation of linear recurrences, including a fully verified solver for these recurrences.

I then want to employ methods from analytic combinatorics to find asymptotic bounds for complicated recurrences, ideally with some degree of automation. This is interesting because the time complexities of recursively-defined functions can often be expressed as such recurrences. For example, the Lambda-Upsilon-Omega system by Flajolet et al.[2] analyses functions that recursively traverse algebraic data types (e.g. finding the derivative of a function term) by syntactically deriving recurrence relations for both the underlying data types and the programs, finding asymptotic approximations for these relations using various methods from analytic combinatorics, and then deriving an asymptotic approximation for the overall time complexity from these.

I will attempt to recreate some of these methods in Isabelle and hope to analyse programs in a similar fashion in Isabelle, ideally semi-automatically.

[1] T. Leighton, "Notes on better Master theorems for divide-and-conquer recurrences," Lecture notes, MIT, 1996.

[2] P. Flajolet, P. Zimmermann, and B. Salvy, "Automatic average-case analysis of algorithms," INRIA, Projet ICSLA, Research Report RR-1233, 1990.

1.4 Polynomial Analysis of Probabilistic Workflow Nets

Philipp Hoffmann (ph.hoffmann@tum.de)
Supervisor/s: Javier Esparza

We study Workflow nets[1] and reduction methods thereof. Inspired by reduction rules for finite automata[2], we give a reduction algorithm based on reduction rules which are applied to reduce the size of the net. We characterize a class of nets which are well-formed, called sound, and show that with our rules exactly the sound nets can be reduced to a single transition. We also give a polynomial bound for the number of rule aplications neccesary.

Contrary to previous work, our rules do not only preserve soundness, but also the dataflow semantics: The net can be enriched by transformers, relations that change an internal state of the net. During the reduction, these transformers are also modified so that in the sound case, the single transition retained contains the whole input output relation of the net.

We also study a probabilistic extension of Workflow nets where after a nondeterministic choice of the tokens that move next the transition is chosen probabilistically. We give the semantics by means of an MDP[3] and also introduce a cost/reward model. Based on the rule bases reduction procedure, we present reduction rules to compute the expected cost of a complete execution of the workflow.

[1] W. M. P. van der Aalst, "The application of petri nets to workflow management," *Journal of Circuits, Systems, and Computers*, vol. 8, no. 1, pp. 21–66, 1998.

[2] J. E. Hopcroft, R. Motwani, and J. D. Ullman, *Introduction to automata theory, languages, and computation (3rd edition)*. Addison-Wesley Longman Publishing Co., Inc., 2006.

[3] M. L. Puterman, *Markov decision processes: Discrete stochastic dynamic programming*. John Wiley & Sons, 2014.

1.5 Formalization of Rigorous Numerical Methods for ODEs

Fabian Immler (immler@in.tum.de)
Supervisor/s: Prof. Tobias Nipkow, Ph.D.

Ordinary differential equations (ODEs) are ubiquitous when modeling continuous dynamics. Classical numerical methods compute approximations, here we present an algorithm that computes enclosures of the solution and which is mechanically verified with respect to the formalization of ODEs in Isabelle/HOL. We use the data structure of affine forms to perform the rigorous numerical computations, i.e., to enclose round-off and discretization errors. The algorithm is based on adaptive Runge-Kutta methods. We present optimizations like splitting, intersecting, and reducing reachable sets, which are important for analyzing chaotic systems.

One such chaotic system is given by the Lorenz equations. A long-standing conjecture concerning the existence of a strange attractor for those equations could be confirmed by Warwick Tucker in 1999. His proof relies on rigorous numerical computations and therefore on the correctness of algorithms. We use our verified algorithm to certify (parts of) Warwick Tucker's computer aided proof.

1.6 Analysis via Strategy Iteration and its Advantages

Zuzana Kretinska (kretinska.zuzana@tum.de)
Supervisor/s: Prof. Dr. Helmut Seidl

Systems of equations with addition, multiplication, constants, maxima, and minima are a fundamental structure, which can be used in many contexts such as for describing two-player zero-sum games or in abstract interpretation of programs. There are several approaches to compute solutions of such systems, most importantly methods based on dynamic programming: strategy iteration and value iteration. Moreover, if only minima or only maxima are present, then linear programming can be used, too. Besides, the methods can be combined: for instance, strategy iteration can be used to improve only maxima and the equation system with minima can be evaluated using linear programming. This has been suggested and applied to program analysis for systems over rationals[1], for systems over integers[2], and variants for improving maxima and improving minima are compared[3].

However, these approaches have been compared in a few contexts only. We intend to compare variants of strategy iteration, value iteration, and linear programming in the setting of (i) program analysis via abstract interpretation, (ii) analysis of (a) Markov decision processes, (b) stochastic games, and (c) energy games, each with different objectives, such as reachability or long-run properties. The comparison shall be made with respect to the following aspects: (i) speed of convergence to (a) the optimal solution, and to (b) an epsilon-approximation of a solution for a predefined epsilon; (ii) robustness of the approaches when the equation system is perturbed; (iii) applicability of the approaches to the parametric setting, where the equation system contains parameters that are (a) integral[4], or (b) real.

While strategy iteration has been used mainly for solving two-player games so far, the thorough comparison will identify contexts where strategy iteration methods have not been used, but actually are more appropriate than currently used methods.

[1] T. Gawlitza and H. Seidl, "Precise relational invariants through strategy iteration," in *Computer science logic, 21st international workshop, CSL 2007, 16th annual conference of the EACSL, Lausanne, Switzerland, September 11-15, 2007, Proceedings*, 2007, vol. 4646, pp. 23–40.

[2] T. M. Gawlitza and H. Seidl, "Abstract interpretation over zones without widening," in *Second international workshop on invariant generation, WING 2009, York, UK, March 29, 2009 and third international workshop on invariant generation, WING 2010, Edinburgh, UK, July 21, 2010*, 2010, vol. 1, pp. 12–43.

[3] T. M. Gawlitza, H. Seidl, A. Adjé, S. Gaubert, and E. Goubault, "Abstract interpretation meets convex optimization," *J. Symb. Comput.*, vol. 47, no. 12, pp. 1416–1446, 2012.

[4] H. Seidl, T. M. Gawlitza, and M. S. Schwarz, "Parametric strategy iteration," in *6th international symposium on symbolic computation in software science, SCSS 2014, Gammarth, La Marsa, Tunisia, December 7-8, 2014*, 2014, vol. 30, pp. 62–76.

1.7 Formally-Correct Control of Autonomous Vehicles

Silvia Magdici (silvia.magdici@tum.de)
Supervisor/s: Prof. Dr.-Ing. Matthias Althoff

Autonomous vehicles are expected to provide a broad range of benefits comparedto human-driven vehicles. Among them are increased road safety and mobilityfor disabled people, and better traffic throughput. However, in order to guaranteesafety, formal and certifiable control methods are required. Relevant tasks on planning and control of a single vehicle were alreadyaddressed, solved, and demonstrated in a real environment. Based on thisprevious work, this thesis addresses the problem of safe (cooperative) control ofautonomous vehicles.

In the non-cooperative case, the occupancy sets of the other traffic participants are computed such that safety can be enhanced, by considering these sets as constraints in the optimisation control problem.

The investigated methods for collaborative vehicles are safe-by-construction suchthat all traffic participants action towards the common goal, so the criticalbehaviours are avoided, and thus safe driving is ensured.Moreover, the method will ensure safe interaction with the traffic participantsoutside the cooperative block and it will be verified if the vehicles are behaving according to the traffic rules.

1.8 Analysis of Hyperproperties

Christian Müller (christian.mueller@tum.de)
Supervisor/s: Helmut Seidl

Hyperproperties, first introduced by Clarkson[1], are trace properties of systems. Both safety properties and liveness properties hold on a single execution trace of a system. There are many properties that can not be expressed using a single trace, for example noninterference and many other security-related properties.

There are several ways how hyperproperties can be verified. We define a modeling language for information flow properties of workflows with an arbitrary number of participating agents. For these workflows, we provide a verification algorithm for a higher order logic based on Hyper-LTL[2] with quantifiers over execution traces. As this logic is undecidable in general, we use a decidable fragment that is still expressive enough for interesting properties. The verification itself is done by computing an abstract weakest precondition and checking if it is satisfiable in the initial state.

For programming languages, we introduce a way of proving hyperproperties based on the programs' self-composition[3]. Our approach works in two phases: First, a self-composition of the program is constructed. Then, we analyze this self-composition using an abstract weakest precondition calculus. Similarly to the universal information flow type system of Hunt and Sands, our analysis explicitly computes the dependencies of variables in the final state on variables in the initial state. While our analysis runs in polynomial time, we prove that it never loses precision against the type system of Hunt and Sands. It may even gain extra precision by taking similarities between different branches of conditionals into account, which can be shown even on simple examples.

Both approaches leverage abstract weakest precondition calculi that can be used to find counterexamples where the property is violated. The precondition is thus able to provide insights on how the property can be violated and how to improve the system such that the property is satisfied.

[1] M. R. Clarkson and F. B. Schneider, "Hyperproperties," *Journal of Computer Security*, vol. 18, no. 6, pp. 1157–1210, 2010.

[2] M. R. Clarkson, B. Finkbeiner, M. Koleini, K. K. Micinski, M. N. Rabe, and C. Sánchez, "Temporal logics for hyperproperties," in *Principles of security and trust*, Springer, 2014, pp. 265–284.

[3] G. Barthe, P. R. D'Argenio, and T. Rezk, "Secure information flow by self-composition," in *Computer security foundations workshop, 2004. proceedings. 17th IEEE*, 2004, pp. 100–114.

1.9 Decision Procedures with Certification

Christian Neukirchen (neukirchen@tcs.ifi.lmu.de)
Supervisor/s: Prof. Martin Hofmann, PhD

Decision procedures play an important role in program verification and automated theorem proving. To be useful in practice, decision procedures need to walk a fine line between being efficient and being correct. Formally proven correct implementations are a lot of initial work, and then are hard to adapt when the decision procedure needs to be optimized or extended; in complex implementations, apparently safe optimizations often put correctness at risk.

A solution is to split the problem into two: At first, we make the decision procedure not only decide, but also emit a *certificate* of why its output is correct. Then, a second program, the *certificate checker*, will verify this certificate (given access to the same input data), and declare whether it is correct. Now, it is enough to only formally verify that the certificate checker is correct, while the decision procedure itself can be optimized and modified independently. In case an erroneous optimization yields a wrong result, it will be detected by the certificate checker. Ideally, the certificate checker is based upon simple algorithms and data structures and has low runtime and memory complexity.

In my Master's thesis[1], we have implemented this technique for the propositional mu-calculus for which no implemented certification existed as yet, by instrumenting fixpoint iteration to compute winning strategies for a corresponding parity game[2]. The computed certificates are compact and can be checked efficiently in low polynomial time by a separate routine. The approach works well, but the certificate checker has not yet been formally verified, which will be tackled as part of this thesis.

Another class of decision procedures where above approach should be fruitful are SAT solvers. Recent developments such as certificates based on *Reverse Unit Propagation* and *Resolution Asymmetric Tautology* allow both efficient computation and compact representation of UNSAT certificates[3], and are powerful enough to support techniques such as *inprocessing* which current state-of-the-art SAT solvers with conflict-driven clause learning use.

We are working on algorithms to efficiently check these certificates and will try to integrate them into the Coq theorem prover to be used as a tactic.

[1] C. Neukirchen, "Computation of winning strategies for μ-calculus by fixpoint iteration," Master thesis, Ludwig-Maximilians-Universität München, 2014.

[2] M. Hofmann, C. Neukirchen, and H. Rueß, "Certification for μ-calculus with winning strategies," in *23rd international SPIN symposium on model checking of software*, 2016.

[3] M. J. H. Heule, W. A. Hunt, Jr., and N. Wetzler, "Verifying refutations with extended resolution," in *Automated deduction – CADE-24*, vol. 7898, Springer Berlin Heidelberg, 2013, pp. 345–359.

1.10 A Formally Verified Checker of the Safe Distance Traffic Rules for Autonomous Vehicles

Albert Rizaldi (rizaldi@in.tum.de)
Supervisor/s: Prof. Dr.-Ing. Matthias Althoff

Liability is an important but rarely studied area in autonomous vehicle technology. For example, who should be held liable when a collision involving an autonomous vehicle occurs? In our previous work[1], we proposed to solve this issue by formalising vehicles' behaviours and traffic rules in Isabelle/HOL. This formalisation allows us to check formally whether an autonomous vehicle complies with traffic rules. If autonomous vehicles always comply with traffic rules, then they should not be held liable for any accident.

One of the most important traffic rules is to maintain a safe distance between a vehicle and the vehicle in front of it. The Vienna Convention on Road Traffic defines a 'safe distance' as the distance such that *a collision between vehicles can be avoided if the vehicle in front performs an emergency brake*[2]. This rule states the requirement for safe distance descriptively; there is no prescriptive expression against which a distance can be compared. This makes the process of formally checking the compliance of an autonomous vehicle's behaviour with the safe distance rule problematic.

We formalise a descriptive notion of safe distance from the Vienna Convention on Road Traffic. This formalised descriptive definition of safe distance is turned into a prescriptive one as follows:

1. identifying all possible relative positions of stopping (braking) distances;
2. selecting those positions from which a collision freedom can be deduced; and
3. reformulating these relative positions such that lower bounds of the safe distance can be obtained.

These lower bounds are then the prescriptive definition of the safe distance, and we combine them into a checker which we prove to be sound and complete.

We generate executable and formally verified checkers in SML for validating the the US Highway 101 data set from the Next Generation SIMulation (NGSIM) project as benchmark for our checkers. Our formalised prescriptive definition of *safe distance* generalises all definitions of safe distance in the literature. Not only does our work serve as a specification for autonomous vehicle manufacturers, but it could also be used to determine who is liable in court cases and for online verification of autonomous vehicles' trajectory planner.

[1] A. Rizaldi and M. Althoff, "Formalising traffic rules for accountability of autonomous vehicles," in *IEEE conference on intelligent transportation systems*, 2015, pp. 1658–1665.

[2] B. Vanholme, D. Gruyer, B. Lusetti, S. Glaser, and S. Mammar, "Highly automated driving on highways based on legal safety," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 1, pp. 333–347, 2013.

1.11 Deterministic ω-Automata and Synthesis Procedures for Temporal Logic Specifications

Salomon Sickert (sickert@in.tum.de)
Supervisor/s: Javier Esparza

It is a well known fact since the 60's[1] that logic and automata theory are closely related to each other and logical specifications can be turned into equivalent automaton representations and vice-versa. Since then two prominent related problems have been extensively studied:

First, the synthesis problem, also known as Church's problem[2], is a long standing topic of theoretical computer science. The task is to find an automaton that computes a given transformation of infinite words specified in a suitable logic. This problem has been rephrased several times and also investigated in the context of temporal logic specifications. Second, model checking, which was introduced in the early 80's[3], tests if a system modeled as an automaton fulfills a correctness specification given in a temporal logic.

For probabilistic model checking as well as the synthesis problem it is essential that the resulting automaton is deterministic and small in order to obtain fast and efficient algorithms. Recently, a novel approach was presented directly translating Linear Time Logic (LTL), a popular temporal specification language, to deterministic (generalized) Rabin automata[4]. The construction is compositional, preserves the logical structure of the formula and yields small ω-automata.

The scope of the thesis is to adapt and to extend the ideas outlined there to support different kinds of ω-automaton such as the parity and limit-deterministic automata. This step would enable the use of parity games to synthesize systems. Furthermore limit-deterministic systems with a special structure can be used for quantitative probabilistic model checking. Finally, in order to achieve the highest level of trustability in these constructions, which is necessary for software verification, the original translation as well as potentially variations of it are formalized and mechanically verified using the proof assistant Isabelle/HOL.

[1] J. Büchi, "Weak second-order arithmetic and finite automata," *Z. Math. Logik Grundlagen Math.*, vol. 6, pp. 66–92, 1960.

[2] A. Church, "Applications of recursive arithmetic to the problem of circuit synthesis," *Summaries of the Summer Institute of Symbolic Logic*, vol. I, pp. 3–50, 1957.

[3] E. A. E. Edmund M. Clarke, "Design and synthesis of synchronization skeletons using branching time temporal logic," *Logics of Programs, Lecture Notes in Computer Science*, vol. 131, pp. 52–71, 1982.

[4] J. K. Javier Esparza, "From LTL to deterministic automata: A safraless compositional approach," *CAV*, pp. 192–208, 2014.

2 RTG 1564: Imaging New Modalities (INM)

Prof. Dr.-Ing. Andreas Kolb (andreas.kolb@uni-siegen.de)
University of Siegen
http://www.grk1564.uni-siegen.de/

Imaging technologies are one of the most important cross-cutting technologies for national and international research activities, high-tech industries and information societies. This is especially true for civil security applications. Here, the primary challenge is the development of highly automated systems, which take the result of the ongoing ethical and legal discussions regarding this topic into account.

The focus of this Research Training Group is the integrated investigation of imaging sensors and data processing components for civil security systems. Regarding sensing, new imaging devices are needed in order to increase the spectral resolution in the visible range or beyond, as well as to deliver additional depth information. In comparison with classical 2D sensors, these sensors reveal new possibilities for the recognition of persons, biometrics, surveillance and material analysis. The research activities include sensor data processing as the focal point as well as sensor development and sensor data analysis. Within this scope, different data processing and information extraction concepts will be comprehensively investigated.

An important characteristic of the research topic addressed by the Research Training Group is the methodical link from image acquisition to security application, which is bridged by image data processing components. Major challenges are the orthogonality and redundancy of multimodal data and the development of new techniques to process data from new imaging sensors. Additionally, the question of data security and data integrity for new and multi-modal data is investigated.

2.1 Integrated Simulation, Evaluation and Algorithm Development for Time-of-Flight Cameras

David Bulczak (david.bulczak@uni-siegen.de)
Supervisor/s: Prof. Dr. Andreas Kolb

For approximately 15 years there has been done a lot of research in the field of *Time-of-Flight* cameras and their popularity is increasing. Nowadays the ToF technology has reached the consumer market e.g. *Microsoft Kinect* and *PMD Technologies GmbH*. Nevertheless there are are still unsolved or insufficiently solved, practice-oriented problems in this context. To name some of them: *close range effects*, *motion artifacts*, *intensity related errors*, *multipath effects*. The research of this problems is of strong scientific interest.

To allow quantitative assessments of future sensors and algorithms an integrated investigation of sensor modeling, simulation and evaluation is one major part of my research at the chair for Computer Graphics. Together with our industrial partner pmd technologies gmbh we will enhance models which will be used in an improved version of a previously developed simulator. For a given input parametrization (light source, sensor, ...) and a given 3D scene the simulator will compute the incoming light per sensor pixel so that the afore mentioned problems will be simulated properly. The simulation of multipath effects leads to global illumination problems. The entrainment of physical units will allow development of enhanced inspection methodologies of new sensor designs in electronic simulation.

The main goal of the evaluation part is the development of an evaluation framework that allows the verification of simulated results, the evaluation of sensory data and evaluation of developed algorithms to improve the data. To allow comparability of algorithms simulated and real-world test scenes will be specified that allow isolated inspection of ToF sensor problems.

In the context of algorithms the goal is to develop robust and efficient (real-time) techniques that improve the data quality through reducing or resolving the afore mentioned problems. Through simulation and evaluation we can evaluate already published approaches and investigate how they can be realized and improved in context of pmd technologies gmbh hardware. The efficient implementation of these developed algorithms on GPUs will a further part of my work.

2.2 Dynamic Light Fields

Andreas Görlitz (andreas.goerlitz@uni-siegen.de)
Supervisor/s: Prof. Dr.-Ing. Andreas Kolb

The bidirectional reflectance distribution function (BRDF) describes the reflectance of light of a surface. This material property is used a.o. in computer graphics in physically based rendering (PBR) methods to increase the photorealism of rendered scenes.

Although there are common BRDF datasets, such as the MERL BRDF dataset[1], none of these databases provides the precise specifications of the used materials. Indeed this data is needed e.g. to evaluate a particular PBR method by creating a Cornell box scene out of these materials, and compare this real world scene with the rendered data.

To meet this need we measured the BRDF of six different materials in R, G, B and infra-red spectra and provide additionally the specifications of the used materials. To demonstrate the use of these measured BRDFs we developed a PBR renderer based on reflective shadow maps (RSM)[2] and a Cornell box scene of the measured materials.

[1] W. Matusik, H. Pfister, M. Brand, and L. McMillan, "A data-driven reflectance model," *ACM Transactions on Graphics*, vol. 22, no. 3, pp. 759–769, Jul. 2003.

[2] C. Dachsbacher and M. Stamminger, "Reflective shadow maps," in *Proceedings of the 2005 symposium on Interactive 3D graphics and games*, 2005, pp. 203–231.

2.3 Understanding of Object and Image Features at Human Perceptual Level

Ha Mai Lan (hamailan@informatik.uni-siegen.de)
Supervisor/s: Prof. Volker Blanz

Our motivation is to enable computers to see and understand images as humans do. We are investigating features that are familiar to human perception in order to model objects and images. These features are related to shape, contours, colour, texture and structure. A better way of representing objects and scenes can lead to significant improvements in many computer vision applications such as object detection, recognition, matching and classification to name a few.

Our current research is focused on finding a reliable method to establish correspondences between images at different resolutions. Instead of using point features, e.g. patch descriptors, we use open curve features and their structures to model objects. The advantages are the invariance across different resolutions, better tolerance over noise and lighting changes. We also expect that curves and their structure are able to model perceptual features better and improve matching performance. After all, one can more easily recognise objects from sketches than a bundle of small image patches.

Similar to descriptor matching approaches, we propose a 2-phase method for matching curves of objects between two different image resolutions. The two phases are pair-wise curve matching and set curve matching.

- In pair-wise curve matching, the method compares individual pairs of open curves in two images using normals along the curves. For each pair, one curve can match with a subset of the other curve. This allows the flexibility for matching curves at different scales. Our method is used for images that are not only different in resolution and framing, but also slightly variant in viewpoint.
- In phase two, we use the relative spatial relationships of curves in each image as a global spatial constraint to match two sets of curves. The method performs RANSAC and confidence voting to find the correct homography between the two sets of curves.

Our preliminary results show that the proposed methods are promising. Our methods can be applied to many applications such as image retrieval across different resolutions, multimodal image retrieval (e.g. image retrieval from sketches), image super resolution, pre-processing for optical flow algorithms.

2.4 Detection and Recognition of Articulating Objects Using Distinctive Feature Sets

Jens Hedrich (jenshedrich@uni-koblenz.de)
Supervisor/s: Prof. Dr. Marcin Grzegorzek, Prof. Dr. Andreas Kolb, Prof. Dr. Dietrich Paulus

The objective of the proposed dissertation topic is to detect and recognise articulating objects, by using distinctive feature sets of the objects partitions. The to be defined and generated feature sets need to have a sufficient discriminatory power for solving such a multi-class labeling problem. A comprehensive description of articulating objects will be outlined, upon which the representational needs over different perception domains have to be deliberated, namely in depth, color, and motion. It is assumed that each articulating object has at least one key feature which is consistent over a certain number of observation views and its articulated motion (e.g. the head shoulder contour in the application of recognising pedestrians). In order to elaborate this research topic three major steps constitute the scientific contribution. First, segmenting and clustering over the given perception domains (RGB-D). Secondly, based on the clustered segments, feature transform descriptors are used to generate key features out of the local minima of an object partition. These key features will be used in conjunction with a state of the art machine learning approach (such as latent-SVM or a bag-of-feature approach). To generate key features of object partitions, prior knowledge is given though labeled databases, which also encodes the region of interest of the object partitions. Once a set of key features is generated for partitions of an object category, the features can be used independently from each other within the underlying perception domain for re-recognising the specific object. Thirdly, the generated key features will be tested on publicly available databases to demonstrate the universal discriminatory power. For this recognition evaluation the sampling density, given though RGB-D and motion, is not mandatory.

In conclusion this research work will investigate the hypothesis that the discriminatory power of key features of articulating objects can be enhanced if a feature describes an object from its shape interior. It is assumed that the center of a shape interior can be approximated by investigating a dense grid of local minima (super-pixels).

2.5 Compressive Sensing for Photonic Mixer Device

Miguel Heredia Conde (heredia@zess.uni-siegen.de)
Supervisor/s: Prof. Otmar Loffeld, Prof. Andreas Kolb

The aim of this work is to overcome the main limitations of PMD-based ToF technology and offer images with higher lateral resolution and depth accuracy applying Compressed Sensing (CS) techniques, which rely on the idea that a signal can be exactly recovered from few measurements if it admits a sparse representation in a certain domain. A realistic sensing model is a necessary condition for successful CS-recovery. We have presented an accurate characterization of the spatial response of PMD pixels with micrometer resolution[1]. The responses are given both in 2D spatial domain and 3D, adding the phase shift between incoming light and reference as third dimension. Expanding the concept of spatial response to areas covering several pixels, cross-responses between closely-located pixels can be obtained and used to model systematic crosstalk effects between PMD pixels. This way, we have obtained an accurate characterization of crosstalk for PMD pixels[2] and used it for crosstalk compensation of PMD raw data through deconvolution.

A critical element of any ToF sensor is the illumination system. LEDs are an economic alternative to laser, still allowing for Megahertz frequencies. Unfortunately, the non-negligible asymmetric rising and falling times of LEDs produce a neither square nor sinusoidal illumination signal, which is responsible for systematic depth errors. Evaluating the quality of an illumination system is a time-consuming task, requiring a fast photodiode and an oscilloscope.

We use CS for recovering periodic illumination signals in the frequency domain from few correlation measurements gathered by a single PMD pixel applying CS. When the approach is applied to all pixels in a PMD chip, it allows for an accurate evaluation of the illumination system[3], equivalent to having the same number of fast photodiodes as pixels in the array (e.g., 19200 in a 19k chip), uniformly distributed over the illuminated area and gathering data simultaneously.

Current work focuses on modifying the PMD frontend, in order to allow correlation against pseudorandom binary codes and recover several frequencies of a single periodic and non-sinusoidal illumination signal.

[1] M. Heredia Conde, K. Hartmann, and O. Loffeld, "Subpixel spatial response of PMD pixels," in *Imaging Systems and Techniques (IST), 2014 IEEE International Conference on*, 2014, pp. 297–302.

[2] M. Heredia Conde, K. Hartmann, and O. Loffeld, "Crosstalk characterization of PMD pixels using the spatial response function at subpixel level," in *IS&T/SPIE Electronic Imaging, Three-Dimensional Image Processing, Measurement (3DIPM), and Applications*, 2015.

[3] M. Heredia Conde, K. Hartmann, and O. Loffeld, "Turning a ToF camera into an illumination tester: Multichannel waveform recovery from few measurements using compressed sensing," in *3D Imaging (IC3D), 2014 International Conference on*, 2014.

2.6 High-Quality Online Scene Reconstruction

Markus Kluge (markus.kluge@uni-siegen.de)
Supervisor/s: Prof. Dr. Andreas Kolb

The reconstruction of the environment is an important element of various applications, e.g. security systems in the context of scene observations. In order to satisfy the requirements of highly variable scenes, it is necessary to capture the scene using different sensor systems. Color data is useful to describe the appearance of objects in the scene, whereas depth data is preferable in order to reconstruct an object's shape. Therefore, the aim of this work is the research of robust and real-time capable methods for spatial/temporal sensor-data fusion. Many approaches for real-time reconstructions using a moving RGB-D camera focus on an accurate capturing of the object's geometry, whereas the reconstruction of an object's appearance often suffers from visual artifacts, e.g. blurring and ghosting. Existing approaches for improving color reconstructions mainly operate on the basis of offline methods. Therefore, this work focuses on the research of real-time capable methods that improve the quality of appearance reconstructions. For this purpose, the representation, accumulation and registration of color data as well as the mapping of color onto the geometric reconstruction need to be optimized. In order to find a suitable scene representation, the investigation of mesh based approaches is part of this work. Previous approaches are based on volumetric or point-based representations. The research of methods for representing the reflection characteristics of a surface as well as its incremental integration and accumulation is another part of this work.

2.7 Recursive State Estimation using Multiple Sensors

Lukas Köping (lukas.koeping@uni-siegen.de)
Supervisor/s: Prof. Dr. Marcin Grzegorzek

Many applications require the estimation of states that are not directly observable by any sensor. These hidden states can be estimated over time with the help of multiple sensors. This process is called recursive state estimation and mainly consists of two parts. Firstly, the state transition models the probability of moving from one state to the next state during one time step, and secondly the evaluation models the probability of a state given current sensor readings. Within this second part, the data of different sensors can be fused to gather information, that would not be available if only a single sensor alone would be used. In the current state of our research we are using particle filters as realisation of the recursive state estimation. Particle filters approximate the probability density of the state space with the help of weighted samples (particles).

Indoor localisation is a typical example of a state estimation problem, since it is not possible to directly observe the pedestrian's position within buildings with any kind of sensor. While in outdoor areas positions can be easily found using GPS, its signals are too weak to be measurable within buildings. Instead we fuse the information of many different sensors to estimate the user's position. For this we make use of sensors that are already provided by smartphones or that can be accessed by smartphones like signal-information of Wi-Fi or iBeacons.

Our contributions to this field are twofold: State-of-the-art methods are not able to update the system at arbitrary times because they assume a linear movement between two points in time. We provide a new state transition that models the pedestrian's movement within buildings based on random walks on graphs. This makes it possible to update the density estimation at arbitrary times. Also, current methods assume that the position of the phone is fixed during the whole localisation process. Our approach relaxes this assumption by providing a statistical model that is capable to detect changes of the smartphone's position. Because sensor readings during the phone's position change are heavily erroneous, these measurements should not be used as information for a heading change. Our model identifies the change of the phone's position using Principal Component Analysis and utilises this information within the von Mises distribution to neglect these sensor readings. In consequence, we provide a method that can automatically detect faulty measurements[1].

In our future work we will apply the developed methods to activity recognition and multimodal scene analysis.

[1] F. Ebner, T. Fetzer, L. Köping, M. Grzegorzek, and F. Deinzer, "Multi sensor 3D indoor localisation," in *Indoor Positioning and Indoor Navigation (IPIN), 2015 International Conference on*, 2015, pp. 1–11.

2.8 Registration and Analysis of Multimodal Datastreams in Raman- and Infrared Microspectroscopy

Christoph Pomrehn (christoph.pomrehn@inf.h-brs.de)
Supervisor/s: Prof. Dr.-Ing Rainer Herpers, Prof. Dr.-Ing. Andreas Kolb

Raman- and Infrared-Spectroscopy are vibrational spectroscopic methods which are used to identify the molecular structure of materials. Monomodal variants of these approaches are widely used in several fields of research[1]. For microspectroscopic devices, both measuring concepts provide a set of hyperspectral data, which contains information respective specific molecular vibrations. Furthermore, the acquired data can spatially be assigned to positions in corresponding microscopic images. Thus, an analysis of the hyperspectral datasets enables a spatially-resolved identification of the investigated Raman- or Infrared-active material. In theory, the complementary nature of both spectroscopic approaches leads to hyperspectral datasets which contain complementary information. That would enable a general extension of the spectral feature space due to a common multimodal data processing. Thus, the analysis of datastreams from two spectroscopic modalities provides the potential of a more robust and clearer identification process in material sciences.

Due to the significant difference in the spatial resolution of the two spectroscopic approaches, a multimodal data processing necessitates a registration of the corresponding datasets. Following a successful data registration, the complementary data sets will be analyzed with the intention of substance identification and localization. Therefore, the extension of the spectral feature space requires methods for multimodal feature extraction which emphasize relevant spectral information and disregard redundancy. Additional objectives are a qualified visualization of the results and a successful practical application in the field of food science or civil security.

This project is researched at Bonn-Rhein-Sieg University of Applied Sciences, that participates in this RTG.

[1] B. Schrader, *Infrared and raman spectroscopy: Methods and applications.* John Wiley & Sons, 2008.

2.9 Pulse-Based TOF range sensing

Hamed Sarbolandi (hamed.sarbolandi@uni-siegen.de)
Supervisor/s: Prof. Andreas Kolb

In the past decade, the contribution to the self driving cars is growing exponentially. Using gestures to interact with the navigation systems is already utilized by some of the automotive companies. For these applications reliable optical sensors are needed to observe the surrounding of the car by measuring the distance to upcoming objects. For this radar or lidar object detection systems, time of flight cameras (ToF) or conventional CCD cameras can be used. CCD cameras do not deliver any distance information, nevertheless they can be useful if object shapes are detected using image processing algorithms. Radar and lidar systems have only one receiver and must use a mechanical system to fan out their visible range. The photo receiver of ToF cameras holds a grid of pixels that are able to measure the time of flight. Hence they are able to capture several two dimensional distance images per second. ToF cameras can be used in near and far range. This makes them useful for a wide field of applications in and outside the car. Cameras optimized for inside could help to detect gestures, track the passengers positions for intelligent safety systems and prevent car theft by observing the interior when the car is parked. Outward cameras can help to increase safety by observing the surrounding of the car. They help to keep track of the lane, the distance to other vehicles and can detect pedestrians and upcoming objects.

Different ToF camera methods and implementations are existing, but for an application in the automotive environment an accurate, reliable, eye-save and energy efficient system is required. The goal of this project is to evaluate a pulse based ToF camera prototype that and find a suitable distance calibration.

2.10 Face and Scene Understanding

Davoud Shahlaei (davoud.shahlaei@uni-siegen.de)
Supervisor/s: Volker Blanz, Marcin Grzegorzek

Realistic inverse lighting from single 2D facial image is a difficult inverse problem with many unknowns; the face shape, reflectance and imaging conditions are not given. First, we estimate the 3D face model and albedo from the input image, using a 3D Morphable Model. Next, we take the estimated 3D shape and generate a gallery of images of that face under a virtual light stage, thereby an average human face albedo and reflectance is used for rendering. Then, based on the superposition principle for light, we estimate the light source intensities as optimized non-negative coefficients for a linear combination of the gallery images of that face. Each image of the gallery is lighted by a directional light source and rendered with a non-lambertian reflectance and non-convex geometry. Therefore, the estimated RGB coefficents for each gallery image provide the intensity and color of the fixed light source from the virtual light stage that is used to render that gallery image. The estimation is done with a regularized non-negative least squares optimization approach. The input image can be reconstructed by accepting the estimated coefficients as the weights for linear combination of the gallery images, or alternatively, by accepting the estimated coefficients as RGB values for corresponding light sources of the virtual light stage.

Our algorithm maintains a good color management and works better than previous work on face images with complex lighting. As a result, it is possible to de-illuminate the input image, re-illuminate faces given in images, add objects to the seen, while preserving the physically plausible lighting. We show that lighting can be swapped between two input images or apply the lighting from one image to other faces. See[1] and[2].

[1] D. Shahlaei and V. Blanz, "Realistic inverse lighting from a single 2D image of a face, taken under unknown and complex lighting," in *Automatic face and gesture recognition (FG), 2015 11th IEEE international conference on*, 2015, pp. 1–8.

[2] M. Heredia Conde, D. Shahlaei, V. Blanz, and O. Loffeld, "Efficient and robust inverse lighting of a single face image using compressive sensing," in *The IEEE International Conference on Computer Vision (ICCV) Workshops*, 2015.

2.11 Active Multispectral SWIR Imaging for Skin Detection and Face Verification

Holger Steiner (holger.steiner@h-brs.de)
Supervisor/s: Prof. Dr. Andreas Kolb / Prof. Dr. Volker Blanz

The detection of human skin in images is a very desirable feature for safety or security applications: at robot workplaces or manually-fed machines, the detection and tracking of persons and limbs can help to prevent accidents, while face detection and recognition is becoming more frequently used in different biometric application scenarios. However, distinguishing real skin from other materials based on imagery captured in the visual spectrum alone can be very difficult and unreliable[1]. Therefore, spoofing attacks with facial disguises or masks are a serious problem for state of the art face recognition algorithms[2].

This work presents a novel approach for reliable skin detection based on spectral remission properties in the short-wave infrared (SWIR) spectrum and proposes a cross-modal method that enhances existing solutions for face verification to ensure the authenticity of a face even in the presence of partial disguises or masks. Furthermore, it presents a reference design and the necessary building blocks for an active multispectral camera system that implements this approach, as well as an in-depth evaluation.

The described system acquires four-band multispectral images within 50ms. Using an SVM-based classifier, it achieves unprecedented skin detection accuracy, even in the presence of skin-like materials used for spoofing attacks. Paired with a commercial face recognition software, the system successfully rejected all evaluated attempts to counterfeit a foreign face.

[1] H. Steiner, O. Schwaneberg, and N. Jung, "Advances in active near-infrared sensor systems for material classification," in *Imaging systems and applications*, 2012, p. ITu2C.2.

[2] H. Steiner, S. Sporrer, A. Kolb, and N. Jung, "Design of an active multispectral SWIR camera system for skin detection and face verification," *Journal of Sensors*, vol. 2016, no. 1, 2016.

3 RTG 1651: Service-oriented Architectures for the Integration of Software-based Processes, exemplified by Health Care Systems and Medical Technology (SOAMED)

Prof. Dr. Ulf Leser (leser@informatik.hu-berlin.de)
Humboldt-Universität zu Berlin, Technische Universität zu Berlin,
Charite Universitätsmedizin Berlin, Hasso-Plattner-Institut an der Universität Potsdam
http://www.informatik.hu-berlin.de/de/forschung/gebiete/soamed

Service orientation is a promising architectural concept to quickly and cost-efficiently couple autonomous software components to support IT processes, and to be able to flexibly adapt processes to new requirements. Service orientation as a development paradigm has evolved from pragmatic solutions to practical problems; limited attention has been given to its theoretical and conceptual foundation. A particular promising domain for SOA is the area of health care. Compared to other domains, IT processes in the health care domain are more versatile, reliability and correctness requirements are higher, the participating partners are more heterogeneous, and processes are running for a longer period of time. Methods for the versatile, secure, and efficient integration of services in the medical domain are thus in urgent need. In its first phase the graduate school SOAMED developed concepts, methods and tools that underpin service-orientation with conceptual and theoretical foundations. We focused on topics such as process orchestration, process monitoring, process modelling, and privacy and trust in SOA. All PhD students studied current and concrete problems within the health care domain as use case scenarios to ensure applicability of their conceptual SOA-related results even in this difficult area.

In its second phase, SOAMED-2 continues these successful lines of research, but it also undertakes some notable changes. Most importantly, we extended the range of research questions to include also data analysis processes and we (a) focus more on interacting processes between multiple organizations and (b) pay more attention to privacy requirements in SOA.

3.1 Action Refinement for Dynamic Event Structures

Paul-David Brodmann (p.brodmann@tu-berlin.de)
Supervisor/s: Uwe Nestmann

Prime event structures as presented by Winskel in[1] have been extensively studied. They have proven to be well suited to model concurrent systems. In[2] Van Glabbeek and Goltz discuss action refinement for prime event structures and other flavors of event structures. They argue that action refinement enables a top down system specification which is widely used in software engineering.

In[3] Arbach et al. present an extension to prime event structures that allows dynamic creation and deletion of action dependencies. This extension is concise jet expressive enough to model real world work-flows.

We combine these two extensions, namely action refinement and dynamic creation/deletion of dependencies. Yet we take a more detailed approach than Van Glabbeek and Goltz. We add an interface to events that are to be refined. This interface allows us to specify how the refinement should interact with the abstract system. We now can use a top down approach to model systems and maintain different abstraction layers. Additionally we keep the expressiveness and simplicity of dynamic event structures.

[1] G. Winskel, "Events in computation," PhD thesis, University of Edinburgh, 1980.

[2] R. van Glabbeek and U. Goltz, "Refinement of actions and equivalence notions for concurrent systems," *Acta Informatica*, vol. 37, no. 4, pp. 229–327.

[3] Y. Arbach, D. Karcher, K. Peters, and U. Nestmann, "Dynamic causality in event structures," in *Formal techniques for distributed objects, components, and systems: 35th IFIP WG 6.1 international conference, FORTE 2015, held as part of the 10th international federated conference on distributed computing techniques, DisCoTec 2015, Grenoble, France, June 2-4, 2015, Proceedings*, 2015, pp. 83–97.

3.2 Data Flow Control in Scientific Workflow Systems

Wladislaw Gusew (gusewwla@informatik.hu-berlin.de)
Supervisor/s: Prof. Dr. Björn Scheuermann

Research in scientific fields, like, for instance, medical sciences, computer sciences, engineering, or natural sciences is often conducted by evaluating large quantities of measured and collected data. In many cases, processing of data is subdivided into several steps, each performing computations regarding specific aspects. These steps are components of the overall process of transforming raw data into the required results.

Scientific workflows are a formalization of such a process and enable compositions of individual steps which are represented by *tasks*. A common representation of a workflow is a *directed acyclic graph* where nodes correspond to tasks, while edges define the data dependencies between these tasks. In contrast to business workflows which often focus on the flow-control, scientific workflows are data flow oriented and process large amounts of heterogeneous data. Hence, scientific workflows can become computationally intensive so that reasonable total runtimes can only be achieved by exploiting parallelism and executing on distributed resources. Research in this domain has induced the development of several *Scientific Workflow Management Systems* (SWfMS), including Kepler, Pegasus, and Taverna.

An essential part of SWfMS is the execution of workflows on distributed systems, like, for instance, grids, computing clusters, or a cloud environment. There, the scheduling strategies depend on the network properties of the system in use, determined by the topology, heterogeneity, and communication protocols. We investigate the effects of these parameters on the total runtime of a workflow and the utilization of resources, and develop techniques in order to optimize the performance. We consider two ways to realize this: firstly by adjusting the scheduling algorithm for distributing workflow tasks and the corresponding data during runtime, and secondly by adapting the network properties to an optimal configuration during the execution. The latter method can be applied by employing the recently emerged paradigm of *Software-Defined Networking* (SDN).

With SDN, a central controller manages all data routing decisions of network devices, such as routers and switches. By dynamically changing data routes with a central instance, the entire network becomes programmable. We investigate methods to algorithmically adjust scheduling of scientific workflow tasks in order to improve the overall performance.

3.3 Process Information and Guidance Systems for Medical Treatments in Hospitals

Marcin Hewelt (hewelt@soamed.de)
Supervisor/s: Prof. Dr. Mathias Weske, Prof. Dr. Uwe Nestmann

Doctors, nurses, and health care professionals interact in various hospital processes to provide effective and efficient treatment to patients. Besides disease-specific knowledge captured in clinical practice guidelines (CPG), hospitals employ organizational processes, like patient admission, and standard operating procedures (SOP). The treatment of a single patient hence is based on a variety of processes, which are selected during runtime and contribute to the overall treatment case. This is especially true considering multi-morbid patients, for whom multiple CPGs apply.

Existing IT systems in hospitals are not process-oriented. Business Process Management (BPM) could help in this regard, however, classical BPM approaches fail to address integrated execution of multiple process models. Therefore, my dissertation explores a new approach for IT-supported case enactment. The aim of the Process Information and Guidance System approach is twofold: 1) to monitor running treatment cases, and 2) to recommend treatment steps based on patient data, treatment history and process models. As many actors and processes are involved in a treatment case, I expect that an overview of the treatment history, i.e. who has done what, when, and to what result, eases communication about the patient and coordination of the treatment. At the same time the further treatment of the patient needs to be planned. Therefore, I aim to provide guidance to medical practitioners, by recommending those activities that are advised by CPGs, SOPs, and organizational processes for a particular patient. Because the approach takes into account multiple process models for one treatment case, it needs to consider redundant as well as contradicting activities when recommending treatment steps. Both visualization and recommendations are based on a formal representation of the treatment case as a partial order of events.

3.4 Seamless Failover and Recovery of Stateful Services using Optimistic Replication

Tim Jungnickel (tim.jungnickel@tu-berlin.de)
Supervisor/s: Odej Kao

Since all modern enterprises rely on IT services to operate well, the availability of the services is crucial. Unfortunately, a wide range of possible failures is constantly threatening the availability. Since not all threats cannot be avoided, the services needs to be prepared to face the failures. In this thesis we introduce a novel approach to preserve the availability of stateful services by relaxing the consistency for the time in which failures are present.

According to the CAP theorem, it is impossible in a distributed system to simultaneously provide all three guarantees: consistency, availability and partition tolerance[1]. Hence the availability needs to be traded against consistency or partition tolerance. Unfortunately, most services expect strong consistency. One common solution is failure masquerading i.e., in case of a failure, the functionality of the service is reduced to avoid inconsistencies.

In contrast to failure masquerading, within our approach full functionality is preserved. Instead of reducing the functionality, we temporarily reduce the strength of the consistency. We use the guarantees of optimistic replication mechanisms to regain a consistent state after all (possible conflicting) changes of the failing components are recovered.

To show the validity of our approach, we develop various example services with the support of a seamless failover and recovery. We perform experiments and show that we are able to perform a seamless failover and regain a consistent state after all recovered changes are synchronized.

[1] S. Gilbert and N. Lynch, "Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services," *SIGACT News*, vol. 33, no. 2, pp. 51–59, 2002.

3.5 Verification of Hybrid Systems in the Medical Context

Timm Liebrenz (liebrenz@soamed.de)
Supervisor/s: Prof. Sabine Glesner

In the medical context, we often find hybrid systems that are used in safety critical areas. Hybrid systems contain continuous parts, which can be described by differential equations, and discrete parts, which describe the control behavior of the system. Medical devices often interact with the physical environment and show hybrid behavior, e.g., when concentrations of infusions are calculated with differential equations that are dependent on a control mode. The correctness of such devices is particularly important, because faulty behavior can threaten human lives. There exist various analysis and verification approaches for hybrid systems, however limited scalability poses still a major challenge and limits their applicability to complex systems.

When performing formal verification of large systems, the state space explosion often hampers or even prevents an efficient verification. Furthermore, systems that have a hybrid character cause additional challenges, it is necessary to handle the continuous and discrete system behavior as well as their interaction in the verification. To enable the verification of safety critical properties, it is necessary to reduce the complexity of the system.

We propose an approach to tackle the verification of hybrid systems. We aim to slice a system into services. In our representation, a service contains elements of the system that perform a functional task, and input and output interfaces that are used to communicate with other system parts. We analyze each service and enable the verification of properties by automatically transforming a service into an input representation of a hybrid verification tool and therefore are able to handle the hybrid character of the services. With the use of a verification tool, we intend to enable a semi-automatic verification of properties for individual services. Furthermore, we use the gathered information to generate contracts for each individual service to establish a connection between their input and output data. With proven properties of individual services, we will be able to infer properties of the whole system. To this end, we use the generated contract information and the underlying system logic to verify properties about the interplay of all services of the system. To enable reuse of already proven properties, we store the corresponding information about services. During service slicing, this information can be used to create services more efficiently and the verification process can be accelerated by using already proven properties.

Our approach enables a scalable, semi-automatic verification of hybrid systems. This can be used to ensure the correctness of systems that are used in safety critical areas, like devices in medical context.

3.6 RESTful Business Process Choreographies

Adriatikj Nikaj (nikaj@soamed.de)
Supervisor/s: Prof. Dr. Mathias Weske

Today, enterprises are increasingly exchanging information and services to meet the customers' complex demands. Business processes are used to organize enterprises internal work with the help of the so called business process engines. These engines are responsible for the implementation of the modeled business processes. However, less attention is payed to the interactions between enterprises and their implementation. In my research, I address this research gap by introducing an intermediate modeling language which serves as a vessel for deriving implementation-based information from interaction models. More specifically, starting from a BPMN business process choreography, a standard specification language for modeling interactions, I derive a RESTful choreography, a specification language for modeling REST-based interactions. RESTful choreography, is an adaptation of BPMN process choreography to model RESTful interactions. Furthermore, a systemic semi-automatic method is introduced for deriving a RESTful choreography from a business process choreography. The purpose of this method is to achieve a greater separation of concerns between the business process modeler and the REST expert responsible for the implementation. RESTful choreography is also equipped with formal correctness properties which allows automatic verification. Future work include the evaluation of such a specification language with respect to its usefulness to REST implementers.

3.7 Distributed multidimensional Index Structures for Genomic Data

Stefan Sprenger (sprengsz@informatik.hu-berlin.de)
Supervisor/s: Prof. Dr. Ulf Leser

In the early 2000s, DNA sequencing experienced a game-changing innovation: new sequencing technologies, called Next-Generation Sequencing (NGS), were invented. NGS allows faster and way more efficient sequencing of genomes and achieves higher throughput compared to older technologies like Sanger sequencing, i.e., it sequences much more parts of a genome per run resulting in larger output data[1]. NGS technology is steadily improving month by month resulting in lower sequencing cost, higher throughput and even more output data that need to be analyzed. Since 2005 sequencing cost is halving every 5 months resulting in a growing number of sequenced genomes[2].

In the last years, NGS was used in many studies and projects like the 1000 Genomes Project[3] to sequence whole human genomes. Today, large databases of genetic variations and tools like genome browsers exist that can be used by researchers to analyze and visualize genomic data for basic research or translational medicine. In most cases, such analysis is conducted in an explorative manner, i.e., researchers interactively navigate through visualizations of sets of genomes to explore variations and their correlations to certain phenotypes. Though modern genome visualization tools provide basic interactive analysis processes, they lack the support for a "near real-time" search on large data. Taking the growing size and complexity of to-be-considered data into account, these analysis tools become the limiting factor in genomic research[4].

In this dissertation, a distributed multidimensional index structure is devised that can be used by tools like genome browsers to search a large amount of genomic data in "near real-time". It is tailored to genomic data, i.e., only certain query types, e.g., point, range and aggregation, are supported. We especially focus on storing the index structure in main-memory and exploit the architecture of modern CPUs, i.e., we take parameters like cache (line) size into account, in order to achieve efficient query execution and provide interactive search.

[1] E. R. Mardis, "The impact of next-generation sequencing technology on genetics," *Trends in genetics*, vol. 24, no. 3, pp. 133–141, 2008.
[2] L. D. Stein and others, "The case for cloud computing in genome informatics," *Genome Biol*, vol. 11, no. 5, p. 207, 2010.
[3] 1. G. P. Consortium and others, "A map of human genome variation from population-scale sequencing," *Nature*, vol. 467, no. 7319, pp. 1061–1073, 2010.
[4] V. Marx, "Biology: The big challenges of big data," *Nature*, vol. 498, no. 7453, pp. 255–260, 2013.

3.8 Shared Data in Communicating Business Processes

Marvin Triebel (triebel@hu-berlin.de)
Supervisor/s: Prof. Dr. Wolfgang Reisig

Business process modeling has become a popular tool for the design, management and analysis of information systems and organizations such as hospitals. However, most modeling techniques focus around the control flow and the communication between the agents participating in a business process. Other aspects of business operations such as data integrity are ignored or remain only implicit in the control flow. However, in real-world processes, the control flow is intertwined inherently with the data operations. Moreover, the evolution of data over time is a core aspect of an organization and may reflect most of its business value.

In our research, we focus on a technique to jointly model and analyze data- and control-flow aspects of business processes. To this end, we assume that agents operate on a shared database and in parallel communicate to each other.

Consider a patient transfer process between hospitals as an example: Each hospital can be modeled as an agent of the process. The patient transfer process models the transport of patients from one location to another: The process starts with a request from one location. The request may be denied, i.e. due to capacity restrictions or due to an operational interruption like illness of employees. If the request is accepted, the actual transfer is performed. The locations of all patients are managed in a shared database. Thus, the fate of the process strongly depends on the values in the database. Furthermore, the transfer has to be protocolled in the database. Every transfer process hence consists of two parts: First, the communication between the agents and, second, the manipulation of the shared data. In our modeling approach, we want to reflect both aspects to emphasize the interdependence.

There exist several techniques that focus on communication and abstract from data such as Service Nets (Petri nets with interfaces). On the other hand, there are techniques that focus on data and restrict communication such as data-centric dynamic systems. As the example suggests, for many applications communication and data manipulation are interdependent and describing them in separate models cannot reveal errors caused by interdependence. Therefore, it is worthwhile to study combined modeling techniques.

3.9 Congestion Control for Routing Overlays

Florian Tschorsch (tschorsch@informatik.hu-berlin.de)
Supervisor/s: Prof. Dr. Björn Scheuermann

Distributed services and their requirements become more complex. Advanced services lead away from simple direct communication between end systems. To this end, additional end systems, which act as intermediaries and augment application protocols are introduced Middlewares, especially grid and anonymity networks, are an example for such services. Technically they are realized as overlays, i.e., they add another instance of routing and transport functionality on top of the protocol stack. However, there are little insights into how to design the overlay in such a way that it makes efficient and proper use of network resources. Particularly, congestion control is challenging.

There it is tempting to take up concepts from the Internet counterparts. As we revealed in our research an unreflected reuse incurs multiple side effects. Aware of the broad design space and its existing pitfalls, this thesis intends to provide an integral perspective on performance aspects of transport in routing overlays. In particular, we are interested in the interrelations between underlay transport, transmission scheduling, and overlay transport, with respect to throughput, latency, and fairness. Since services often transport sensitive data, privacy and security aspects need to be considered as well.

Based on these insights we envision a tailored solution, which we call BackTap: Backpressure-based Transport Protocol. Through per-hop flow control, we allow the upstream node to control its sending behavior according to variations in the queue size of the respective downstream node. The result is backpressure that propagates towards the source if a bottleneck is encountered. In packet level simulations we confirmed the expected improvement of BackTap.

4 RTG 1763: QuantLA - Quantitative Logics and Automata

Franz Baader (baader@tcs.inf.tu-dresden.de)
TU Dresden and Universität Leipzig
http://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, natural language processing, or the design of XML technology. 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 processing of tree-structured data.

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 softskills courses offered by the participating universities.

4.1 Automatic Extraction of Matrix-based Language Models

Shima Asaadi (shima.asaadi@tu-dresden.de)
Supervisor/s: 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 its variations are prominently used in information retrieval, sentiment analysis and other fields of natural language processing (NLP). In the application of meaning representation of text in NLP, vector-space models embody the distributional hypothesis of meaning, according to which the meaning of words is defined by contexts in which they (co-)occur. However, until recently, little attention has been paid to the task of modeling complex conceptual text structures (e.g. sentence) with such models, which constitutes a barrier for semantic vector models.

In 2010, Rudolph and Giesbrecht[1] proposed a novel quantitative language model based on matrix multiplication for the meaning representation of complex texts. They showed that this model subsumes many of known models, both quantitative (vector-space models) and qualitative (regular languages). Although this framework has been shown to be a theoretically elegant way to model composition and represent compositional aspects of language, training such models has to be done carefully. Initial attempts with mixed results have been made by some other researchers, such as Yessenalina[2] as well as Socher[3], but only for rather small examples and under certain assumptions.

On the other hand, many tasks in NLP or learning models of the environment require estimating functions mapping variable length sequences (sentences) to real numbers. A broad class of such functions can be defined by weighted automata.

The idea in this work is to develop appropriate learning methods, which allow to automatically learn such matrix-based models of language from given training data such as linguistic corpora. We investigate if and how novel methods for learning weighted automata[4] can be applied to solve the task of meaning representation of complex text structures. These methods will have to be modified and adapted to the specific setting and interleaved with other NLP techniques such as dimensionality reduction in order to arrive at a satisfactory solution. The developed approaches will then be analyzed theoretically, concerning their computational complexity. They will also be evaluated in NLP settings, using standardized tasks from international competitions.

[1] S. Rudolph and E. Giesbrecht, "Compositional Matrix-Space Models of Language," in *Proceedings of the 48th Annual Meeting of the Association for Computational Linguistics*, 2010, pp. 907–916.

[2] A. Yessenalina and C. Cardie, "Compositional Matrix-space Models for Sentiment Analysis," in *Proceedings of the Conference on Empirical Methods in Natural Language Processing*, 2011, pp. 172–182.

[3] R. Socher, B. Huval, C. D. Manning, and A. Y. Ng, "Semantic Compositionality Through Recursive Matrix-vector Spaces," in *Proceedings of the 2012 Joint Conference on Empirical Methods in Natural Language Processing and Computational Natural Language Learning*, 2012, pp. 1201–1211.

[4] B. Balle and M. Mohri, "Learning Weighted Automata," *Algebraic Informatics, Springer International Publishing*, pp. 1–21, September 2015.

4.2 Weighted Automata and Logics on Graphs

Stefan Dück (dueck@informatik.uni-leipzig.de)
Supervisor/s: Prof. Dr. Manfred Droste, Prof. Dr.-Ing. Heiko Vogler

Recently, there has been much interest in quantitative features for the specification and analysis of systems. These features can be modeled by using quantitative automata and quantitative logics, which generalize classical automata respectively logics using weights. A result of Droste and Gastin, extending the classical result of Büchi-Elgot-Trakhtenbrot, shows that if the weights are taken from an arbitrary semiring, then quantitative automata and a syntactically defined fragment of the quantitative MSO-logic are expressively equivalent. Subsequently, many authors considered different possible extensions of this result either in generalizing the underlying models to trees, nested words, pictures or texts; or in generalizing the computation of weights from a semiring-product to a more general valuation function of a valuation monoid. It is the goal of this dissertation to investigate quantitative automata and logics, to establish a general result over graphs comprising the previous results, and to derive further structure properties of these weighted automata.

As starting point, we were able to prove a weighted version of a Büchi-like result for finite and infinite nested words with a valuation monoid as underlying weight structure, thus extending prior results for nested words. This result was published at LATA 2014[1] and a full version was accepted at *Information and Computation*[2].

In addition, we studied the connection between weighted logics and weighted automata over more general structures like graphs and the problems encountered when trying to apply some of the known techniques to this case. In this context, pictures and weighted picture automata play an important role and were studied.

Subsequently, using a semiring-weighted extension of Thomas' graph acceptors and their connection to Hanf's Lemma, we succeeded in proving a weighted version of a Büchi-like theorem and a Nivat-like theorem for graphs. These results were published at MFCS 2015[3] and are the desired generalization of the previous results to general graphs.

Finally, possible extensions using valuation monoids instead of commutative semirings were studied and yielded further results. Using an extension of Hanf's Lemma for a logic featuring an infinity-quantifier, we also answered the difficult question how to extend our results to infinite graphs[4]. Other points of interest are applications of our results to data-graphs, which are graphs over a possibly infinite alphabet.

[1] M. Droste and S. Dück, "Weighted Automata and Logics for Infinite Nested Words," in *Language and Automata Theory and Applications (LATA)*, 2014, vol. 8370, pp. 323–334.
[2] M. Droste and S. Dück, "Weighted Automata and Logics for Infinite Nested Words," *Information and Compututation*, In press.
[3] M. Droste and S. Dück, "Weighted Automata and Logics on Graphs," in *Symposium on Mathematical Foundations of Computer Science (MFCS), Part I*, 2015, vol. 9234, pp. 192–204.
[4] S. Dück, "Weighted Automata and Logics on Infinite Graphs,", Submitted.

4.3 Weighted Automata with Storage

Luisa Herrmann (luisa.herrmann@tu-dresden.de)
Supervisor/s: 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 some sets 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 to that of *K-weighted automata with storage* where K is a *unital valuation monoid*[2]. Motivated by the wish to model quantitative aspects of technical systems such as average consumption of some resource, there is a need for the ability to calculate weights in a global manner. Instead of semirings, that only handle local calculations, unital valuation monoids allow this global type of computations.

This research project has among others the following aims. We want to *compare our automata model with existing models*, e.g. by specialization. Another goal is the *theoretical investigation* of weighted automata with storage regarding their closure properties and by extending classical characterizations. Moreover we aim to *develop* this automaton model further, conceivably to structured words, trees, or graphs.

Hitherto I proved together with Heiko Vogler a *Chomsky-Schützenberger theorem* for the class of weighted languages recognizable by weighted automata with storage[3]; this was part of my master's thesis. Furthermore, Heiko Vogler, Manfred Droste and I introduced a *weighted MSO logic with storage behaviour* and proved that this logic is expressively equivalent to weighted automata with storage[4]. Moreover, we obtained that the new logic has a decidable satisfiability problem in case of n-iterated pushdown storage and a zero-sum-free commutative strong bimonoid with decidable zero generation problem.

[1] D. Scott, "Some Definitional Suggestions for Automata Theory," *Journal of Compututer and System Sciences*, vol. 1, pp. 187–212, 1967.

[2] M. Droste and H. Vogler, "The Chomsky-Schützenberger Theorem for Quantitative Context-Free Languages," in *Proc. of Developments in Language Theory 2013*, 2013, pp. 203–214, see also: *International Journal of Foundations of Computer Science* 25(8):955–969, 2014.

[3] L. Herrmann and H. Vogler, "A Chomsky-Schützenberger Theorem for Weighted Automata with Storage," in *Proc. 6th Int. Conf. on Algebraic Informatics (CAI)*, 2015, vol. 9270, pp. 115–127.

[4] H. Vogler, M. Droste, and L. Herrmann, "A Weighted MSO Logic with Storage Behaviour and its Büchi-Elgot-Trakhtenbrot Theorem," in *Proc. 10th Int. Conf. on Language and Automata Theory and Applications (LATA 2016)*, 2016, accepted for publication.

4.4 Parametrization in Probabilistic Model Checking

Lisa Hutschenreiter (lisa.hutschenreiter@tu-dresden.de)
Supervisor/s: Prof. Dr. Christel Baier, Prof. Dr. Manuel Bodirsky

A prominent technique for the fully automatic verification and quantitative analysis of probabilisitic systems against various properties is probabilistic model checking. During the last few years it has become popular to consider parameterized versions of Markovian models for specifying families of systems that have the same graph structure, but vary in the precise transition probabilities. Methods for computing rational functions as a symbolic representation of reachability probabilities and expected rewards in parametric Markov chains have been examined and implemented in the recent tools PARAM and PROPheSY among others. Techniques for the approximate analysis of parametric Markov decision processes and continuous-time Markov chains have been presented by various authors.

Despite the recent interest in parametric probabilistic models, many problems are left open. The thesis will investigate the decidability and complexity of the parameter-synthesis problem for Markovian models and weighted temporal logics, where either the model or the logic or both contain parameters. The thesis will address parametric transition probabilities and parametric reward structures in Markovian models and linear- and branching-time temporal logics with parametric reward bounds. The task of the parameter-synthesis problem is to find concrete values for the parameters such that the model satisfies a given formula. Even more challenging is the generation of compact symbolic representations, for example based on first-order or other logics, of the set of all parameter evaluations where the formula holds for the model. The existing work provides solutions for the parameter-synthesis problem for parametric Markov chains and non-parametric linear temporal logic (LTL) formulas and partial solutions for branching-time logics, such as probabilistic computation tree logic (PCTL). However, the complexity of the parameter synthesis problem for branching-time logics and parametric models is still an open problem.

First steps towards the parameter synthesis for parametric temporal logics interpreted over probabilistic models have been presented by Chakraborty and Katoen who considered a variant of LTL with parametric step bounds interpreted over non-parametric Markov chains. They also showed undecidability in general and identified decidable fragments of step-parametric LTL. The thesis will focus on other fragments of step-parametric LTL as well as parametric variants of LTL and PCTL-like branching-time logics. One idea to escape from undecidability that will be pursued is to consider properties with parametric reward bounds and fixed step bounds.

4.5 Quantitative Variants of Language Equations and their Applications to Description Logics

Pavlos Marantidis (pavlos.marantidis@tu-dresden.de)
Supervisor/s: Prof. Dr.-Ing. Franz Baader, Prof. Dr. Sebastian Rudolph

Description Logics are a family of knowledge representation languages with a formal, logic-based semantics. Often though, when creating the formal representation of the relevant knowledge of an application domain in a team of knowledge engineers, redundancies are introduced in the form of concepts that are intended to be the same, but have different (even non-equivalent) formal representations. *Unification in Description Logics* was introduced as a method for discovering such redundancies, also suggesting possible ways to remedy them by providing a unifier[1]. However, the existence of an exact unifier, which makes the concepts equivalent, is sometimes too strong a requirement for finding redundancies. To overcome this problem, we introduce *approximate unification*, which searches for concepts that can be made "similar" (with respect to a certain measure) rather than equivalent.

Unification was first considered for the description logic $\mathcal{FL}_0$ by Baader and Narendran[1]. They reduce testing for unifiability and computing unifiers to the problem of solving certain language equations. Motivated by this construction, we reduce the problem of approximate unification to approximately solving language equations with respect to some distance between languages. Currently, we have introduced two (relatively simple) such distances w.r.t. which we are exploring approximate solvability of language equations. To do this, we modify already known automata-based methods for solving language equations[2] by introducing weighted versions of them.

Afterwards, we will consider other distance measures from the formal language literature, with an emphasis on those that have a meaningful translation to description logics. It will be interesting to investigate whether and how these translations correspond to the similarity measures introduced by Andreas Ecke (QuantLA doctoral student in the first generation) in his thesis. Further work is scheduled to include approximate unification in other, more expressive description logics. Prior to this, the investigation of matching (a special case of unification) could provide some basic instructive results[3]. Finally, the addition of terminological knowledge (TBoxes) could be another direction to be considered.

[1] F. Baader and P. Narendran, "Unification of Concept Terms in Description Logics," *J. of Symbolic Computation*, vol. 31, no. 3, pp. 277–305, 2001.
[2] F. Baader and A. Okhotin, "On Language Equations with One-sided Concatenation," *Fundamenta Informaticae*, vol. 126, no. 1, pp. 1–35, 2013.
[3] F. Baader, R. Küsters, A. Borgida, and D. L. McGuinness, "Matching in Description Logics," *J. of Logic and Computation*, vol. 9, no. 3, pp. 411–447, 1999.

4.6 Arithmetic Constraint Satisfaction Problems

Antoine Mottet (antoine.mottet@tu-dresden.de)
Supervisor/s: Prof. Dr. Manuel Bodirsky, Prof. Dr. Manfred Droste

The constraint satisfaction problem CSP($\mathbb{A}$) of a relational structure $\mathbb{A}$ is the decision problem that takes as input a formula ϕ of the form $\exists x_1, \ldots, x_n. \bigwedge R_i(x_{i1}, \ldots, x_{ir_i})$ where each R_i is a relation from $\mathbb{A}$, and that asks whether ϕ is true in $\mathbb{A}$. The structure $\mathbb{A}$ is often called the *template* or the *constraint language* of the CSP. Every decision problem is polynomial-time equivalent to CSP($\mathbb{A}$) for a suitable $\mathbb{A}$[1]. While $\mathbb{A}$ can sometimes be taken to be a finite or ω-categorical structure, problems of quantitative nature are typically represented as the CSPs of non-ω-categorical templates. The long-term goal of my research project is the investigation of the complexity of constraint satisfaction problems whose templates are definable over various fragments of arithmetic, such as Presburger arithmetic. Such problems are very natural – consider for example the problem of satisfiability of diophantine equations, or of inequations, over the integers – yet their complexity is currently not well understood. The computational complexity of the mentioned problems varies greatly. While it is possible to solve linear diophantine equations in polynomial time[2], solving systems of linear equalities over the integers is NP-complete, and it is not possible to decide if a system of general diophantine equations admits a solution: this is a negative answer to the famous Hilbert's tenth problem[3]. For comparison, the constraint satisfaction problem of a finite structure is necessarily in NP. The classical tools used in constraint satisfaction are often not applicable in the non-ω-categorical realm. In a recent paper[4], the authors presented new tools that allow to systematically study problems over non-ω-categorical templates. This new approach has been successfully used to classify the complexity of the constraint satisfaction problems whose templates can be defined using first-order formulas over the integers with successor[5]. We believe that this new approach can be harnessed to study the constraint satisfaction problems whose templates can be first-order defined over more elaborate non-ω-categorical structures, such as $(\mathbb{Z}; <)$ or $(\mathbb{Z}; <, +)$.

[1] M. Bodirsky and M. Grohe, "Non-dichotomies in Constraint Satisfaction Complexity," in *Proceedings of the 35th International Colloquium on Automata, Languages, and Programming (ICALP 2008)*, 2008, pp. 184–196.

[2] R. Kannan and A. Bachem, "Polynomial Algorithms for Computing the Smith and Hermite Normal Forms of an Integer Matrix," *SIAM Journal on Computing*, vol. 8, no. 4, pp. 499–507, 1978.

[3] Y. Matiyasevich, "Enumerable sets are Diophantine," *Doklady Akademii Nauk SSSR*, vol. 191, no. 2, pp. 279–282, 1970.

[4] M. Bodirsky, M. Hils, and B. Martin, "On the scope of the Universal-Algebraic Approach to Constraint Satisfaction," in *Proceedings of the 25th Symposium of Logic In Computer Science*, 2010, pp. 90–99.

[5] M. Bodirsky, B. Martin, and A. Mottet, "Constraint Satisfaction Problems over the Integers with Successor," in *Proceedings of the 42th International Colloquium on Automata, Languages, and Programming (ICALP 2015)*, 2015, vol. 9134, pp. 256–267.

4.7 The Structure of Weighted Automata on Trees and Tree-like Graphs

Erik Paul (epaul@informatik.uni-leipzig.de)
Supervisor/s: 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.

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

4.8 Qualitative and Quantitative Approaches to Reasoning in Defeasible Description Logics

Maximilian Pensel (maximilian.pensel@tu-dresden.de)
Supervisor/s: PD. Dr.-Ing. Anni-Yasmin Turhan, Prof. Dr. Gerhard Brewka

Classical *description logics* (DL) can be used to represent and reason over domain knowledge in a formal and intuitive way. Clear–cut DL *concepts* and concept inclusions are used to describe properties and relations of categories from an application domain. Inferring implicit knowledge with classical semantics in a monotone way might however fail us when modelling default assumptions. Treating inconsistencies, once an assumption is defeated by more specific knowledge requires nonmonotonic reasoning. In *defeasible description logics* (DDL) we can describe defeasible inclusion relationships between concept descriptions. In practice, defeasible statements can in part be used to model typicality, e.g. stating that "usually, birds fly", which can be used to obtain further inferences as long as no exceptions to the default assumption are present.

In recent years DDLs have been investigated for relatively inexpressive DLs under different semantics[1] mainly for satisfiability and subsumption. Semantics using *preferential nonmonotonic entailment*[2] and *rational closure* as well as the more specific *relevant closure*[3] were investigated for the interest in preferred minimal models. This research project includes a systematic comparison of the existing semantics as well as capturing a formal foundation to allow further investigations towards reasoning with prototypes and inconsistency-tolerant inferences. More practical reasoning tasks such as instance retrieval and the more prominent conjunctive query answering will also be part of this research project in the future.

A defeasible statement might be overwritten by more specific knowledge. However, obtaining this specific knowledge via other defeasible inferences yields the difficulty to decide which assumptions prevail. We propose that the quantitative method of assigning defeasibility degrees will provide the means to realistically capture a measure over the obtained results. Joining advanced results of qualitative defeasible query answering with quantitative measures in defeasible knowledge representation provides incentive for later research within this doctoral project.

[1] P. A. Bonatti, M. Faella, and L. Sauro, "Defeasible Inclusions in Low-Complexity DLs," *Journal of Artificial Intelligence Research. (JAIR)*, vol. 42, pp. 719–764, 2011.

[2] L. Giordano, V. Gliozzi, N. Olivetti, and G. L. Pozzato, "Preferential vs Rational Description Logics: which one for Reasoning About Typicality?" in *In Proceedings of the 19th European Conference on Artificial Intelligence (ECAI 2010)*, 2010, vol. 215, pp. 1069–1070.

[3] G. Casini, T. Meyer, K. Moodley, and R. Nortje, "Relevant Closure: A New Form of Defeasible Reasoning for Description Logics," in *Proceedings of the 14th European Conference on Logics in Artificial Intelligence JELIA*, 2014, vol. 8761, pp. 92–106.

4.9 Answer Set Optimization

Markus Ulbricht (mulbricht@informatik.uni-leipzig.de)
Supervisor/s: Prof. Dr. Gerhard Brewka, Prof. Dr. Sebastian Rudolph

In the area of symbolic Artificial Intelligence, two main research branches have developed from the beginning, namely logic and probability theory. Attempts to combine those areas trace back at least to the 1980s. However, the combination turned out to be surprisingly difficult. Recently, Richardson and Domingos introduced a promising model, originating from machine learning: Markov logic networks[1]. A Markov logic network (MLN) combines Markov random fields and first order logic to enable reasoning under uncertainty. Formulas and annotated real numbers induce a Markov random field, representing a probability distribution over possible worlds.

The fundamental question to be explored in this PhD project is the following: is it possible to adapt the way MLNs combine logic and probabilities to develop a combination between probability theory and non-classical logic, especially non-monotonic logics? In our research, we will focus on logic programming under answer set semantics.

There exists already some research combining logic programming and probability theory. We will take this work as starting point for our own investigations. However, for the purpose of knowledge representation we want to overcome some of the limitations of existing approaches and aim for greater flexibility and expressiveness. An example of existing work worth mentioning is Problog[2] developed in the group of Luc de Raedt. Problog is based on Prolog, yet logical facts and disjunctions can be associated with probabilities, inducing a probability distribution over possible worlds. In addition, logic programming rules are used to represent background knowledge.

We are planning to pursue first a systematic study of the existing work, highlighting its restrictions and limitations. We will then come up with a generalized approach inspired by MLNs. Thereby, we want to investigate and compare two different approaches, namely a direct one based on a probabilistic extension of answer set semantics, and a translation-based one. It is well-known that logic programs under answer set semantics can be represented in classical logic. We will investigate whether a similar approach is sufficient for non-monotonic MLNs and if so, how it relates to the direct one. Based on this generalization, we also plan to study appropriate representations of utility functions for answer sets. Thereby, we aim to combine these functions with probabilistic logic programs to develop ASP-based techniques for decision making.

[1] M. Richardson and P. Domingos, "Markov Logic Networks," *Machine Learning*, vol. 62, no. 1, pp. 107–136, 2006.

[2] A. Dries, A. Kimmig, W. Meert, J. Renkens, G. Van den Broeck, J. Vlasselaer, and L. De Raedt, "ProbLog2: Probabilistic Logic Programming," in *European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases, ECML PKDD 2015, Porto, Portugal, September 7-11, 2015, Proceedings, Part III*, 2015, pp. 312–315.

5 RTG 1765: System Correctness under Adverse Conditions

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

SCARE addresses computerized systems that are placed in an environment with which they cooperate. System correctness means that the cooperation between environment and system satisfies desired behavioral properties. SCARE systematically investigates the problem of system correctness under adverse, only partially predictable conditions which can influence the behavior of the system, the system context and the assumptions made for verifying correctness. The research training group will consider three aspects of adverse conditions, both individually and in their combination:

- limited knowledge
- unpredictable behavior,
- changing system environment and system structure.

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

5.1 Verification Techniques for Dynamically Typed Programs

Björn Engelmann (bjoern.engelmann@uni-oldenburg.de)
Supervisor/s: Prof. Dr. Ernst-Rüdiger Olderog

For internet programming often script languages like JavaScript, Python, or Ruby are used, which are object-oriented and dynamically typed, i.e. the type safety of method calls can be checked only at run time. On the one hand, these languages enable programmers to write elegant, reusable and extendable programs, on the other hand, they create challenges to software verification. In the sense of the correctness relation, the methods of the program represent a system Sys that has only limited knowledge of the way how it will be used by the environment Env in the form of method calls.

Additionally, some of these languages offer more advanced dynamic features like reflection, method update or code generation, allowing the type system, the program or even the language itself to become the object of runtime manipulations. Techniques for establishing the correctness of programs in such dynamic environments Env under an appropriate set of assumptions Asm shall also be investigated.

5.2 System Synthesis and Distributability Using Petri Nets

Evgeny Erofeev (evgeny.erofeev@informatik.uni-oldenburg.de)
Supervisor/s: Prof. Dr. Eike Best

Distribution of a system over several locations can require a significant effort[1], even if concurrency is manifested in the system description. This happens because of choices and communications between processes in different locations, which always occur in a non-zero time for any kind of implementation of the description. To treat this aspect, unlabelled Petri nets are considered to be a conviniet model, since they are coming with an inbuilt notion of distributability, allowing implement the distribution between locations safely. For this reason we are interested in specifications which can be realised by Petri nets.

The main task of system synthesis is to construct an implementation for a given specification of desirable behaviour. System specification can be represented by different classes of formal objects, such as finite automata, regular expressions, or labelled or modal transition systems. We investigate the case when a behavioural specification is given in the form of a labelled transition system, and we raise the following question: in which circumstances can this transition system be implemented with an injectively labelled Petri net? By an implementation (or a solution) with Petri net, an isomorphism between the given labelled transition system and the reachability graph of the net is meant. The injective labelledness of the target object allows to distinguish different agents acting in the modelled system.

Petri net region theory[2] investigates the conditions under which a labelled transition system is isomorphic to the reachability graph of a Petri net. Solvability of a transition system by a Petri net requires event separation and can be explained by linear algebra. However, we are looking for a direct and more efficiently implementable characterisation. Starting with the (seemingly) simple case of a linearly ordered finite transition system (a word) and two labels (i.e., Petri net transitions), so far we have obtained a characterisation for staraight-line substructures which cannot be synthesised a Petri net. This has led to fast algorithms detecting such cases, as well as to very fast synthesis algorithms in certain special cases. In future extensions of this line of work, we intend to study the solvability of a transition system within particular classes of Petri nets, for instance safe, k-bounded, pure, or plain nets, and conditions for distributability of the net synthesised.

[1] E. Best and P. Darondeau, "Perspectives of systems informatics: 8th international Andrei Ershov memorial conference, PSI 2011, Novosibirsk, Russia, June 27 - July 1, 2011, revised selected papers," Springer Berlin Heidelberg, 2012, pp. 1–18.

[2] E. Badouel and P. Darondeau, "Lectures on petri nets I: Basic models: Advances in petri nets," Springer Berlin Heidelberg, 1998, pp. 529–586.

5.3 Correctness of Structure-Changing Systems under Adverse Conditions

Nils Erik Flick (flick@informatik.uni-oldenburg.de)
Supervisor/s: Prof. Dr. Annegret Habel

Graph programs are a formalism for describing concurrent, discrete systems generalising Petri nets. They allow an abstract treatment of graph-like aspects of imperative programs, expressing heap operations as graph transformations, and the direct modelling of many discrete, distributed systems. The goal of my thesis project is to provide a theoretically founded formalism for specifying properties of such systems under adverse conditions, and a proof-based approach to verifying them. To this aim, existing work on the correctness of graph programs is extended. Correctness is understood with respect to specifications consisting of pre- and postconditions as graph conditions: graphical expressions akin to formulae of graph logics. The expressivity of new kinds of spatio-temporal graph properties is examined, and the decidability of classes of properties that are interesting from a modelling point of view, i.e. whether a given system model, under a set of assumptions (Asm), satisfies (sat) a given specification ($Spec$) of correct system behaviour. Under certain adverse conditions a relaxed specification may hold. To address adverse conditions, it is important to understand how to present an integrated view of the interplay of the environment and the system. It would be unreasonable to impose a sequentialisation on system operation and faults, as this does not correspond to the distributed functioning of large systems. Env and Sys can be understood as actors playing an asynchronous game. Both parts are composed in parallel ($\|$) and interact only via the shared state. Case studies include concurrent access to data structures, where only (relaxed) consistent states should be reachable. We have studied[1] language-theoretic correctness notions and found that even for structure-changing Petri nets (an intuitive and apparently simple special case of graph programs), properties one would be interested in are already undecidable while others can be decided for very restricted subclasses. Overall, these results confirm the fundamental insufficiency of fully automatic reasoning for the verification of graph programs. We have introduced state assertions (μ-conditions introduced in[2]) which would be of interest in verifying graph programs that model operations on data structures such as search trees. This includes a weakest-precondition calculus that allows graph programs to be proved correct with respect to μ-conditions logical deduction, significantly expanding upon existing work in this direction. We are still investigating the interaction of system and environment from a game-theoretic point of view, especially under the assumption of intermittent faults.

[1] N. E. Flick and B. Engelmann, "Analysis of Petri nets with context-free structure changes," *Electronic Communications of the EASST*, vol. 71(1), 2015.

[2] N. E. Flick, "On correctness of graph programs relative to recursively nested conditions," in *CEUR proceedings, workshop on graph computation models (GCM) 2015*, 2015, pp. 97–112.

5.4 Verification of Stochastic Systems by Stochastic Satisfiability Modulo Theories with Continuous Domain (CSSMT)

Yang Gao (yang.gao@uni-oldenburg.de)
Supervisor/s: Prof. Dr. Martin Fränzle and Prof. Dr. Ernst-Rüdiger Olderog

Stochastic Satisfiability Modulo Theories (SSMT) is a quantitative extension of classical Satisfiability Modulo Theories (SMT) inspired by stochastic logics. It extends SMT by the usual as well as randomized quantifiers, facilitating capture of stochastic game properties in the logic, like reachability analysis of hybrid-state Markov decision processes. Solving for SSMT formulae with quantification over finite and thus discrete domain has been addressed by Tino Teige et al.

In my PhD work, I consider extending their work to SSMT over continuous quantifier domains (CSSMT) in order to enable to capture of, e.g., continuous disturbances and uncertainty in hybrid systems[1,2]. CSSMT extends the semantics of SSMT and introduces a corresponding solving procedure. My PhD work concentrate on the solving procedure and its soundness for CSSMT along with its algorithmic enhancements, the translation from stochastic hybrid systems to CSSMT formulae and their capability to analyse reachability properties are also considered as the main parts of my PhD work. Meanwhile, the corresponding CSSMT solver is implemented so that the CSSMT formulae can be encoded and solved automatically. Potential applications such as stochastic control problems, scheduling problems etc., are also pursued.

[1] Y. Gao and M. Fränzle, "A solving procedure for stochastic satisfiability modulo theories with continuous domain," in *Quantitative evaluation of systems*, vol. 9259, Springer, 2015, pp. 295–311.

[2] Y. Gao and M. Fränzle, "Verification of stochastic systems by stochastic satisfiability modulo theories with continuous domain," in *Symbolic and numerical methods for reachability analysis, 1st international workshop, SNR 2015*, 2015, vol. 37, pp. 2–10.

5.5 Geometry-Predicting Communication Protocols for Car2X Applications

Saifullah Khan (saifullah.khan@informatik.uni-oldenburg.de)
Supervisor/s: Prof. Dr. Martin Fränzle

Vehicular Ad-hoc Networks (VANETs) have a broad range of applications that varies from safety applications to comfort systems. Such networks hold unique characteristics induced by their application domain that necessitate their study from a substantially different perspective and with respect to other design goals than the prevailing paradigm for conventional mobile ad-hoc networks. The international standard IEEE 802.11p defines the low layer protocols for VANETs aiming at support for Intelligent Transportation System (ITS) applications. Complementing this standard, we argue that the Network Layer and the MAC Layer are of crucial importance to reliability, availability, and performance of VANET communication. Addressing this issue, we propose a novel routing protocol called Traffic Aware Segment-based Routing (TASR)[1] protocol, which is a multi-hop routing protocol specifically designed for the challenges of urban environments with their complex and dynamically changing topologies due to ubiquitous occlusions and, relatively to the reach, high agent mobility. Reflecting this network dynamics and its consequential channel access and window contention among the set of possible relay nodes, we propose a Cooperation and Network-Coding based Medium Access Control (CNC-MAC)[2] extending IEEE 802.11 to improve the network throughput and the transmission reliability by allowing intermediate relay nodes to combine received packets. Furthermore, as IEEE 1609.4 defines a MAC layer implementation for multichannel operations in VANET, we add a novel Multi-Channel Mode (MCM-MAC) protocol for emergency systems to improve the channel utilization of the control channel (CCH) and uniformly distribute the channel load on service channels (SCHs). In the proposed protocol, subnetworks change their modes from general to emergency mode to increase the probability for an urgent, time and safety-critical message to arrive in time.

[1] S. Khan and M. Fränzle, "Robust mid-range communication in urban VANETs," in *17th IEEE advanced communication technology (ICACT)*, 2015, pp. 115–120.

[2] S. Khan, M. Alam, N. Müllner, and M. Fränzle, "Cooperation and network coding based MAC protocol for VANETs," in *IEEE vehicular networking conference (VNC)*, 2015, pp. 64–67.

5.6 Handling Delay Differential Equations in Automatic Verification of Hybrid Systems

Peter Nazier Mosaad (peter.nazier.mosaad@informatik.uni-oldenburg.de)
Supervisor/s: Prof. Dr. Martin Fränzle

Hybrid systems are mathematical models for real life systems whose behaviors involve a mixture of discrete and continuous dynamics. In consideration of modeling and formal verification, a lot of research in this area has been done to automatically verify such hybrid systems involving ordinary differential equations (ODEs) for continuous behavior, e.g., Egger's integration into SAT modulo theory[1,2]. The most common example of hybrid systems occurs when discrete/digital controllers switch between different continuous processes. Unmodeled delays in a control loop have the potential to invalidate any stability or safety certificate obtained on the delay-free model, as delays may significantly deteriorate control performance. In order to model the delay in the differential equations, this leads to what is called delay differential equations (DDEs). Delay differential equations (DDEs) play an important role in the modeling of processes with time delays, both natural and manmade processes, in biology, physics, economics, engineering, etc. Given such delays in modern control schemes like networked distributed control, one might thus expect tools permitting their safe automatic analysis to abound. Unfortunately that is not the case.

In my thesis, I focus on automatic verification and analysis for hybrid systems featuring delays, extending the techniques of safely enclosing set-based initial value problem of ODEs to DDEs. As a first step, we have exposed an automatic method for the stability and safety verification of a simple class of DDE, which the presented delay is single and constant[3]. The work in progress, we extend this method to verify class of safety properties in the form of linear temporal logic (LTL) specifications. Also, we pursue a closer integration of the integration and the sensitivity-related state bloating algorithms underlying verification by simulation, together yielding a safe enclosure algorithm for DDEs suitable for use in automated formal verification. Beyond that, as a less immediate future work, different kinds of DDEs will be considered as DDE with time-dependent or more generally state-dependent delay.

[1] A. Eggers, M. Fränzle, and C. Herde, "SAT modulo ODE: A direct SAT approach to hybrid systems," in *Automated technology for verification and analysis, 6th international symposium, ATVA 2008, Seoul, Korea, October 20-23, 2008. Proceedings*, 2008, pp. 171–185.

[2] A. Eggers, N. Ramdani, N. S. Nedialkov, and M. Fränzle, "Improving the SAT modulo ODE approach to hybrid systems analysis by combining different enclosure methods," *Software and System Modeling*, vol. 14, no. 1, pp. 121–148, 2015.

[3] L. Zou, M. Fränzle, N. Zhan, and P. N. Mosaad, "Automatic verification of stability and safety for delay differential equations," in *Computer aided verification - 27th international conference, CAV 2015, San Francisco, CA, USA, July 18-24, 2015, Proceedings, part II*, 2015, pp. 338–355.

5.7 Robust Spatio-Temporal Logic for Mobile Agents

Heinrich Ody (heinrich.ody@uni-oldenburg.de)
Supervisor/s: Prof. Dr. Ernst-Rüdiger Olderog

Traditionally, to define a controller for a car in highway traffic scenarios the desired behaviours like lane change manoeuvres are defined as differential equations. To prove that the controller is safe i.e. it avoids collisions for example a hybrid automaton is built for which the desired property is checked in some way. However, proving properties for hybrid automata is very difficult.

It has been argued that to prove spatial properties like collision avoidance only positional information and the braking distance are needed[1]. During such a proof, the car dynamics can be abstracted away, if the assumptions on the car dynamics are explicitly stated. Subsequently, it has to be proven that the car dynamics actually satisfy the assumptions made, which the authors believe will be much easier, as spatial properties like e.g. safety do not have to be considered anymore. To reason about spatial aspects independently of the car dynamics the authors introduced *Multi-Lane Spatial Logic* (MLSL), which allows to formulate spatial properties for cars on highways.

Currently, MLSL depends on exact and correct spatial values. In this thesis we extend MLSL to be robust against small errors, which are introduced by e.g. inaccurate sensors. To make MLSL robust one possible approach may be to define a quantitative semantics for it, as it has been done for Duration Calculus[2]. We hope that a robust semantics of MLSL will make the logic more relevant to practice and that it allows for more efficient decision procedures.

[1] M. Hilscher, S. Linker, E.-R. Olderog, and A. P. Ravn, "An Abstract Model for Proving Safety of Multi-Lane Traffic Manoeuvres," in *Formal Methods and Software Engineering - ICFEM*, 2011, vol. 6991, pp. 404–419.

[2] M. Fränzle and M. R. Hansen, "A robust interpretation of duration calculus," in *Theoretical Aspects of Computing - ICTAC*, 2005, vol. 3722, pp. 257–271.

5.8 Graph Transformation Games for Modeling Adverse Conditions

Christoph Peuser (christoph.peuser@informatik.uni-oldenburg.de)
Supervisor/s: Prof. Dr. Annegret Habel

Graph transformation systems are an elegant solution for many modelling problems in computer science. The system state is modelled as a graph and state changes are rule applications that change the graph. The existing correctness notions for graph transformation systems, for example by Pennemann[1] or Poskitt[2], allow proving correctness of a system with respect to given pre- and postconditions.

In this PhD thesis, we will investigate systems under adverse conditions, e.g. systems under the influence of an unpredictable environment. Such systems will frequently allow the intermittent violation of desired properties, as long as these properties can be recovered after some time.

We propose to model these systems as games, with the system and its environment as opposing players. The system is correct if it can reestablish the desired properties despite the environments interference, that is, if there is a winning strategy for the system.

The goal of the thesis is the investigation of graph transformation games, i.e. games in which the players moves are applications of graph transformation rules, as a notion of correctness for systems under adverse conditions.

The SCARE formula

$$Asm \vdash (Sys \| Env)\ sat\ Spec$$

is instantiated with a system Sys and environment Env consisting of attributed graph transformation rules. Their composition $\|$ is a game with the specification $Spec$, a temporal graph condition, as the winning condition and sat is the satisfaction of this condition, i.e. the existence of a winning strategy for Sys. Finally, the assumption Asm is a regular language, specifying the frequency with which system or environment may change the system state.

The results are to be illustrated with the help of case studies, for example a telephone system or a railroad system.

[1] K.-H. Pennemann, "Development of correct graph transformation systems," PhD thesis, Universität Oldenburg, 2009.
[2] C. M. Poskitt, "Verification of graph programs," PhD thesis, University of York, 2013.

5.9 A Theory of HR* Graph Conditions and their Application to Meta-Modeling

Hendrik Radke (hendrik.radke@uni-oldenburg.de)
Supervisor/s: Prof. Dr. Annegret Habel

As software systems grow more complex, there is a growing need for design concepts that allow an intuitive overview of a system. This is usually achieved through visual modeling techniques. Graph transformation systems are an established visual modeling approach, modeling systems as graphs. Structural properties of the graphs can be expressed by nested conditions[1]. However, nested conditions are not expressive enough to formulate non-local properties often encountered in real-world problems, like the existence of arbitrary-length paths, connectedness or circle-freeness.

We therefore propose HR* conditions, an extension to nested conditions. HR* conditions are enriched with hyperedges, which are then replaced by graphs according to a hyperedge replacement system. The expressiveness of HR* conditions lies between counting monadic second-order logic and second-order logic. Several variants of HR* conditions are introduced and their respective advantages and disadvantages are discussed.

The correctness of a specification, i.e. a triple of graph program, pre- and postcondition in the form of HR* conditions, can be checked. Basic transformations are used on the graph program and the postcondition to generate a weakest precondition. This can then be compared with the original precondition to check the correctness of the specification.

HR* conditions are applied to the problem of instance generation for UML meta-models with OCL constraints. The meta-model's type graph can be transformed into a graph grammar[2]. Essential OCL constraints belonging to the type graph are transformed into HR* conditions. Using HR* conditions allows the translation of OCL constraints that go beyond first-order. The conditions are then transformed into application conditions for the graph grammar's rules. This ensures that the grammar only generates instances which satisfy the OCL constraints. The grammar-based approach allows the simple generation of a large number of instances.

[1] A. Habel and K.-H. Pennemann, "Correctness of high-level transformation systems relative to nested conditions," *MSCS*, vol. 19, pp. 245–296, 2009.

[2] K. Ehrig, J. M. Küster, and G. Taentzer, "Generating instance models from meta models," *Software and System Modeling*, vol. 8, no. 4, pp. 479–500, 2009.

5.10 Car2X Network Security for Road Hazard Warning Applications

Md Habibur Rahman (md.habibur.rahman@uni-oldenburg.de)
Supervisor/s: Prof. Dr. Werner Damm and Dr. Sibylle Fröschle

Car2X communication security based on IEEE 802.11p has attracted automotive industry, researchers, and standardized bodies for the intelligent transportation systems (ITS). For protecting communication security, and development of a robust routing mechanism is an open issue for the Car2X safety message dissemination.

The motivation of the PhD thesis is not only followed the European Telecommunications Standards (ETSI) and the PRESERVE Project to design and implementation of a reliable, scalable, secure communication protocols, but also provide a flexible framework for the road hazard based delay sensitive safety applications. We assume that each car has sensors to detect hazards on the highway or urban area, equipped with GPS, and digital maps. In car system which include road hazard basic attribute through the application layer, and the facilities layer using the Decentralized Environmental Notification Message (DENM) mechanism to disseminate the hazard message towards the destination region using the Geo-broadcasting mechanism in a distributed manner along with the existing on-board security module on the car. The hazard warning message transmission, dissemination will be evaluated by the misbehavior detection mechanism to determine the different ratio of honest or attackers, different types of attacks, and different traffic density scenarios.

5.11 Design and Analysis of Highly Reliable Region-Adherent Distributed Algorithms in Faulty Environments

Dilshod Rahmatov (dilshod.rahmatov@informatik.uni-oldenburg.de)
Supervisor/s: Prof. Dr.-Ing. Oliver Theel

Self-stabilizing systems are famous realizations of fault-tolerant systems. Such a system is always live, but due to faults or improper initialization, it might not be safe. Because its "inner design," a self-stabilizing system - as long as it is not in a state from whereon it exhibits safe behavior - autonomously works towards establishing or re-establishing this safe behavior. And importantly, it does so in an upper-bounded number of execution steps (in the absence of newly occurring faults), a property called convergence. Thus, one can regard self-stabilizing systems as systems that limit the invalidation of their safety property in time. An alternative, thought, is restricting it in space.

Our research work is exploring a new class of fault-tolerant distributed algorithms based on a concept which we call region-adherence[1]. In contrast to self-stabilizing systems which are clearly non-masking fault-tolerant systems, region adherent systems can be realized as either being masking or non-masking. A region-adherent system can be perceived as a system exhibiting a particular variant of gracefully degrading behavior: it gracefully degrades the service quality provided by the system per fault up to some maximal number of faults, the system is able to withstand. Additionally, degradation is upper-bounded per fault. With service quality, we mean some application-specific quality-of-service notion: without faults, the system delivers some service with 100% quality. When faults occur, then the service quality gets more and more reduced. A region-adherent system exhibits desirable fault tolerance properties. When region adherence is realized in a system, it manifests gracefully degrading, quantified quality-of-service guarantees in case up to f faults happen. Thus, at any time knowing the number of faults that have happened, the system user can take an a priori known minimal service quality for granted: a very valuable information in various critical settings!

[1] J. S. Becker, D. Rahmatov, and O. Theel, "Dependable Systems through Region-Adherent Distributed Algorithms," in *Proc. of the international conference in central asia on internet (ICI '13)*, 2013.

5.12 Petri Net Synthesis and Modal Transition Systems

Uli Schlachter (uli.schlachter@informatik.uni-oldenburg.de)
Supervisor/s: Prof. Dr. Eike Best

The state space of a system can be represented explicitly as a labelled transition system consisting of states and transitions between states, which are labelled by letters of some alphabet. Given a system, it is relatively straightforward to calculate its state space, although it often is quite time consuming. The synthesis problem is the other direction: Decide if an implementation exists that has some given behaviour.

Such a labelled transition system could model a mobile sensor node. After receiving a request for a new measurement, the system measures some value and responds with the result. Initially the system is waiting for a request.

In Petri net synthesis, the desired system is a Petri net and the state space is its reachability graph. Region theory was introduced for solving this problem for elementary nets[1]. Since then this theory was extended to other classes of Petri nets and more general problems, for example finding a Petri net that generates a given language[2,3].

Our work consists of two parts. We have implemented the Petri net synthesis algorithm. The performance of this implementation is comparable to existing tools and provides features that are, to our knowledge, not available in any other tool. For example it is possible to ask for a conflict-free Petri net. This is acomplished by choosing between several algorithms based on the input, so that simpler problems are solved via faster algorithms[4].

Based on this, the synthesis problem for modal transition systems is investigated. We showed that this problem is undecidable and are now identifying decidable subcases. A modal transition system, as introduced by Larsen and Thomsen in 1988, can be seen as a generalisation of labelled transition systems where there are two kind of arcs. *Must arcs* describe behaviour that is required from a system while *may arcs* are allowed, but can also be omitted.

These systems are more expressive than labelled transition systems and thus give more flexibility to the user. For example one can extend the mobile sensor node by an option to log measurements locally before sending a reply, without requiring this behaviour from all sensor nodes.

[1] A. Ehrenfeucht and G. Rozenberg, "Partial (set) 2-structures. part I: basic notions and the representation problem; part II: state spaces of concurrent systems," *Acta Inf.*, vol. 27, no. 4, pp. 315–368, 1990.

[2] P. Darondeau, "Deriving unbounded petri nets from formal languages," in *CONCUR '98: Concurrency theory, 9th international conference, Nice, France, September 8-11, 1998, Proceedings*, 1998, vol. 1466, pp. 533–548.

[3] E. Badouel, L. Bernardinello, and P. Darondeau, *Petri net synthesis*. Springer, 2015.

[4] E. Best and U. Schlachter, "Analysis of petri nets and transition systems," in *Proceedings 8th interaction and concurrency experience, ICE 2015, Grenoble, France, 4-5th June 2015.*, 2015, vol. 189, pp. 53–67.

5.13 Properties of Communicating Controllers for Safe Traffic Manoeuvres

Maike Schwammberger (schwammberger@informatik.uni-oldenburg.de)
Supervisor/s: Prof. Dr. Ernst-Rüdiger Olderog

Traffic safety is a relevant topic, as driving assistant systems and probably soon fully autonomous driving cars are increasingly capturing the market. In previous work, an abstract model for traffic safety on freeways[1] and countryroads[2] was considered by Hilscher et al.. For that purpose the authors introduced the Multi-lane spatial logic (MLSL) and a concept for a lane-change controller.

Martin Hilscher and myself furthermore extended the existing model and logic MLSL to an abstract model for proving safety in urban traffic scenarios[3]. Another achievement of this work was the introduction of automotive-controlling timed automata to specify the existing lane-change controller and its extension to a crossing controller.

For both country roads and urban traffic only a concept of perfect knowledge was considered, where every car perceives the full safety envelope (comprising the physical size and braking distance) of every other car.

As the first part of my PhD thesis, I plan to extend the work on countryroads and urban traffic by considering a more realistic model without perfect knowledge, where a cars sensors may only perceive the physical size of other cars but not their braking distance. In this case, cars need to communicate with each other to prevent collisions. To this end, I will extend the existing controllers by a concept of communication with broadcast channels.

As second part, I will consider liveness and fairness properties of the controllers by first extending the logic MLSL to express such properties. To prove liveness, one could use a tool-driven approach to test reachability of specific states.

[1] M. Hilscher, S. Linker, E.-R. Olderog, and A. Ravn, "An abstract model for proving safety of multi-lane traffic manoeuvres," in *Int'l conf. on formal engineering methods (ICFEM)*, 2011, vol. 6991.

[2] M. Hilscher, S. Linker, and E.-R. Olderog, "Proving safety of traffic manoeuvres on country roads," in *Theories of programming and formal methods*, vol. 8051, Springer Berlin Heidelberg, 2013, pp. 196–212.

[3] M. Hilscher and M. Schwammberger, "Extending an abstract model for proving safety of motorway manoeuvres to urban traffic scenarios," Manuscript, Manuscript, 2015.

5.14 Model-Based Safety and Security Analysis

Thomas Strathmann (thomas.strathmann@offis.de)
Supervisor/s: Sibylle Fröschle

The goal of this thesis is to incorporate security analyses into the development process for safety-critical systems, e.g. in the automotive domain. Individual vehicles are increasingly networked to provide convenience and safety features. With a growing number of interfaces to the outside world, the risk of security attacks rises. As has been demonstrated by security researchers attacks on the security of a vehicle may impact its safe operation, e.g. by remotely taking control of the steering[1]. Hence, functional safety has to take security threats into account.

To support this endeavour, I propose the *model-based safety and security analysis* (MBSSA). This method builds on an existing technique for analyzing the safety of a system in the presence of faults. The system is given as a behavioral model, e.g. state charts. Variables in the model are annotated with failure modes which describe deviant behavior. The resulting extended system model can be analyzed with respect to a formal specification using model-checking techniques. In this way, cut sets (combinations of faults which together cause the violation of the specification) are computed automatically. This result shows how resilient a design is to certain types of faults.

In order to incorporate security attacks into this approach, I have defined a catalog of attacks along with their safety impact. This collection draws upon attacker models from security verification[2] and concrete attacks. The attacks are injected into a model of the system in much the same way as faults. Among other things, successful attacks may change the behavior of components or interfere with the communication between components. To analyze attack scenarios comprised of multiple attacks, the consequences of the injected attacks are traced as they propagate through the system. The result of this analysis can be visualized in the form of attack trees[3]. By linking safety requirements to components and signals in the model, the impact of security attacks on the system's safety becomes visible.

Another part of the thesis is a modeling language for security architectures. These architectures specify both security requirements like integrity or confidentiality of data and partial knowledge about the implementation such as the allocation of connections to physical bus systems. In this refined model, a more detailed analysis can be performed.

[1] C. Miller and C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle." http://illmatics.com/Remote%20Car%20Hacking.pdf, August-2015.
[2] D. Dolev and A. C. Yao, "On the security of public key protocols," in *Proceedings of the 22nd annual symposium on foundations of computer science*, 1981, pp. 350–357.
[3] B. Schneier, "Attack trees," *Dr. Dobb's Journal*, vol. 24, no. 12, pp. 21–29, December 1999.

5.15 Semantic Data Replication

Awais Usman (awais.usman@uni-oldenburg.de)
Supervisor/s: Prof. Dr. Oliver Theel

Data replication is an important research area, as reliable access to data makes up the base of most of IT services. High operations availability, low operation costs and data consistency are major target conflicts in almost every data replication research. In the thesis, we introduce a data semantic, and data encoding based data replication technique called Semantic Data Replication (SDR). SDR focuses on the exploitation of data semantics, coding schemes, virtualization, and efficient search algorithms to come up with a strategy whose goal is to provide a high level of operations availability with low cost. SDR primarily takes advantage of the finite state space of some the replicated objects, and it uses the prior knowledge from the state map to know in advance of the state transformation, which makes this approach more efficient than existing infinite state space replication techniques. Exploitation of the data coding schemes is a significance contribution in SDR. The coding schemes helps in fast execution of read and write operation. It provides consistent access to the state of the replicated object at low cost while communicating with the replicas.

5.16 Quality of Service Optimization Strategies in Wireless Sensor Networks

Peilin Zhang (peilin.zhang@informatik.uni-oldenburg.de)
Supervisor/s: Prof. Dr.-Ing. Oliver Theel

Wireless sensor network (WSN) has emerged as a promising technology thanks to the recent advances in electronics, networking, and information processing. Over the past years, a wide range of WSN applications has been proposed such as environmental monitoring, forecasting systems, and health monitoring. In most of the applications, low power, inexpensive, and tiny sensor nodes cooperate as a network. Such networks must be energy efficient and able to provide a sufficient level of Quality of Services (QoS). However, QoS provision in WSNs is a very challenging task, where these QoS metrics are typically contradicting and resources such as power source, processing power, and memory are taxed.

First, we propose a novel strategy, referred to as the lifetime planning for achieving best-effort QoS in WSNs, while reaching an adequate lifetime required to complete the assigned task simultaneously. The core idea is to sidestep lifetime maximization strategies in which sensors continue functioning even after their fulfilment of tasks. In these cases, we could deliberately bound the operational lifetime to the expected task lifetime. Thus more energy can be spent throughout the entire lifetime for enhancing the provided service qualities. To demonstrate the effectiveness of our design, we conduct an intensive performance evaluation using an office monitoring scenario as a case study. Furthermore, we examine the profit of adopting our strategy relative to fixed heuristics and blind adaptation. The results show that lifetime planning highly improves the QoS metrics in WSNs. Second, for a range of WSN-based applications, especially mission-critical applications under adverse conditions, maintaining a consistent QoS guarantee throughout the network lifetime is highly required. Namely any degradation over time in these applications should be avoided as much as possible. We plan to focus on adaptive QoS optimization mechanisms with learning and prediction capabilities to provide a consistent level of service qualities for WSN-based applications.

6 RTG 1773: Heterogeneous Image Systems

Prof. Dr. Marc Stamminger (marc.stamminger@informatik.uni-erlangen.de)
University of Erlangen-Nuremberg
http://hbs.fau.de

The research training group "Heterogeneous Image System" examines systems for processing, generating, and transmitting digital images. Typical examples for such systems are high-end desktop computers, gaming consoles, or mobile devices such as smart phones. All these systems use dedicated hardware for certain image processing tasks, such as graphics or signal processors, or video de- and encoders. For many applications, only with such heterogeneous architectures it is possible to meet the demands in terms of performance, latency, or power consumption.

The heterogeneity of these image systems is twofold: Firstly, the computation is spread over several components within a system. Secondly, there are numerous heterogeneous sets of architecture on which different image applications are executed.

Our group examines three different aspects of such heterogeneous image systems: In project area A, we work on novel dedicated hardware for capturing and encoding image and video data. In area B, we research and develop novel tools and methods for programming such architectures, in particular for modeling, run-time systems, mapping of algorithms, and hardware abstraction of these heterogeneous systems. Applications are examined in project area C, where we look at medical image processing tasks, capturing of multispectral images and 3D-information, as well as global illumination simulation. In two industry-funded projects we further research the application for image guided surgical procedures and the rendering on display devices in cars.

6.1 Motion Correction for Weight-Bearing C-Arm CT of Knees

Bastian Bier, Jennifer Maier (bastian.bier@fau.de, jennifer.maier@fau.de)
Supervisor/s: Prof. Dr. Andreas Maier

Particularly in aging populations, Osteoarthritis (OA) is one of the leading causes for disability and functional decline of the body[1]. Yet, the causes and progression of OA, especially in the early stages, remain poorly understood. Current OA imaging measures require long scan times and are logistically challenging. Furthermore, they are often insensitive to early changes of the tissue.

The overarching goal of this project is the development of a novel computed tomography imaging system allowing for an analysis of the knee cartilage under weight-bearing conditions. The articular cartilage deformation under different weight-bearing conditions reveals information about abnormal motion patterns, which can be an early indicator for arthritis. This can help to detect the medical condition at an early stage. To allow for a scan in standing or squatting position, we opted for a C-arm CT device that can be almost arbitrarily positioned in space. The standard application area for C-arm CT is in the interventional suite, where images are acquired on a vertical trajectory around the patient. For the recording of the knees, a horizontal trajectory has been developed.

This system allows for an analysis of the knee joint under weight-bearing conditions. In terms of reconstruction, there are several challenges. One of the main issues is involuntary patient movement during the scan. This motion will result in artifacts in the reconstruction that reduce the diagnostic image quality. Current approaches use fiducial markers[2,3] or the registration of previously segmented bones[4] to correct for the motion.

In this project, we investigate novel methods to estimate the patient motion during the scan to reduce these artifacts. One approach is to compute the internal motion field of the knee using surface cameras. Another approach is the design and evaluation of a biomechanical model of the knee using inertial sensors.

After the correction of the motion artifacts, the reconstructed volume is used for the segmentation and quantitative analysis of the knee joint tissue. This will give information about the risk or the progression of an arthrosis disease.

This project is in collaboration with the Radiological Sciences Lab, Stanford University, Stanford, CA, USA.

[1] R. F. Loeser, S. R. Goldring, C. R. Scanzello, and M. B. Goldring, "Osteoarthritis: A disease of the joint as an organ," *Arthritis & Rheumatism*, vol. 64, no. 6, pp. 1697–1707, 2012.

[2] J.-H. Choi at al., "Fiducial marker-based correction for involuntary motion in weight-bearing C-arm CT scanning of knees. II. experiment," *Med. Phys.*, vol. 41, no. 6, 2014.

[3] K. Müller at al., "Automatic motion estimation and compensation framework for weight-bearing C-arm CT scans using fiducial markers," in *IFMBE proceedings*, 2015, pp. 58–61.

[4] M. Berger at al., "Marker-free motion correction in weight-bearing cone-beam CT of the knee joint," *Medical Physics*, vol. 43, no. 3, pp. 1235–1248, 2016.

6.2 Development of Multivariate Mathematical Morphology for Hyperspectral Image Classification

AmirAbbas Davari (amir.davari@fau.de)
Supervisor/s: Prof. Dr.-Ing. habil. Andreas Maier

Remote sensing is nowadays of paramount importance for several application fields, including environmental monitoring, urban planning, ecosystem-oriented natural resources management, urban change detection and agricultural region monitoring[1]. Majority of the aforementioned monitoring and detection applications require at some stage a label map of the remotely sensed images, where individual pixels are marked as members of specific classes, e.g. water, asphalt, grass, etc. In other words, classification is a crucial step for several remote sensing applications.

It is widely acknowledged that exploiting both the spectral as well as spatial properties of pixels, improves classification performance with respect to using only spectral based features[2]. In this regard, morphological profiles (MP) are one of the popular and powerful image analysis techniques that enable us to compute such spectral-spatial pixel descriptions. They have been studied extensively in the last decade and their effectiveness has been validated repeatedly[3].

The characterization of spatial information obtained by the application of a MP is particularly suitable for representing the multiscale variations of image structures, but they are limited by the shape of the structuring elements. To avoid this limitation, morphological attribute profiles (AP) have been developed. By operating directly on connected components instead of pixels, not only they enable us to employ arbitrary region descriptors (e.g. shape, color, texture, etc) but they pave the way for object based image analysis as well. In addition they can also be implemented efficiently by means of hierarchical image representations.

The aforementioned proposed techniques for hyper-spectral remote sensing image analysis are basically based on marginal processing of the image, i.e. analyzing each spectral channel individually and not simultaneously. Our project focuses on extending the mathematical morphology to the field of hyperspectral image processing and applying morphological content based operators, e.g. MP and AP, on all of the spectral bands simultaneously rather than marginally.

[1] S. Valero, P. Salembier, and J. Chanussot, "Hyperspectral image representation and processing with binary partition trees," *IEEE Transactions on Image Processing*, vol. 22, no. 4, pp. 1430–1443, April 2013.

[2] D. A. Landgrebe, *Signal theory methods in multispectral remote sensing*. John Wiley & Sons, Inc., 2005.

[3] J. A. Benediktsson, M. Pesaresi, and K. Amason, "Classification and feature extraction for remote sensing images from urban areas based on morphological transformations," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 41, no. 9, pp. 1940–1949, Sept 2003.

6.3 Model Support in Design, Test and Monitoring of Image System Architectures

Anna Deitsch, Vitali Schneider (anna.deitsch@fau.de, vitali.schneider@fau.de)
Supervisor/s: Prof. Dr. Reinhard German

Image processing systems are characterized by very high computational demand caused by the large amount of data, the response time, or the complexity of the image processing algorithms. For these reasons, specialized hardware solutions based on multiple processing cores, non-uniform memory, complex interconnect or custom hardware elements such as DSPs and FPGAs are used for image processing. Furthermore, development of applications for heterogeneous hardware architectures is challenging due to distribution of computational tasks among processors and programmable logic units. Therefore, we investigate new methodologies and tools for more efficient development of image system architectures.

Our research focuses on the application of model-driven engineering (MDE) techniques in main phases of the development process: from requirements modeling, through system design and specification to code generation and validation. To specify widely diverse aspects of a multidisciplinary domain like an image system we propose a modeling methodology based on UML as a common language and tailored by a special combination[1] of several UML extension profiles standardized by the OMG group.

However, the standard UML profiles couldn't provide enough semantics for the effective development process of image systems. In order to introduce the required semantics, we are working on a specific profile for image systems[2]. The usage of the UML profiles instead of domain-specific modeling languages avoids the additional effort for learning a new modeling language as well as designing, implementing, and maintaining domain-specific model editors, because the existent UML editors and the widely known modeling language can be applied.

Besides our ongoing work on the modeling methodology, we are developing a framework, which offers an integrated tool environment to provide widely automated support for modeling, validation, model-to-simulation code transformation, simulation, and analysis of such complex model-based system specifications[3].

[1] V. Schneider, A. Yupatova, W. Dulz, and R. German, "How to avoid model interferences for test-driven agile simulation based on standardized UML profiles (work in progress)," in *Proceedings of the symposium on theory of modeling & simulation - DEVS integrative*, 2014, pp. 35:1–35:6.

[2] A. Deitsch, V. Schneider, J. Kane, W. Dulz, and R. German, "Towards an Efficient High-Level Modeling of Heterogeneous Image Processing Systems," in *Proceedings of the Symposium on Theory of Modeling & Simulation - DEVS Integrative (DEVS'16)*, 2016.

[3] V. Schneider, A. Deitsch, W. Dulz, and R. German, "Principles of performance and reliability modeling and evaluation," Springer International Publishing, 2016, pp. 499–523.

6.4 Signal Processing and Video Coding Algorithms Adapted to Fisheye Image and Video Data

Andrea Eichenseer (andrea.eichenseer@fau.de)
Supervisor/s: Prof. Dr.-Ing. André Kaup

To survey a large area with a single camera, video surveillance and automotive systems often employ fisheye cameras which provide a very wide field of view of above 180 degrees. Due to the non-perspective mapping of the 3D scene to the image plane, the resulting fisheye images and videos exhibit characteristics that are quite different from conventional rectilinear image and video data. The most evident characteristic is the appearance of straight lines in the world as arcs in the captured image. Typical signal processing techniques, however, do not take into account these fisheye characteristics. Motion estimation and compensation methods, for example, are usually based on a translational motion model, as translation is generally considered the predominant motion in a scene.

In the course of this project, the effect of radial distortion on video coding was therefore examined by means of distortion corrected fisheye video sequences[1]. From this preliminary investigation, it was concluded that exploiting knowledge about the inherent fisheye characteristics should lead to gains in coding efficiency. Subsequently, a modification of traditional motion estimation towards equisolid fisheye video sequences was conducted, resulting in an adapted hybrid motion estimation technique[2]. The gains of this method over the traditional approach were further substantiated by an application of the fisheye-adapted motion estimation technique on temporal error concealment[3]. To allow for a thorough analysis, synthetic ground-truth fisheye video sequences rendered from 3D scenes as well as real-world videos captured with an actual fisheye camera were compiled in a publically available data set[4]. Current research includes the incorporation of camera calibration information into the motion estimation process as well as the investigation of modified multi-image super-resolution for fisheye video sequences.

[1] A. Eichenseer and A. Kaup, "Coding of Distortion-Corrected Fisheye Video Sequences Using H.265/HEVC," in *Proceedings of the IEEE International Conference on Image Processing*, Paris, France, October 2014, pp. 4132–4136.

[2] A. Eichenseer, M. Bätz, J. Seiler, and A. Kaup, "A Hybrid Motion Estimation Technique for Fisheye Video Sequences Based on Equisolid Re-Projection," in *Proceedings of the IEEE International Conference on Image Processing*, Quebec City, Canada, September 2015, pp. 3565–3569.

[3] A. Eichenseer, J. Seiler, M. Bätz, and A. Kaup, "Temporal Error Concealment for Fisheye Video Sequences Based on Equisolid Re-Projection," in *Proceedings of the European Signal Processing Conference*, Nice, France, September 2015, pp. 1636–1640.

[4] A. Eichenseer and A. Kaup, "A Data Set Providing Synthetic and Real-World Fisheye Video Sequences," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing*, Shanghai, China, March 2016, Available online: `www.lms.lnt.de/fisheyedataset`.

6.5 Design and Mapping of Image Processing Operators for Reconfigurable Hardware

Konrad Häublein (konrad.haeublein@fau.de)
Supervisor/s: Prof. Dr.-Ing. Dietmar Fey

Image processing algorithms applied on embedded programmable systems very often do not meet the given constraints in form of real-time capability. Mapping these algorithms to reconfigurable hardware solves this issue, but demands further specific knowledge in hardware development, since the developer is required to describe the algorithm in a hardware description language (HDL). Utilizing high level synthesis (HLS) on the other hand hides the hardware layer, but the quality of generated hardware depend on an optimal description, given constraints and on the synthesis process of the HLS tool.

Nevertheless, the design process can be accelerated by combining the strengths of both design flows in form of a hybrid approach. HDL implementations are well suited for reusable artifacts, like memory structures and state machines, since they need to be designed only once as generic hardware and later used with the desired configuration. Since the memory access patterns for many image processing operators is quite similar, the structural description can be provided as generic templates from a library as designed in[1]. By utilizing code transformation techniques these templates can be generated out of a structural XML description, which eliminates the use of an HDL language for the developer.

Data flow descriptions, which are used for explicit kernel definitions, may differ from kernel to kernel. Hence, they need to be redesigned for specific needs. Designing kernels with an HDL can become quite time consuming and error-prone, since parallelization and pipelining need to be handled by the developer. An HLS framework takes care of these architectural descriptions. The design space of a data flow description is limited, which unloads the synthesis process, saves time of the mapping process, and lowers the resulting resource utilization.

At the current state it is possible to map any combination of point and local operators to an FPGA by utilizing a hybrid design flow using an XML file and a C++ HLS description for each kernel as input. In future work we aim to add more complex memory structures for more sophisticated operators in order to support the usage of a template for stereo images[2] and global image processing operators.

[1] K. Häublein, C. Hartmann, M. Reichenbach, and D. Fey, "Fast and resource aware image processing operators utilizing highly configurable IP blocks," in *To appear in: Proceedings of ARC 2016 (applied reconfigurable computing)*, 2016, pp. 1–8.

[2] K. Häublein, M. Reichenbach, and D. Fey, "Fast and generic hardware architecture for stereo block matching applications on embedded systems," in *Proceedings of ReConFig' 14*, 2014, pp. 1–6.

6.6 IPAS - A Design Framework for Analysis, Synthesis and Optimization of Image Processing Applications for Heterogenous Computing Architectures

Christian Hartmann (christian.hartmann@fau.de)
Supervisor/s: Prof. Dr-Ing Dietmar Fey

In recent years, the use of image processing systems has increased steadily. However, most of them are very complex and contain several tasks with different complexities which result in varying requirements for computing architectures. Nevertheless, a general processing scheme in every image processing application has a similar structure, called image processing pipeline: (1) capturing an image, (2) pre-processing using local operators, (3) processing with global operators and (4) post-processing using complex operations. In the traditional industrial image processing field, engineers follow Moore's Law and use standard CPUs for their image processing applications. This solution is not resource aware and does not work for embedded applications. The restrictions of the embedded field do not allow the use of oversized general purpose hardware architectures. Specialized cores have less power, resource and area consumption. This lead to the usage of more application-specialized computing architectures such as GPUs, DSPs or own specialized circuits utilizing FPGAs. Therefore, not only software engineers, but especially hardware engineers, application engineers and system designers are needed, in order to cover all parts of such a system development. With an automated design flow and compiler, high-level synthesis tools give engineers the opportunity for developing image processing systems without a deeper knowledge of hardware architectures. This tools offer a holistic view for system design and automated mapping strategies. However the results of high-level synthesis tools are often suboptimal and not fully developed. They are often not specialized for a specific domain, e.g. image processing. The do not consider image processing specialized hardware architectures such as the Full Buffering. Therefore, the Image Processing Architecture Synthesis (IPAS)[1] describes a new way for image processing design, by considering the algorithm access pattern, the hardware architectures and the polymorphism of image processing algorithms. The system designer is able to create an image processing application in an abstract layer like UML, without any deeper knowledge of hardware architecture[2]. With global constraints (e.g. fps, power consumption, accuracy) in the abstract specification the designer has the opportunity to alter the system architecture for their purposes.

[1] C. Hartmann, A. Deitsch, M. Reichenbach., D. Fey, and R. German, "A holistic approach for modeling and synthesis of image processing applications for heterogeneous computing architectures." in *HIS workshop. design, automation and test in europe (DATE)*, 2015, pp. 28–29.

[2] C. Hartmann, M. Reichenbach., and D. Fey, "IPOL - a domain specific language for image processing applications," in *Proceedings of the international symposium on international conference on systems*, 2015, pp. 40–43.

6.7 Energy Consumption of Video Decoding Systems

Christian Herglotz (christian.herglotz@FAU.de)
Supervisor/s: Prof. Dr.-Ing. André Kaup

In the past two decades, video codecs became more and more sophisticated enabling video compression with extremely low bitrates at high visual qualities. To achieve this, a high number of novel and complex coding tools was introduced such that the complexity and hence the energy consumption of state-of-the-art video codecs has increased dramatically. As nowadays, a common use case of video playback is online streaming on portable and battery constrained devices, energy efficient video coding is of high interest as the operating times of these devices could be extended.

To this end, this thesis focuses on two major topics: Energy modeling and energy saving. For the first one, extensive tests and studies have been performed to construct valid and useful energy models. Therefore, different hard- and software solutions for video decoders were measured and characterized. Our research revealed that the decoding energy for state-of-the-art HEVC video decoders can be modeled using different approaches: The decoding time[1], bit stream[2] or high-level features of the coded sequence[3], or instruction counts and memory accesses of the underlying processing unit. Estimation errors as well as advantages and disadvantages of the models have been studied extensively such that depending on the use case and requirements of an application, a suitable model can be chosen.

Our current research deals with the second topic. Here, novel methods are applied to achieve energy savings without losing image quality. In the most promising approach, the classic rate-distortion optimization algorithm in the encoder is extended to a decoding-energy-rate-distortion optimization, where next to the classic parameters rate and distortion also the decoding energy is considered. To this end, the bit stream feature based model from the first topic is incorporated into the encoder such that energy saving encoding decisions can be taken. Extensive tests with different soft- and hardware will be performed and the influence of the transmission via a wireless network will also be considered. First results indicate that at the expense of a small bitrate increase, energy savings of around 10% can be achieved[4].

[1] C. Herglotz, E. Walencik, and A. Kaup, "Estimating the HEVC decoding energy using the decoder processing time," in *Proc. international symposium on circuits and systems (ISCAS)*, 2015, pp. 513–516.

[2] C. Herglotz, D. Springer, and A. Kaup, "Modeling the energy consumption of HEVC P- and B-frame decoding," in *Proc. international conference on image processing (ICIP)*, 2014, pp. 3661–3665.

[3] C. Herglotz and A. Kaup, "Estimating the HEVC decoding energy using high-level video features," in *Proc. european signal processing conference (EUSIPCO)*, 2015.

[4] C. Herglotz and A. Kaup, "Joint optimization of rate, distortion, and decoding energy for HEVC intraframe coding," in *Submitted to international conference on image processing (ICIP)*, 2016.

6.8 Advanced Image Processing for Optical Coherence Tomography Angiography

Lennart Husvogt (lennart.husvogt@fau.de)
Supervisor/s: Prof. Dr.-Ing. Andreas Maier, Prof. Dr.-Ing. Joachim Hornegger

Age-related macula degeneration (AMD) is the major cause of blindness in the western world, diabetic retinopathy (ER) is the leading cause of blindness among patients aged 20 to 61 and glaucoma is the leading causes for blindness worldwide. Angiographic imaging using optical coherence tomography (OCT) is a non-invasive modality that allows to image structural and angiographic data from the retina in micrometer resolution. OCT angiography has already been used to successfully image blood vessel alterations associated with AMD[1] and glaucoma[2].

It is this project's goal to develop methods to identify structural and functional markers of early disease or disease progression from OCT angiography data using image processing and machine learning algorithms. Potential markers are density, size and tortuosity of retinal vessels, size of the foveal avascular area and areas of dropout in the choriocapillaris. Furthermore, structural markers can also be taken into account, such as drusen, loss of retinal pigmental epithelium and thicknesses of retinal layers.

For OCT angiography, the same location is imaged multiple times (up to five times) and observed changes in the structural data indicate blood flow. A major challenges is the prevalence of motion artifacts in acquired volume data, for which our group already developed a working solution[3].

So far, a GPU accelerated OCT angiography pipeline has been developed, which is used by clinical collaborators at New England Eye Center and our collaborators from the group of Prof. James G. Fujimoto from the Biomedical Optical Imaging and Biophotonics Group at the Massachusetts Institute of Technology. A new visualization method for the combined display of structural and angiography OCT data sets has been submitted to Arvo 2016 and has been accepted.

[1] E. Moult, W. Choi, N. K. Waheed, M. Adhi, B. Lee, C. D. Lu, V. Jayaraman, B. Potsaid, P. J. Rosenfeld, J. S. Duker, and J. G. Fujimoto, "Ultrahigh-speed swept-source OCT angiography in exudative AMD," *Ophthalmic surgery, lasers & imaging retina*, vol. 45, no. 6, p. 496—505, 2014.

[2] Y. Jia, E. Wei, X. Wang, X. Zhang, J. C. Morrison, M. Parikh, L. H. Lombardi, D. M. Gattey, R. L. Armour, B. Edmunds, M. F. Kraus, J. G. Fujimoto, and D. Huang, "Optical coherence tomography angiography of optic disc perfusion in glaucoma," *Ophthalmology*, vol. 121, no. 7, pp. 1322–1332, 2014.

[3] M. F. Kraus, J. J. Liu, J. Schottenhamml, C.-L. Chen, A. Budai, L. Branchini, T. Ko, H. Ishikawa, G. Wollstein, J. Schuman, J. S. Duker, J. G. Fujimoto, and J. Hornegger, "Quantitative 3D-OCT motion correction with tilt and illumination correction, robust similarity measure and regularization," *Biomedical optics express*, vol. 5, no. 8, p. 2591—2613, August 2014.

6.9 Scalable Global Illumination

Benjamin Keinert (benjamin.keinert@fau.de)
Supervisor/s: Prof. Marc Stamminger

The synthesis of realistic images is an important topic in the field of computer graphics. In order to generate convincing and realistic images it is necessary to involve the effects of global illumination. This is often implemented by the use of Monte Carlo methods such as path tracing[1], bi-directional path tracing[2] and Metropolis Light Transport[3].

In order to use the above methods, ray casting the scenes' geometry is crucial. In our paper "Enhanced Sphere Tracing"[4] we present methods to enhance performance and quality for the ray casting of procedural distance bounds. Additionally improvements of these techniques can be found in our article "Improved Ray Casting of Procedural Distance Bounds"[5].

Further, we investigated the use of spherical Fibonacci (SF) points set for the storage of signals on spherical surfaces. These point sets are easy to generate and yield nearly uniform sample distributions on the unit sphere. We developed an efficient inverse mapping algorithm for SF Point Sets[6], which finds the nearest neighbor in an arbitrarily sized SF point set for an arbitrary point on the unit sphere in constant time. This inverse mapping allows the use of SF point sets for a variety of applications. Among other things we showcased its use for texture mapping, unit vector quantization and procedural modeling.

Further research will include the development of image synthesis algorithms incorporating machine learning techniques.

[1] J. T. Kajiya, "The rendering equation," in *Proceedings of the 13th annual conference on computer graphics and interactive techniques*, 1986, pp. 143–150.

[2] E. P. Lafortune and Y. D. Willems, "Bi-directional path tracing," in *Proceedings of the third international conference on computational graphics and visualization techniques (COMPUGRAPHICS '93)*, 1993, pp. 145–153.

[3] E. Veach and L. J. Guibas, "Metropolis light transport," in *Proceedings of the 24th annual conference on computer graphics and interactive techniques*, 1997, pp. 65–76.

[4] B. Keinert, H. Schäfer, J. Korndörfer, U. Ganse, and M. Stamminger, "Enhanced Sphere Tracing," in *Smart tools and apps for graphics - eurographics italian chapter conference*, 2014.

[5] B. Keinert, H. Schäfer, J. Korndörfer, U. Ganse, and M. Stamminger, "Improved ray casting of procedural distance bounds," *J. Graphics Tools*, vol. 17, no. 4, pp. 127–138, 2015.

[6] B. Keinert, M. Innmann, M. Sänger, and M. Stamminger, "Spherical fibonacci mapping," *ACM Trans. Graph.*, vol. 34, no. 6, pp. 193:1–193:7, Oct. 2015.

6.10 Image Reconstruction from Pixels Located at Non-Integer Positions

Ján Koloda (jan.koloda@fau.de)
Supervisor/s: Prof. Dr.-Ing. André Kaup

Digital images are commonly represented as regular two-dimensional arrays, so pixels are organised in form of a matrix. Pixels within the matrix are then addressed by a pair of integers denoting the corresponding row and column. This regular representation offers multiple advantages. First, it allows an efficient implementation of the acquisition hardware so image sensors are typically manufactured as uniform arrays of light sensitive cells. Second, due to the simple indexing, displaying systems also rely on this type of image representation. Moreover, this representation provides an elegant mathematical tool that facilitates further processing of visual data.

However, the rapid growth of various multimedia applications is imposing new challenges on processing the visual information. In particular, the reconstruction of images from samples located at non-integer positions, called floating mesh, is becoming a crucial step for many tasks. There is a wide range of applications that produce pixels lying on the floating mesh. Such is the case of super-resolution, frame rate up-conversion, depth-based image rendering, optical cluster eye, parallax adjustment, video coding, generation of new views in multicamera systems or fisheye imaging, among many others. These applications turn to be useful in many fields, ranging from surveillance and medical imaging to automotive and entertainment industry. However, the samples on the floating mesh cannot be directly displayed nor efficiently coded so pixels on the regular grid have to be reconstructed.

The vast majority of image reconstruction techniques assumes that the input image is already a regular 2D grid. In general, this is a fundamental assumption so these techniques cannot be extended to the generic mesh-to-grid reconstruction scenario. In order to deal with samples located on the floating mesh, we have proposed a denoising-based refinement framework that aims at improving the reconstruction quality[1]. It relies on the assumption that the reconstruction error can be regarded as additive noise so it is susceptible to denoising. We have designed an adaptive denoising strength controlling mechanism that applies strong denoising to large reconstruction errors while small errors are corrected only slightly or not at all.

Simulations have confirmed an important improvement in reconstruction quality. Current investigations include applying this denoising-based reconstruction technique to super-resolution and fisheye imaging problems.

[1] J. S. J. Koloda and A. Kaup, "Denoising-based Image Reconstruction From Pixels Located at Non-Integer Positions," in *Proceedings of the IEEE International Conference on Image Processing (ICIP)*, Québec, Canada, September 2015, pp. 4565–4569.

6.11 Compressed Geometry Representation for Ray Tracing

Alexander Lier (alexander.lier@fau.de)
Supervisor/s: Prof. Marc Stamminger

The main purpose of global illumination is the creation of realistic images. To do so many different methods of light simulation and approximation have been invented and are still researched. However, all these methods require very fine detailed, thus memory demanding scene models to produce high quality images. This leads to larger acceleration structures, thus the overall memory requirements increase even further, which eventually may result in limitations regarding usable architectures. When a specific limit is reached, GPUs and mobile devices are no longer capable to hold the demanded amount of data, and eventually can no longer be utilized.

There are various approaches to tackle previously mentioned problems. At first the acceleration structure can be compressed without losing detail on geometry level. Additionally it is possible to compress the geometry itself. Most of the methods compressing the accelerations structure rely on quantization[1], whereas the compression of the geometry is mostly realized by avoiding redundancy, for example by utilizing triangle-strips[2]. Finally it is also possible to exchange the geometry with a sufficient approximation, for example height-fields[3], but simultaneously introduce an error.

Nevertheless, further compression without losing detail nor introducing an error is desirable. Currently we are working on a compressed representation for ray tracing parametric surfaces, which surpasses the state-of-the-art method[4] regarding compression by a factor of 2 without introducing an error and by a factor of 16 if we allow minor deviations. As a result of the reduced memory demand even large or very detailed scenes can fit on the GPU memory and thus its performance can be harnessed. Alternatively it is possible to render more detailed models on mobile devices or other limited architectures.

[1] J. A. Mahovsky, "Ray Tracing with Reduced-Precision Bounding Volume Hierarchies," PhD thesis, University of Calgary, 2005.

[2] C. Lauterbach, S.-e. Yoon, M. Tang, and D. Manocha, "ReduceM: Interactive and Memory Efficient Ray Tracing of Large Models," *Computer Graphics Forum*, vol. 27, no. 4, pp. 1313–1321, 2008.

[3] J. Novák and C. Dachsbacher, "Rasterized Bounding Volume Hierarchies," *Computer Graphics Forum*, vol. 31, no. 2, pp. 403–412, 2012.

[4] I. Wald, S. Woop, C. Benthin, G. S. Johnson, and M. Ernst, "Embree–A Ray Tracing Kernel Framework for Efficient CPU Ray Tracing," *ACM Transactions on Graphics (Proceedings of ACM SIGGRAPH)*, 2014.

6.12 ASIP Generation for Image Postprocessing Tasks

Tobias Lieske, Marc Reichenbach (tobias.lieske@fau.de, marc.reichenbach@cs.fau.de)
Supervisor/s: Prof. Dr.-Ing. Dietmar Fey

Complex image processing tasks can be divided into pre- and postprocessing steps. As preprocessing steps often exhibit fixed processing and data accessing patterns, application-specific hardware implementations can be generated due to the similarities between the different preprocessing operators.

Postprocessing algorithms on the other hand do not have that many similarities in general between different operators and often do not feature predictable data access patterns. This makes the generation of application-specific postprocessing architectures extremely difficult. However, implementing an application-specific hardware architecture by hand is possible to perform a certain postprocessing operation with strict constraints, although the implementation is an extremely time-consuming task.

As the flexibility of a programmable architecture greatly reduces development time, software implementations of postprocessing algorithms are preferred. However, the flexibility of general purpose programmable architectures causes a loss in performance compared to the application-specific hardware implementation, which is crucial for embedded real-time image processing applications.

One way to trade of flexibility and performance are application-specific instruction set processors (ASIPs). By constraining the flexibility of a processor to a certain application field, the architecture can be optimized for the required processing steps, resulting in an improved performance, while maintaining constraints for embedded processing.

Due to the wide variety of processing steps and data access patterns in image postprocessing algorithms, it is hard to find one specific ASIP architecture that allows the implementation of any image postprocessing algorithm and simultaneously holds all user constraints. Thus resulting in the need for different, more specialized ASIP architectures for different subsets of postprocessing algorithms. But designing a new ASIP from scratch is again a extremely time-consuming task.

By thoroughly analyzing different postprocessing algorithms, we want to extract general similarities in the processing scheme and the performed arithmetic, such as buffer structures, parallel processing, complex instructions, synchronization mechanisms, etc., that are shared among different postprocessing algorithms. This information will then be used to characterize a configurable ASIP architecture for image postprocessing. A configuration will then determine the structure of the processor architecture and properties of certain components that were derived from the analysis, such as the size of a buffer or the arithmetic function of a complex instruction.

This allows the user to design new ASIP processors within minutes and to control design parameters such as performance, power consumption and area. The goal is to automatically derive a synthesizable HDL description from an architecture configuration.

6.13 Material Decomposition Algorithms for Spectral Computed Tomography

Yanye Lu (yanye.lu@fau.de)
Supervisor/s: Prof. Dr.-Ing. Andreas Maier

Currently, X-ray Computed Tomography (CT) is a widely used x-ray scanning technique that facilitates nondestructive examination in medical and industrial fields, allowing the user to see inside the object non-destructively. Spectral CT was introduced as an improvement CT technology in 1975, which dedicates to gain spectral information on the energy dependent attenuation properties of the object, achieving superior imaging performance and quantitative measurement for the nondestructive examination. The corresponding spectral CT algorithms are dedicated to solve the problems of distinguishing the objective materials that yield the same range of CT numbers in a standard CT image, as well as the quantitative material information, e.g., concentrations or atomic number information of the material constituents. Since the algorithm development is crucial in spectral CT research, many research efforts are dedicated to this area, especially to the clinical purpose of material decomposition.

Material decomposition is an application of spectral CT that enables identification and separation of different chemical components, which has mostly been applied for separation of contrast medium (high-iodine concentration) and bone (high-calcium concentration) for improved bone removal. Material decomposition is based on the fact that the attenuation difference between the high- and the low-kilovolt setting varies between chemical elements according to their x-ray properties, most importantly the K-edge. The material decomposition algorithms are investigated in dozens of papers in the literature, which enable us to summarize the fundamental limits and the challenges.

Machine learning, which have large impact on many segments of science and industry, concerns the construction and study of systems that can learn from data. In past decades, machine learning has evolved from a field of laboratory demonstrations to a field of significant commercial value, made significant inroads in pattern recognition including object recognition, natural language processing, bioinformatics and so forth, even in medical diagnosis. Due to the huge potential, it is very attractive for involving machine learning approaches into the spectral CT algorithm development. This project dedicates to develop material decomposition algorithm using machine learning approaches, proposing novel algorithms for spectral CT applications.

6.14 Iterative Reconstruction Methods for Abdominal Water-Fat MRI

Felix Lugauer (felix.lugauer@fau.de)
Supervisor/s: Prof. Dr.-Ing. Andreas Maier, Prof. Dr.-Ing. Wolfgang Schröder-Preikschat

The signal acquired from MRI is proportional to the density of hydrogen nuclei. The diagnostical value of a measurement can increase significantly when the signal from fat bound hydrogen nuclei is suppressed or exactly measured. The fact that fat-bound hydrogen nuclei have a slightly differing resonance frequency from those bound in water can be used for an exact determination of the signal spectrum. In recent years, this approach for signal separation gained increased interest since it enables both quantitative fat measurements and improved fat suppression compared to conventional methods. However, additional measurements are required causing a lengthened acquisition. Our aim is to reduce the acquisition time by iterative reconstruction techniques.

Scan time reduction via conventional imaging based on non-iterative reconstruction is restricted by a low SNR, which is typically attributed to multi-echo abdominal imaging. Further data reduction at the cost of even lower SNR introduces noise amplification and, consequently, potential bias in quantitative measurements. A reconstruction that iteratively performs denoising based on sparsity assumptions of the signal while ensuring fidelity to the sparsely measured data enables to reconstruct images with higher SNR. Known as Compressed Sensing (CS) for MRI[1], it promises reconstruction from a few sparse samples subject to incoherent acquisition and compressible representations.

For accelerated imaging via CS, we aimed to exploit the redundancies within the multi-echo image series as they show the same anatomical properties at different intensity contrasts. Exploiting that the signal variation is limited by the number of independent spectral components, we proposed an echo-coupled reconstruction using a local low-rank (LLR) regularization[2] and compared this to spatial sparsity regularization via finite differences. LLR showed improved SNR and reduced artifacts for a 6-fold accelerated acquisition using retrospective undersampling[3]. After adapting the MR scanner software to directly acquire sparse data, we conducted a study with 10 volunteers that demonstrated the same accuracy in quantitative measurements and a higher SNR while reducing the acquisition time from 19 to 14 s compared to conventional imaging.

This project is in collaboration with Siemens Healthcare, Erlangen, Germany.

[1] M. Lustig and others, "Compressed Sensing MRI," *Signal Processing Magazine, IEEE*, vol. 25, pp. 72–82, 2008.

[2] J. Trzasko, A. Manduca, and E. Borisch, "Local versus Global Low-Rank Promotion in Dynamic MRI Series Reconstruction," in *Proc. Int. Symp. Magn. Reson. Med*, 2011, p. 4371.

[3] F. Lugauer and others, "Water-Fat Separation Using a Locally Low-Rank Enforcing Reconstruction," in *Proc. Int. Symp. Magn. Reson. Med*, 2015, p. 3652.

6.15 Dynamic Thread Migration for Heterogeneous Coprocessor Systems for Image Processing Applications

Rainer Müller (raimue@cs.fau.de)
Supervisor/s: Daniel Lohmann, Wolfgang Schröder-Preikschat

To enhance the throughput of image processing applications, hardware coprocessors can help to offload computational tasks. The host CPU is responsible for the main scheduling of threads that start computations to be run on the coprocessor, which often uses a distinct instruction set architecture and manages its own local memory. Thus, such systems with coprocessors inherently form heterogeneous architectures.

Advances in chip technology enabled the production of coprocessors offering many general-purpose cores. For example, the Intel Xeon Phi allows execution of up to 244 hardware threads in parallel on a single PCIe extension card. The common technique to program these general-purpose coprocessors is to use source code annotations for sections that should be executed on the coprocessor. The compiler then generates optimized machine code depending whether the section is meant to be executed on the host CPU or on the coprocessor, with a runtime system handling the control-flow transition.

However, while waiting for the results from the coprocessor, the host CPU will not be used for computation. This behavior is especially an issue when the host system has one or more CPUs consisting of multiple cores each. This processing power will not be used at all during the execution on the coprocessor. Furthermore, usually a single program is granted exclusive access to the whole coprocessor in the system, even if the application cannot execute on all cores due to constraints in parallelism.

These drawbacks of inefficient resource usage should be solved by migrating threads dynamically between the host system and the coprocessor. Migration decisions at runtime would allow better usage of the available resources due to possible adaptation to the current load on both the host system and the coprocessors. In the case of the Intel Xeon Phi, host and coprocessor also share a common subset of their instruction sets. The compatible ISA reduces the cost of the migration itself as the common state does not require transformation and latency can be hidden with a *copy-on-demand* policy. As both architectures can execute a common machine code, unnecessary or short migrations can be avoided. By merging code for both architectures into *fat binaries*, the machine-specific instructions such as vector operations can still be used for performance improvements. The binary for an application could even contain code for different coprocessors and automatically use those available to the host system.

Overall, this proposed approach for dynamic thread migration will help to utilize coprocessors outside the domain of high-performance computing, which is currently their main use.

6.16 High Level Synthesis from Domain-Specific Languages

Mehmet Akif Özkan (akif.oezkan@fau.de)
Supervisor/s: Dr. Frank Hannig and Prof. Dr. Jürgen Teich

A great variety of hardware architectures exist to meet the requirements of the image systems in terms of speed, power, energy, and cost. Heterogeneous platforms including GPUs, FPGAs and CPUs have become very popular to exploit individual benefits. Moreover, parallel programming models (e.g. CUDA, OpenCL) are emerged to control and program many core processor systems. Yet, using existing programming tools, writing high performance image processing programs require sacrificing readability, portability, and modularity. Diversity in hardware architectures and programming models require a high development effort and expert knowledge of underlying architecture. Numerous attributes should be added and data management should be carefully considered for efficient coding. Excessive design time, even for experts, makes FPGAs even more unattractive although the energy efficiency, up to 1000x, and the throughput can be significantly increased over GPUs[1].

In this work we investigated Altera's OpenCL high level synthesis (HLS) tool for FPGAs. Thanks to OpenCL HLS, an accelerator cannot only be generated but also be controlled as a component in a heterogeneous system like GPU programming. However, experimental results show that the code generation is significantly more successful when the HLS code is written in hardware development manner. As an example, clamping boundaries on a small 5-by-5 mean filter, processing 8-bit pixels, increased the logic utilization of the logic resources from 18% to 42% of an Altera Cyclone-5 FPGA. On the other hand, a hardware approach, in which a pipeline mechanism and multiplexing conditional statements are strictly described as if designing with a HDL, reduced the effect of boundary condition to smaller than 0.01% of logic utilization. Moreover, the size of the code is increased 10x in this way. We propose to use domain-specific characteristics of image processing applications so that a source-to-source compiler can generate efficient implementations. In this context we developed an Altera OpenCL compiler backend for HIPA^{cc}—The Heterogeneous Image Processing Acceleration Framework[2]. Moreover, we extended it with a vectorization mechanism, which is not supported by OpenCL HLS for pipelined code, that can be configured by compiler flags. Finally, we compared the resulting hardware accelerators to existing HLS frameworks and GPU implementations, generated by the same DSL, in terms of power and performance requirements.

[1] M. Schmid, O. Reiche, F. Hannig, and J. Teich, "Loop coarsening in C-based high-level synthesis," *Proceedings of the 26th IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP)*, pp. 166–173, 2015.

[2] R. Membarth, O. Reiche, F. Hannig, J. Teich, M. Körner, and W. Eckert, "HIPAcc: A domain-specific language and compiler for image processing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 1, pp. 210–224, 2016.

6.17 Processing Architectures for Heterogeneous 3D-ICs

Benjamin Pfundt (benjamin.pfundt@fau.de)
Supervisor/s: Prof. Dr.-Ing. Dietmar Fey

State-of-the-art image processing systems still employ only few transmission connections. The read-out of current CMOS image sensors is still limited to a couple of serial links, although the pixel array could be read out in parallel. Also, in the domain of smart cameras where e.g. pattern recognition tasks lead to a data reduction, the transfer rate for raw sensor images inside the camera is often the limiting factor. This bottleneck is mainly due to the planar layout of image sensor and processing chips which poses a limited possibility for interconnects. The solution which has been looked forward to for years has now become a reality: modern IC design enables the stacking of single chips, but more importantly, these chips can be connected by a multitude of so called through-silicon vias (TSVs). One of the first companies offering this technology known as 3D chip stacking is Tezzaron which provides TSVs as small as 1.2 micrometer in diameter. Other renowned semiconductor manufactures like STMicroelectronics or Austrian Micro Systems slowly catch up.

Besides a dramatically higher bandwidth, other advantages arise from a chip stacked assembly. For example, the footprint of the final chip decreases heavily while the single layers can easily operate in parallel e.g. as a pipeline. At the same time, the interconnect length is reduced, thus low latencies can be achieved. Furthermore, the integration of heterogeneous ICs which have been fabricated in different technologies becomes possible. This avoids an error prone large mixed signal design on a single chip. Unfortunately, the high integration density in chip stacked systems renders heat dissipation and thermal stress critical. To cope with the possibilities of 3D ICs and to mitigate the problems, new processing architectures have to be devised.

Together with another subproject of the research training group we developed a exemplary chip stack for pre-processing purposes[1]. In this collaboration, our focus was on the digital processing layer, while an image sensor with parallel read-out and possible analog processing capabilities has been topic of the other group. In our 3D IC, raw pixel data is transmitted via TSVs directly to the digital processing layer where filter masks can be applied to e.g. detect edges or reduce noise. Due to local data dependencies of the filter kernels, parallelism can be exploited easily. Therefore, both the sensor and the processing layer is partitioned into tiles which are processed in parallel. A special full buffering scheme is applied to save resources and thus alleviate the thermal stress. Due to the parallel transmission and the low latency of the short interconnects, high frame rates can be achieved which are especially beneficial for real-time applications.

[1] B. Pfundt, M. Reichenbach, C. Söll, and D. Fey, "Novel Image Processing Architecture for 3D Integrated Circuits," *Parallel-Algorithmen und Rechnerstrukturen*, vols. Mitteilungen - Gesellschaft für Informatik e.V., pp. 5–15, 2015.

6.18 Consistent Programming Models and Tools for Designing Heterogeneous Image Systems

Oliver Reiche (oliver.reiche@cs.fau.de)
Supervisor/s: Dr. Frank Hannig and Prof. Dr. Jürgen Teich

The variety of different image systems and their requirements has led to the need for various architecture types. Many compute-intensive image processing applications can be sped up by running them in parallel on special graphics processors (GPUs), massively parallel processor fields, or reconfigurable field programmable gate arrays (FPGAs), in contrast to conventional processors (CPUs). In particular on embedded devices, harnessing the processing power of these parallel and heterogeneous platforms is essential to meet performance and power constraints at the same time. State of the art parallel programming models for GPUs (e.g., CUDA, OpenCL, Renderscript) enable efficient programming and optimization on a low abstraction level, which is time-consuming and does not cover the need for performance portability. To target FPGAs, C-based High-Level Synthesis (HLS) promises to ease the process of hardware accelerator generation, but still requires a high development effort and architecture expert knowledge.

In this project, we research methods and tools to efficiently map a wide range of image processing algorithms to heterogeneous architectures. Inspired by domain-specific characteristics, the programming takes place on a higher abstraction level like the HIPA^{cc} framework[1] for medical image preprocessing. Using this approach, efficient implementations can be created without the need for an architecture expert and therefore increases the productivity and flexibility for writing algorithms. Furthermore, for FPGAs finding the right design point between achieving as much throughput as necessary while spending as few resources as possible is a challenging task. By elevating the description of image algorithms to such a higher abstraction level, an automatic optimization process can be applied to give the algorithm developer even more control over trading execution time for resource usage[2].

This project is structured as follows: Imaging applications within the different GRK projects are analyzed and certain reoccurring tasks are reduced to their core functionality. With respect to a specific application domain, a domain-specific language can be designed, which allows to easily express an algorithm by using a common description in a succinct and readable way. Hereby, the algorithm is decoupled from any architecture-specific characteristics, which ensures a high productivity and flexibility.

[1] R. Membarth, O. Reiche, F. Hannig, J. Teich, M. Körner, and W. Eckert, "HIPAcc: A domain-specific language and compiler for image processing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 1, pp. 210–224, Jan. 2016.

[2] O. Reiche, K. Häublein, M. Reichenbach, M. Schmid, F. Hannig, J. Teich, and D. Fey, "Synthesis and optimization of image processing accelerators using domain knowledge," *Journal of Systems Architecture*, vol. 61, no. 10, pp. 646–658, Oct. 2015.

6.19 Feature Selection and Motion Models for Feature-Based Rigid 2-D/3-D Registration

Roman Schaffert (roman.schrom.schaffert@fau.de)
Supervisor/s: Dr.-Ing. Anja Borsdorf and Prof. Dr.-Ing. Andreas Maier

In interventional radiology, live X-ray images are used in order to guide the surgeon during the procedure. As important anatomical structures may not be visible in these images, preoperatively acquired 3-D images such as CT- or MRI-scans can be overlaid with the 2-D image in order to visualize such structures. 2-D/3-D registration methods are used in order to estimate the pose of the 3-D image for the overlay.

A feature-based tracking[1] and registration method has been developed at the pattern recognition lab for the registration of CT to live fluoroscopic images which can cope especially well with registration using a single 2-D image. This method makes use of a motion model which is able to estimate rigid 3-D transformations from 2-D displacements of a set of points.

In this research project, feature point selection methods and motion model extensions are explored which can further improve the robustness as well as the accuracy of the registration method. Although different point-of-interest extraction methods are described in the literature, the setting in medical 2-D/3-D registration is unique in that the imaged objects are translucent for the X-ray imaging system. Also, the criteria for the desired points in our registration method differs from that of typical point-of-interest-based applications. The selection of good points is done adapting to the use case. This includes feature selection depending on the body regions which are registered as well as different acquisition parameters, and therefore different image quality. Extensions of the motion model are also considered to make optimal use of the displacement information which can be gained depending on the feature properties (for example, only a 1-D component of the displacement can be estimated at edge points due to the aperture problem while 2-D displacement can be estimated at corners).

This project is in collaboration with Siemens Healthcare GmbH, Forchheim, Germany.

[1] J. Wang, A. Borsdorf, B. Heigl, T. Kohler, and J. Hornegger, "Gradient-Based Differential Approach for 3-D Motion Compensation in Interventional 2-D/3-D Image Fusion," in *3D vision (3DV), 2014 2nd international conference on*, 2014, vol. 1, pp. 293–300.

6.20 Scalable Global Illumination

Kai Selgrad (kai.selgrad@fau.de)
Supervisor/s: Prof. Marc Stamminger

The central component of global illumination simulations is the determination of visibility between scene positions. Employing this information diffusion of light can be computed. Determining visibility between scene elements is, however, a global problem and as such computationally demanding, in contrast to local illumination which does not include visibility. The lack of such global illumination strongly decreases visual quality. Search for efficient solutions to the problem of visibility determination is, since long, an active area of research.

Visibility can be computed by directly accessing the scene geometry (Ray Casting), which is usually accurate, but suffers from being computationally expensive. Recent advances improve performance by better adaption to the underlying hardware, both on CPUs and GPUs, as well as by general algorithmic considerations.

Schemes based on Shadow Mapping are generally fast and mostly useful to estimate visibility between scene positions and a light source. This representation is a discretized subset of the scene geometry visible from the position of the light source (which also causes a number of artefacts).

Another, more recent, branch of visibility estimation is the use of a voxel based scene representation. The voxelized scene representation, however, suffers from discretization artefacts as well as from being overly conservative.

The main objective of our efforts is to improve upon existing algorithms[1,2] and devise new solutions[3,4] to the visibility problem which are not confined to a specific platform[5,6] and allow to scale the quality of the results to the level provided by the performance of a given target platform.

[1] K. Selgrad, J. Müller, and M. Stamminger, "Faster Ray-Traced Shadows for Hybrid Rendering of Fully Dynamic Scenes by Pre-BVH Culling," in *Smart tools and apps for graphics - eurographics italian chapter conference*, 2015.

[2] C. Benthin, S. Woop, M. Nießner, K. Selgrad, and I. Wald, "Efficient Ray Tracing of Subdivision Surfaces using Tessellation Caching," in *Proc. high-performance graphics 2015*, 2015.

[3] K. Selgrad, C. Dachsbacher, Q. Meyer, and M. Stamminger, "Filtering Multi-Layer Shadow Maps for Accurate Soft Shadows," *Comput. Graph. Forum*, vol. 34, no. 1, pp. 205–215, Feb. 2015.

[4] K. Selgrad, C. Reintges, D. Penk, P. Wagner, and M. Stamminger, "Real-time Depth of Field Using Multi-layer Filtering," in *Proceedings of the 19th symposium on interactive 3D graphics and games*, 2015, pp. 121–127.

[5] K. Selgrad, A. Lier, M. Wittmann, D. Lohmann, and M. Stamminger, "Defmacro for C: Lightweight, Ad Hoc Code Generation," in *Proceedings of ELS 2014 7rd european lisp symposium*, 2014, pp. 80–87.

[6] K. Selgrad, A. Lier, F. Köferl, M. Stamminger, and D. Lohmann, "Lightweight, Generative Variant Exploration for High-performance Graphics Applications," in *Proceedings of the 2015 ACM SIGPLAN international conference on generative programming: Concepts and experiences*, 2015, pp. 141–150.

6.21 A Tone Mapping Algorithm Suited for Analog-Signal Real-Time Image Processing

Lan Shi (lan.shi@fau.de)
Supervisor/s: Prof. Robert Weigel and Prof. Marc Stamminger

Since the last two decades, the researchers in the area of digital image processing and computer graphics have studied a variety of tone mapping methods and algorithms to adjust the high dynamic range of image data to the limited dynamic range of conventional displays. An image processing in the digital domain has the advantage of disposition of data acquisition, flexibility of calculation complexity. But the computation time is too long to apply a Tone Mapping Operator (TMO) as a real-time processing on camera sophisticatedly.

Our research presents an analog domain TMO which is based on Photographic Tone Reproduction (PTR) and is suited for analog circuit design in a CMOS image sensor in order to reduce the hardware cost and operation time for real-time image processing. The characteristic advantage and calculation limitation of analog technology are considered in the TMO algorithm proposal. The appropriate modelling is built and simulated in Verilog-A. And the function of the algorithm is feasible for analog processing from pixel to pixel without parallel accessing or buffering of any other pixel value. The overflow problem is not yet considered in the computing circuit, it will be taken into account in on-going research based on it will be taken into account in on-going research[1]. The input parameter can be calibrated by photography environment or be set manually by user.

Further research will investigate the CMOS-integrated circuit design of the proposed analog TMO. The analog circuit noise, inaccuracies and overflow problems, specially in arithmetical circuits, will be considered in circuit design. Furthermore, a stage-pipeline for speed-up of the analog computing could also be implemented as an enhancement to this study at the next step.

[1] C. Soell, L. Shi, A. Baenisch, J. Roeber, T. Ussmueller, and R. Weigel, "Analog computation methods with the help of analog and pseudo-digital carry signals," in *Circuit theory and design (ECCTD), 2015 european conference on*, 2015, pp. 1–4.

6.22 Integrated Circuits for Analog Signalprocessing in Heterogeneous Image Systems

Christopher Soell (christopher.soell@fau.de)
Supervisor/s: Prof. D. Fey and Prof. R. Weigel

Common digital camera systems exclusively process the raw image data in the digital domain, where complex algorithms can be implemented fairly easy, but also require a large amount of processing time. This is critical in real time systems, especially due to the growing number of pixels in modern image sensors. In order to accelerate the processing, several digital algorithms shall be transferred to the analog domain, which are significantly faster and consume less chip area and power. Moreover, for special smart camera systems only required to execute specific tasks like edge or marker detection, these algorithms can be processed in the analog domain exclusively without the need for power-hungry ADCs or digital processing stages.

Therefore, an image sensor system is developed and modified, that is able to execute analog computations[1]. Thereby, occurring overflows constitute a special challenge and have to be handled adequately[2]. Performed algorithms so far include tone mapping, de-noising, debayering and edge detection. As these do not only need the values of one pixel, but also take spatial information into account, the image sensor has been developed that is able to readout a 3x3 pixel array simultaneously. After the analog processing, the image data is then converted by an ADC to allow further digital processing.

Another interesting topic investigated in this sub-project is the use of memristors for digital multi-level memories and/or analog memories to accelerate image processing with signed-digit ALUs and reduce chip area.

[1] C. Soell, L. Shi, A. Baenisch, T. Ussmueller, and R. Weigel, "A CMOS image sensor with analog pre-processing capability suitable for smart camera applications," in *2015 international symposium on intelligent signal processing and communication systems (ISPACS)*, 2015, pp. 279–284.

[2] C. Soell, L. Shi, A. Baenisch, J. Roeber, T. Ussmueller, and R. Weigel, "Analog computation methods with the help of analog and pseudo-digital carry signals," in *Circuit theory and design (ECCTD), 2015 european conference on*, 2015, pp. 1–4.

6.23 Memory and Interface Architectures for Tightly Coupled Processor Arrays

Éricles Sousa (ericles.sousa@cs.fau.de)
Supervisor/s: Dr.-Ing. Frank Hannig and Prof. Dr.-Ing. Jürgen Teich

Coarse-Grained Reconfigurable Arrays (CGRAs) have emerged as a powerful solution to speedup computationally intensive applications. Heterogeneous MPSoC architectures containing such reconfigurable accelerators have the advantage of providing high flexibility, power-efficiency, and high performance. During my research, I have been working on new solutions for a class of CGRAs called tightly coupled processor arrays (TCPAs). The development of new architecture components (e.g., buffers and reconfigurable bus arbitration) is necessary to embed a TCPA into a heterogeneous MPSoC architecture. TCPAs are programmable hardware accelerators well suited for domain-specific computing from the areas of signal, image, and video processing as well as other streaming processing applications

My current investigations have already presented some major benefits of using TCPAs in the context of resource-aware computing. For instance, we showed efficiency and utilization improvements by algorithmic selection of different resources on an MPSoC architecture. More specifically, we presented how to exploit a dynamic load balancing between multiple RISC cores and TCPAs in order to satisfy different requirements as quality or throughput.

Furthemore, considering a scenario where multiple processors are accessing shared resources (e.g., cache, memory, and bus), we proposed a runtime reconfigurable bus arbitration technique[1] for providing timing predictable execution of concurrent applications on MPSoC architectures.

My recent research also investigates how to accelerate computationally intensive applications on CGRAs by means of increasing data reuse. We developed a reconfigurable buffer architecture[2] that can be configured at runtime to select between different schemes for memory access. We have successfully showcased the benefits of our approach by prototyping a heterogeneous MPSoC architecture containing a RISC processor and a TCPA. The architecture is prototyped in FPGA technology and considering image processing algorithms, we demonstrated that our proposed buffer structures for system integration allow to considerably increase the memory bandwidth utilization.

[1] É. Sousa, D. Gangadharan, F. Hannig, and J. Teich, "Runtime reconfigurable bus arbitration for concurrent applications on heterogeneous MPSoC architectures," in *Proceedings of the EUROMICRO Digital System Design Conference (DSD)*, 2014, pp. 74–81.

[2] É. Sousa, F. Hannig, and J. Teich, "Reconfigurable buffer structures for coarse-grained reconfigurable arrays," in *Proceedings of the International Embedded Systems Symposium (IESS)*, 2015, pp. 01–11.

6.24 Real-time Facial Expression Transfer

Justus Thies (justus.thies@fau.de)
Supervisor/s: Günther Greiner

Based on the improvements of RGB-D cameras and increased horse power of modern GPUs, it is possible to invent new algorithms that are able to reconstruct / represent the world within real-time framerates. In the facial expression transfer project we concentrate our work on the reconstruction and tracking of human faces.

The reconstruction of a human face is an important step before one can track a face. In **„Interactive Model-based Reconstruction of the Human Head using an RGB-D Sensor"**[1] we demonstrate an approach of face reconstruction that is based on a morphable model. The used morphable model is a PCA-basis of a database of 300 scanned faces. This model spans the space of faces with only a few parameters (i.e. 160 parameters for shape and 160 parameters for the albedo). Using this model we are able to reconstruct a 3D face model with a higher resolution than the input data of a RGBD-camera (e.g. a Kinect).

In **„Real-time Expression Transfer for Facial Reenactment"**[2] we also incorporate facial expressions in our model. Using the presented approach we are not only able to reconstruct the shape and the expression, but are also able to modify the face parameters. Beside manipulation of lighting conditions and texture, we demonstrate our tracking in a live reenactment setup. This system allows the user to transfer his expressions to a video stream of another person in real-time. Since we change the expression of the target person, we only have to modify the region of the video that is covert by the face. This is done by rendering the modified face model on top of the input video. The resulting quality is nearly photo-realistic. Based on this technique many new applications are possible. Imagine a multilingual video-conferencing setup in which the video of one participant could be altered in real time to photo-realistically reenact the facial expression and mouth motion of a real-time translator. Application scenarios reach even further as photo-realistic reenactment enables the real-time manipulation of facial expression and motion in videos while making it challenging to detect that the video input is spoofed. This publication also lead to a wide discussion in the media and highlights that beside photos also videos and even live-streams can be spoofed.

[1] M. Zollhöfer, J. Thies, M. Colaianni, M. Stamminger, and G. Greiner, "Interactive model-based reconstruction of the human head using an RGB-D sensor," *Comput. Animat. Virtual Worlds*, vol. 25, no. 3-4, pp. 213–222, May 2014.

[2] J. Thies, M. Zollhöfer, M. Nießner, L. Valgaerts, M. Stamminger, and C. Theobalt, "Real-time expression transfer for facial reenactment," *ACM Trans. Graph.*, vol. 34, no. 6, pp. 183:1–183:14, Oct. 2015.

6.25 Topological Triangle Sorting for predefined Camera Routes

Christoph Weber (christoph.weber@cs.fau.de)
Supervisor/s: Prof. Marc Stamminger

Graphical fidelity on mobile devices is limited. Developers have to reduce energy consumption and heat emission, or the devices simply lack the necessary processing power. The oncoming generations of mobile hardware will only increase this scarcity of performance, much less solve it. One reason is the advent of UltraHD or 4k resolution displays, as it quadruples the workload of mobile GPUs which bareley cope to process HD or 1k images.

For some years now, automobile manufacturers use mobile GPUs to render user interfaces and virtual scenes on displays implemented in the dashboard. Unlike the common interactive exploration associated with computer graphics, this new kind of *automotive visualization* is fully predictable. Car developers define and verify every possible rendering configuration during production and demand that the final product meets the design with pixel-perfection. Using precomputed videos instead of on-site renderings appears to be the obvious but is impractical because the visualizations are highly car-specific and varied. As a result, automotive rendering is uniquely challenging, both regarding to quality and efficiency.

Our previous research addressed the problem of increasing quality of lighting with regard to the limited graphics hardware of mobile GPUs[1].

Our current research utilizes the restrictiveness of automotive renderings. Because we have knowledge of everything that is to be rendered, we can remove invisible data and use the freed resources to improve the quality of the visible geometry. We extend this simple idea and group the scene depending on the visibility over the course of a fixed camera route. Moreover, we implement a sliding window that rolls over the scene data and efficiently renders only the visible parts. This implementation is extended by sorting the triangles depth-wise. Rendering can be done either back-to front or front-to-back. This removes the need of depth tests and allows for a single pass alpha-blending.

[1] C. Weber and M. Stamminger, "Stateless Level of Detail Lighting for Automotive Visualization," in *Proc. Smart Tools and Apps for Graphics*, 2014, pp. 29–36.

6.26 Facilitate Memory Management for CT Reconstruction on GPUs

Hao Wu (haowu@cs.fau.de)
Supervisor/s: Prof. Wolfgang Schröder-Preikschat, Prof. Marc Stamminger

Many tasks in medical image processing have a high computational complexity. However, the performance of such algorithms is often crucial for the underlying procedure. Nowadays, most computers have a heterogeneous structure and allow for parallelized computations on multi-core CPUs or many-core Graphics Processing Units (GPUs). To increase the performance, more and more algorithms exploit such heterogeneous systems by executing computations in parallel. In medical imaging, a large amount of research has been conducted to lower the execution time by using modern GPUs. An important application is the fast back- and forward projection for CT image reconstruction. Significant speedup factors were achieved by outsourcing these computations to GPUs. This substantial improvement has also led to an increased interest in iterative reconstruction algorithms, as they are more and more able to perform in clinically relevant time constraints.

A key problem when using GPUs is that the programming of such devices can still be tedious, as the developer needs to be familiar with specific syntaxes, such as CUDA or OpenCL. Although unified memory architectures have been proposed by industry, many of the devices still use separate memory nodes for CPUs and GPUs, connected by a PCIe bus. Thus, a large amount of the algorithm development is dedicated to the memory-management implementation. Large volume sizes in image reconstruction can easily exceed the memory size of common GPUs, especially when time-resolved methods are of interest that require multiple instances of such volumes. A solution is to subdivide the data into smaller blocks, however, this also imposes additional complexity for the algorithm developer.

With our recent work[1], we provide a library that is able to automatically manage the GPU memory for arbitrary problem sizes and hardware restrictions. We show that the proposed library is able to ease GPU programming and can even improve system throughput due to an overlapping of data transfers and execution. In following work, efficiently cooperating CPUs & GPUs for medical image processing will be considered. To maintain workload balancing and alleviate data transfer, the scheduling policy proposed in our previous work[2] can be potentially incorporated.

[1] H. Wu, Berger, Maier, and D. Lohmann, "A Memory Management Library for CT Reconstruction on GPUs," in *Bildverarbeitung für die Medizin Workshop (BVM16)*, 2016.

[2] H. Wu, D. Lohmann, and W. Schröder-Preikschat, "A Graph-Partition–Based Scheduling Policy for Heterogeneous Architectures," in *Proceedings of the DATE Friday Workshop on Heterogeneous Architectures and Design Methods for Embedded Image Systems (HIS 2015)*, 2015, pp. 22–27.

7 RTG 1780: CrossWorlds - Connecting Virtual and Real Social Worlds

Prof. Dr. Maximilian Eibl (maximilian.eibl@informatik.tu-chemnitz.de)
Technische Universität Chemnitz
www.crossworlds.info

The Research Training Group "Connecting Virtual and Real Social World" addresses the increase in digitization and its resulting virtualization of processes, communication, environments, and finally of the human counterparts. The nature and the degree of virtualization vary significantly, and they depend considerably on the context of application. In addition, media-mediated communication is always restricted in comparison with real-world communication.

Our goal is to overcome the current constraints of media-mediated communication. In doing so, we will study which new ways of interaction and communication are offered by the connection of virtual and real social worlds in comparison with the experience of immediate real interaction and communication. The research program subdivides the connection between virtual and real social environments into the fields of: communication, emotions, sensomotorics, and learning. Research in these areas is performed within interdisciplinary research tandems consisting of computer scientists and social scientists on a doctoral, postdoctoral, and on the supervisory level.

The qualification program is based on the objective of the Research Training Group, which is explicitly focused on joint technology-oriented and social-scientific-oriented media research. Seminars and workshops, some of them to be organized by the fellows, are focused on the research topics of the fellows. Furthermore, tutorials prepare the fellows for the challenges of the national and international scientific community. The qualification program is completed by visits of designated guest scholars.

7.1 Context-aware Collaboration of Humans, Services, and Things

Markus Ast (markus.ast@informatik.tu-chemnitz.de)
Supervisor/s: Prof. Dr.-Ing. Martin Gaedke

The complexity of today's missions and tasks for knowledge work is increasing. This is contrary to the requirements of reducing effort and costs for planning, conducting and eventually re-planning knowledge work. More and more missions and tasks have to be organized fast and efficiently. As missions and tasks tend to change frequently due to unforeseen aspects, time- and cost-efficient mission management is a critical problem and requires sophisticated support from information technology. Even though recent research in the area of UI mashups, End User Development and Semantic Web yielded many helpful solutions to address challenges in knowledge work - the overall aspect of systematically carrying out tasks in a collaborative and goal-oriented way hasn't gained much attention so far. The lack of suitable abstractions and supporting platforms makes it difficult to profit from context-dependent service access, goal-oriented planning, and composition of diverse actors from the Internet of Humans, Services and Things.

The goal of this research is to facilitate context-aware collaboration of humans, services, and things in order to help organizations and individuals in conducting missions in knowledge work. The concept of a mission is modeled around two essential parts: ends and means. Ends are the motivation behind the mission and means are the course of action for achieving them. Management of ends (commonly known as Goal Management) is critical for actual success of missions. We believe that the concept of means and ends can not only be applied as a motivation-model for humans, but also as a concept for integrating services and things in knowledge work missions in a self-organizing way.

To achieve the overall goal, the research project targets the following objectives: 1) Supporting the development and evolution of interactive compositions of Humans, Services and Things by end-users under critical constraints. 2) Enabling trustworthy goal-oriented coordination of services and resources in multi-user scenarios according to contextual conditions. 3) Incorporation of mental state and stress level of users into means of interactions and context-awareness during execution of missions. 4) Formalization of means, ends and environmental conditions using Linked Data to facilitate the composition of Humans, Services, and Things. 5) Employment of distributed and self-organizing mission entities taking constraints like disconnected operation, intermediate connections, and limited bandwidth into account. 6) Supporting authentication and authorization mechanisms in order to enable trustworthy collaborations of distributed entities of the internet of Humans, Services, and Things.

In the end, the achievement of these objectives should enable multi-user mission planning and execution using smart, context-aware and goal-oriented composition of Humans, Services, and Things.

7.2 Digital Tangibles – Connecting Digital Worlds to their Physical Environments

Benedikt Etzold (benedikt.etzold@informatik.tu-chemnitz.de)
Supervisor/s: Prof. Dr. Maximilian Eibl

Tabletops have been in the focus of Human-Computer Interaction for about 20 years. By arranging user interfaces on public or semi-public displays, these devices create environments that enable users to operate applications both alone or in larger groups[1].

This concept has been significantly extended with the introduction of tangible user interfaces by Hiroshi Ishii and Brygg Ullmer in 1997. By connecting analog objects to digital information, they developed a much more direct approach to manipulating entities of the application's digital context[2]. In 2010, Malte Weiss et al. proposed a set of translucent controls, which can - to a certain extend - be modified to give dynamic feedback regarding their appearance, purpose, state, etc[3].

This dissertation project focuses on combining and expanding all these approaches and making them accessible for tabletops of any design including systems missing the tracking abilities of proprietary solutions or extensive self-constructions relying on projection techniques. By using smart phones and tablet computers as tangible objects, applications can be designed to make use of active communication and a great amount of flexibility. In addition to using them as input devices, their screens allow for displaying parts of the user interface directly on the handheld unit. Sensors like cameras or RFID readers even support the inclusion of secondary objects.

The resulting architecture can provide an interesting new link between analog and digital objects. Users can explore their physical environment and then import certain aspects of it as tools onto their handheld devices. These can be used to manipulate information or interface elements that are part of the context of the tabletop.

The research focus lies on different aspects like application design, multi-device networks, multi-screen scenarios, visualization, communication, interaction and participation.

[1] C. Müller-Tomfelde and M. Fjeld, "Tabletops - horizontal interactive displays," Springer London, 2010, pp. 1–24.

[2] H. Ishii and B. Ullmer, "Tangible bits: Towards seamless interfaces between people, bits and atoms." in *Proceedings of the ACM SIGCHI conference on human factors in computing systems*, 1997, pp. 234–241.

[3] M. Weiss, J. D. Hollan, and J. Borchers, "Tabletops - horizontal interactive displays," Springer London, 2010, pp. 149–170.

7.3 Combining Attentional Modulation to Motion Detection as found in the Visual Pathway of the Mammalian Brain

Tobias Höppner (tobias.hoeppner@informatik.tu-chemnitz.de)
Supervisor/s: Prof. Dr. Fred H. Hamker

Attention enhances the relevant parts of the visual to higher cortical processing areas. In the spotlight metaphor attention directs the focus of a additional signal to the visual field. This additional signal modulates the underlying receptive fields and either enhances or diminishes the field's strength. So, parts of the visual field will be more prominent or more unknown to further cortical processing.

From our everyday experience we know that motion events will instantaneously draw attention. This thesis intents to show that this effect can be modeled by combining an attention model[1] with a model for extraction motion cues. The extraction of motion is a tough task and part of an ongoing debate where in the mammalian brain motion is processed. Models for the extraction of motion range from artificial filter models to biologically plausible models[2]. In this thesis a motion model will be used which aims for biological plausible mechanisms. This model was developed by Heeger and Simoncelli[3] and uses Gabor-like filter units.

Together with a established motion detection model this thesis will show that motion cues direct the focus of attention. After combining the two models a test phase is planned. Different stimuli which are used by experimentalists will form the input to the model. The results can then be compared to findings in the literature and the model can be fine tuned to different experimental set ups. As a far goal we want to underpin the hypothesis that attention and motion processing mutually connected.

[1] F. Beuth and F. H. Hamker, "A mechanistic cortical microcircuit of attention for amplification, normalization and suppression," *Vision Res.*, vol. 116, no. Part B, pp. 241–257, Nov. 2015.
[2] D. J. Heeger, E. P. Simoncelli, and J. A. Movshon, "Computational models of cortical visual processing," *Proc. Natl. Acad. Sci.*, vol. 93, no. 2, pp. 623–627, 1996.
[3] E.P. Simoncelli and D.J. Heeger, "A Model of Neuronal Responses in Visual Area MT," *Vision Res.*, vol. 38, no. 5, pp. 743–761, 1998.

7.4 A neuro-computational model of emotional attention

René Richter (rene.richter@cs.tu-chemnitz.de)
Supervisor/s: Prof. Dr. Fred Hamker

Emotions influence our daily decisions and direct our attention to the most valuable stimuli to focus processing resources. In order to transfer this emotional attention to the computer, a biologically realistic model of it must be developed.

The questions arising is, how these stimuli acquire their emotional value and how they can influence attentional processes. Evidence suggests that this association might be learned through conditioning in the amygdala, more specifically the basal lateral amygdala (BLA). Furthermore, feedback connections from the BLA to the visual cortex seem to enhance the activation of neural representations which is a possible top-down attention mechanism.

While neuro-computational models of attention mechanisms attract increasing interest due to their importance for the focused processing of information in the brain, the possible emotional feedback from the amygdala is to date largely unexplored. Therefore, we propose a rate-coded, biological realistic neuro-computational model constructed of 3 smaller functional models.

First, a model of the visual processing pathway for object recognition[1] that includes the retina, the lateral geniculate nucleus, the visual areas V1, V2 and V4 as well as the frontal eye field has been combined with an amygdala model for the associative conditioning of a visual stimulus with a bodily reaction that represens a particular emotional state. Second, in order to provide the model with realistic temporal learning properties, a reward-timing model[2] using the dopamine system as a basis has been integrated to adjust the learning process by dopamine-mediated modulation of plasticity. The timing model includes a number of brain areas, most prominently the ventral tegmental area, the nucleus accumbens, the lateral hypothalamus, the ventral medial prefrontal cortex and the amygdala.

[1] F. Beuth and F. H. Hamker, "A mechanistic cortical microcircuit of attention for amplification, normalization and suppression," *Vision Res.*, vol. 116, pp. 241–257, Nov. 2015.

[2] J. Vitay and F. H. Hamker, "Timing and expectation of reward: a neuro-computational model of the afferents to the ventral tegmental area," *Front. Neurorobot.*, vol. 8, pp. 1–25, Jan. 2014.

7.5 The ‚Escape-Button' as the only way out – When Human-Computer-Interaction breaks down

Ingmar Rothe (ingmar.rothe@phil.tu-chemnitz.de)
Supervisor/s: Prof. Dr. Claudia Fraas

With the increasing presence of interactive interfaces in everyday life, interactions between humans and computers reach new quantity and quality. Multi-touch displays and public displays are installed in public spaces, aiming at making people interact. People have to deal with the specific offer that the computer behind the surface makes, and sometimes they have to overcome various obstacles to use it, e.g., limited access, unknown rules, or terms of use in another than the user's language.

In order to minimize obstacles, designers try to build intuitive displays and software. At the same time observations suggest that people expect intuitive usability. Thus, for users, unsuccessful interactions with the computer may be very disappointing: They run the risk of breaking down. Users often do not try to find a way to make things work but they break down the interaction by using the 'escape button'. So this break down becomes a double failure: The user fails with using the machine. The machine fails with keeping the user in interaction.

A case study 'in the wild' will address the following questions: How do users deal with the break down? or, What can we learn about (un)successful tabletop-design from the users' interactions?

The data has been recorded on the multi-touch tabletop ‚ComforTable'[1], placed at the Museum of Industry Chemnitz. Being installed in an exhibition, its' main mission is to bring visitors togehter to discuss the exhibition's content. The ComforTable was developed within the interdisciplinary research-training-group 'CrossWorlds' (DFG grant #1780) at the TU Chemnitz.

[1] M. Storz, K. Kanellopoulos, C. Fraas, and M. Eibl, "Designing with Ethnography: Tabletops and the Importance of their Physical Setup for Group Interactions in Exhibitions," *i-com*, vol. 14, no. 2, pp. 115–125, Aug. 2015.

7.6 Multi User Dialog Interfaces for Mobile Robots

René Schmidt (rene.schmidt@informatik.tu-chemnitz.de)
Supervisor/s: Prof. Dr. Wolfram Hardt

In the last years, numerous mobile robots has been developed for the usage in museum areas. Robotinho[1] and Fritz[2] are just two examples, which shows that museum guides has been established in museums. Most of the robots interact with the user by using a touch interface. Anyway, the most intuitive way to communicate is the human speech.

Robotinho[1] and Fritz[2] already provide some rudimentary spoken dialog systems, but for the usage on a mobile robot it is just possible to use embedded systems which have limited processing speed and resources. This leads to a big challenge of spoken dialog systems on mobile robots. The processing time on embedded devices is still too long. Actual solution insert fillers, in order to indicate the user that the processing still proceeds.[3] However, psychological research shows that the break between question and answer has to depend on the context.[4]

In Order to generate an intuitive conversation with a robot, a full calculable system is necessary. For this purpose, the new SoC technologies from Altera and Xilinx provide new possible solutions. The combination of ARM processor and FPGA allows the outsourcing of functionality with high processing times to the FPGA, which can provide high data throughput and constant processing times based on his pipeline architectures. The goal is to use an optimized Hardware Software Partitioning to generate a multiuser dialog interface with constant processing times based on the SoC technology. With this approach a deterministic process is generated and provides the needed calculability to adapt the processing time on the context to generate a more intuitive dialog system.

[1] F. Faber, M. Bennewitz, and et.al., "The humanoid museum tour guide robotinho," in *Robot and human interactive communication, 2009. RO-MAN 2009. the 18th IEEE international symposium on*, 2009, pp. 891–896.

[2] M. Bennewitz, F. Faber, D. Joho, and S. Behnke, "Fritz-a humanoid communication robot," in *Robot and human interactive communication, 2007. RO-MAN 2007. the 16th IEEE international symposium on*, 2007, pp. 1072–1077.

[3] T. Shiwa and et al., "How quickly should communication robots respond?" in *Human-robot interaction (HRI), 2008 3rd ACM/IEEE international conference on*, 2008, pp. 153–160.

[4] S. Strömbergsson and et al., "Timing responses to questions in dialogue." in *INTERSPEECH*, 2013, pp. 2584–2588.

7.7 Modeling Load Factors in Multimedia Learning: An ACT-R Approach

Maria Wirzberger (maria.wirzberger@phil.tu-chemnitz.de)
Supervisor/s: Prof. Dr. Günter Daniel Rey

From a cognitive perspective, learning operates on a variety of cognitive processes related to information capture, storage and retrieval, which heavily rely on learners' mental resources. In particular the increasing digitalization of learning facilities has far-reaching implications for instructional settings. Despite the enhanced potential of multimedia teaching and learning opportunities in capturing motivation and engagement amongst learners, the inherent multimodal, interactive and often distributed presentation of information is heavily prone to overload learners' mental capacities. As a consequence, impairing effects on learning performance could result. This project accepts the arising challenge, and investigates selected aspects of learner cognition resulting from media-related learning content on a more detailed level. A prominent theory within this field of research, the Cognitive Load Theory[1], specifies distinct factors that contribute to overall demands arising from instructional situations: Task complexity based on learners' previous knowledge constitutes intrinsic load, while effects of inappropriate instructional presentation add to extraneous load. Additionally, schema acquisition and automation characterize germane load. When attempting to investigate relevant cognitive features underlying such aspects, existing methods of load measurement like subjective questionnaires or physiological indicators face limitations in terms of accessibility, effort and the lack of sensitivity and diagnosticity. Experimental manipulation indeed provides a controlled way of assessment, but the inspection of performance-related outcome measures operates on indirect means as well. For this reason, a cognitive model using the cognitive architecture ACT-R[2] should be developed, since it holds great benefits for clarifying cognitive determinants at a fine grained level. Such provides the opportunity to derive vested predictions about effects of load factors on learners' performance while they have to cope with certain instructional contents. The chosen approach bases upon a biologically validated theoretical framework of information processing modules that are able to explain basic and constant mechanisms of cognition. Furthermore, it offers a computational platform for model execution, which allows to directly test predictions on task-related behavior.

[1] J. Sweller, P. Ayres, and S. Kalyuga, *Cognitive load theory*. Springer Science + Business Media, 2011.
[2] J. R. Anderson, *How can the human mind occur in the physical universe?* Oxford University Press, 2007.

8 RTG 1817: UbiCrypt - New Challenges for Cryptography in Ubiquitous Computing

Prof. Dr. Alexander May (alex.may@rub.de)
Ruhr-Universität Bochum
http://www.ubicrypt.hgi.rub.de/

We are in the midst of the shift toward ubiquitous computing. Mobile multimedia devices with DRM services, intelligent web applications, medical implants that communicate or car-to-car communication have become reality. Such ubiquitous applications are typically not confined to well-defined networks but communication takes place between small embedded nodes and the "cloud", a large and often not well defined network consisting of PCs and servers. Many of the new applications are heavily dependent on security features, for instance telemedicine or intelligent traffic management. Many current security solutions are not applicable any more, e.g., because of a lack of clear network boundaries, resource-constrained devices or new security requirements like anonymous payment schemes on mobile tokens.

The Research Training Group (RTG) will investigate cryptographic mechanisms which form the foundation for security solutions in ubiquitous computing. The research is structured in three levels: cryptographic primitives, device and system level. A common theme is that new cryptographic methods are researched for applications which are distributed and heavily inhomogeneous. The research topics range from cryptographic foundations such as fully homomorphic encryption, which is very desirable for privacy reasons, over security for medical implants to internet security solutions involving new national ID cards.

A central goal of the training plan is an interdisciplinary and structured Ph.D. phase with an innovative two-advisor concept, a close coupling with the RUB Research School and mandatory research visits at leading international research groups. A high quality education is assured by tailored graduate courses, seminars and annual summer schools.

8.1 Differential privacy from the perspective of learning theory

Francesco Aldà (francesco.alda@rub.de)
Supervisor/s: Prof. Dr. Hans Ulrich Simon

The goal of private data analysis is to enable rich and useful statistics on a dataset to be performed while simultaneously preserving the privacy of the users whose data are included in the dataset. The typical scenario is when a trusted party (e.g. hospital, public institution) holds a dataset of sensitive information (e.g. medical records, voter registration information) and is required to provide publicly available statistical information about the dataset.

The trade-off between privacy and usability has attracted a great deal of attention in many different fields, from statistics and theoretical computer science to security. In their seminal work, Dwork et al.[1] introduced the notion of differential privacy, which has become one of the most important paradigms for privacy-preserving statistical analyses. Among its several properties, this definition guarantees that an adversary can gain no information on the data of a specific user by observing the result of the statistics.

In our research, we aim at analysing the issues of private data analysis (under differential privacy) in terms of statistical learning problems. In particular, we study the connections between these two fields, exploring the relevance of models and notions of learning theory in the field of private data analysis. An example of such a connection was recently established by Gupta et al.[2]. In this work, they considered the private query release problem in a distributed setting. This problem consists in designing a differentially private mechanism able to answer a set of statistical queries Q on a dataset up to small error, but the access to the data itself is restricted to statistical queries only. Gupta et al. showed that this challenging problem can be solved if and only if the query class Q is agnostically SQ-learnable. Starting from the important result presented by Gupta et al., we replaced their worst-case analysis by a kind of average-case analysis[3]. While their analysis establishes the very high barrier of agnostic SQ-learnability, our main result shows that the barrier in the average-case, namely weak SQ-learnability under the uniform distribution, is much lower.

[1] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Proc. of TCC '06*, 2006, pp. 265–284.

[2] A. Gupta, M. Hardt, A. Roth, and J. Ullman, "Privately releasing conjunctions and the statistical query barrier," *SIAM Journal on Computing*, vol. 42, no. 4, pp. 1494–1520, 2013.

[3] F. Aldà and H. U. Simon, "Randomized response schemes, privacy and usefulness," in *Proc. of AISec '14*, 2014, pp. 15–26.

8.2 Design and Analysis of Symmetric Primitives

Christof Beierle (christof.beierle@rub.de)
Supervisor/s: Prof. Dr. Gregor Leander

Symmetric cryptographic primitives, especially block ciphers, belong to the building blocks in communication security. Basically, a block cipher is a function mapping blocks of message bits to a ciphertext. This function is further parametrized by a secret key. Without knowledge of the key, an adversary should not be able to obtain any information from the ciphertexts. Nowadays, there is a demand for strong primitives especially designed for different kinds of applications and scenarios. For example, in lightweight cryptography, one seeks for secure designs optimizing efficiency with regard to a certain metric like chip area or energy.

Once a new cipher is proposed, the designers are expected to provide security arguments, at least against the most important and powerful attacks known, that are differential[1] and linear cryptanalysis[2]. Thus, any new design itself should allow for an, if possible simple, security argument. Nowadays, a huge amount of block ciphers is based on Substitution-Permutation (SP) constructions, which iterate both non-linear (substitution) and linear (permutation) operations. Usually, the substitution layer consists of parallel applications of smaller (non-linear) S-boxes.

A common measure of the resistance against differential and linear attacks is the minimal number of active S-boxes. In this context, an S-box is called active if it contains a non-zero input difference (resp. input mask). Unfortunately, not many constructions are known that guarantee a high number of active S-boxes without using computer-aided methods. One therefore may seek for alternative design principles.

One goal of this work is to investigate possible design criteria for cryptographic primitives, both in terms of optimizing efficiency and security. In this context, we already examined the influence of the ShiftRows-like operation on the minimal number of active S-Boxes in AES-like ciphers[3]. From the efficiency point of view, we constructed hardware-efficient linear layers by optimizing finite field multiplications with a fixed element[4].

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," in *Advances in cryptology-CRYPT0' 90*, vol. 537, Springer Berlin Heidelberg, 1991, pp. 2–21.

[2] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in cryptology — EUROCRYPT '93*, vol. 765, Springer Berlin Heidelberg, 1994, pp. 386–397.

[3] C. Beierle, P. Jovanovic, M. M. Lauridsen, G. Leander, and C. Rechberger, "Analyzing permutations for AES-like ciphers: Understanding ShiftRows," in *Topics in cryptology — CT-RSA 2015*, vol. 9048, Springer International Publishing, 2015, pp. 37–58.

[4] C. Beierle, T. Kranz, and G. Leander, "Lightweight multiplication in $GF(2^n)$ with applications to MDS matrices." Cryptology ePrint Archive, Report 2016/119, 2016.

8.3 Hardware security

Susanne Engels (Susanne.Engels@rub.de)
Supervisor/s: Prof. Dr.-Ing. Christof Paar

The aim of this thesis is to analyse different sides of hardware security in order to get an insight on both the attacker's as well as the designer's side regarding cryptographic hardware. The project can be divided into two parts:

The first part focusses on the field of cryptanalysis, where the goal is to overcome the security of a cryptographic system by gaining access to secret components. There exist various forms of cryptanalysis, ranging from analysing the underlying mathematical structure of a cryptographic algorithm to exploiting the physical properties of the implementation of such a cipher. Another approach is launching a brute-force attack, where, as the name induces, a cryptographic algorithm is broken using "brute force", for example by trying all possibilities of the secret key until the correct key is found. This form of attack usually requires a vast amount of computational power because security parameters are generally chosen appropriately large. Often, a single CPU solution is not sufficient, hence, in my doctoral project, we concentrate on brute-force attacks using special purpose hardware. Reprogrammable hardware such as FPGAs offer a structure that allows for large scale parallel programming and are often the platform of choice in the scientific world when a task can be parallelized. Although most cryptanalytic projects are stand-alone projects since they are dedicated to solving a specific problem as efficiently as possible, the acquired skills can be reused in subsequent problems.

In a second phase, we plan to slip into the role of the security engineer designing secure ciphers. Here, the attention is especially turned to securing hardware implementations against side-channel analysis. As opposed to other works which use common techniques such as masking and hiding, the aim is to follow the idea of obfuscating mathematical ciphers such that the attacker is no longer able to conduct hypotheses about the inner state of the cipher. Experience in working with FPGAs is of high importance when deciding where an obfuscation would achieve the best results. To validate what is possible and what is not, scrutinizing our own results and even attacking them again will be of high importance. All in all, in my doctoral project I aim to get a deep look into the field of cryptanalysis on implementation level, and how to successfully disable an attacker.

8.4 Ubiquitous Authentication

Maximilian Golla (maximilian.golla@rub.de)
Supervisor/s: Prof. Dr. Markus Dürmuth

User Authentication, meaning to prove an individual's identity, is an essential component in the design of a secure system.

In a current research project, we analyzed the security of personal knowledge questions, which are used to reset a forgotten password. Using the database of an online dating website, we evaluated statistical guessing metrics to study the security of real-world personal knowledge questions. For the analysis we considered an ideal attacker who knows the distribution of the answers across the population of users. This way we are able to provide a lower bound on the security against a real-world attacker who might only have an approximation of this information at hand. Our approach follows online guessing attack parameters and significance tests established in the literature. Our findings[1] confirm similar results, e.g., we found that the security depends to a certain extent on the age and the origin of a user. Further, we discovered that the favorite sports teams question is particular easy to guess and that in general personal knowledge questions only offer a low level of security. Thus, service providers should deploy more secure alternatives.

To provide a more secure memorable alternative, we explored an implicit memory-based solution. One way to trigger implicit memory is an effect called priming. We use such priming effects that are based on repetition and association of Mooney images for authentication. A Mooney image is a two-tone image that contains a single hidden object derived from an image. This object is hard to recognize at first sight. Once a subject has seen the original image from which the Mooney image was generated, recognition is much faster. During enrollment first a Mooney image, then the original image and a label that describes the object in the image, are presented to the user. At the authentication phase, the primed Mooney images and a disjoint subset of non-primed Mooney images are presented to the user in a randomized order. For each Mooney image presentation, the user is requested to type in the label of the object that the image contains, or skip the image. Authentication is based on the hypothesis that the user labels the primed images more often correctly than the ones the user was not primed on. We performed three user studies to be able to compare our solution to existing work and to observe long-term priming effects. Our findings[2] show that utilizing implicit memory can relieve a user from the burden of actively remembering a password. It significantly improves previous work by using Mooney images and an optimized scoring mechanism.

[1] M. Golla and M. Dürmuth, "Analyzing 4 Million Real-World Personal Knowledge Questions," in *International conference on passwords*, 2015, pp. 70–75.

[2] C. Castelluccia, M. Dürmuth, M. Golla, and F. Imamoglu, "Towards Implicit Visual Memory-Based Authentication,", Submitted.

8.5 Selective Opening Secure Public Key Encryption

Felix Heuer (felix.heuer@rub.de)
Supervisor/s: Eike Kiltz

One major research interest in cryptography is the design of encryption schemes that ensure the confidentiality of the encrypted messages. In the last decades indistinguishability of ciphertexts under chosen plaintext attacks (CPA security), resp. chosen ciphertext attacks (CCA security) became the standard notion of secure encryption. Interestingly, there is a natural scenario where these well-established security notions do not ensure confidentiality of the encrypted messages.

Consider a situation in the public key world where multiple parties, each holding the recipient's public key, send encrypted messages to a common receiver that has the corresponding secret key. Since we are in a public key world, any adversary can encrypt messages on its own. Additionally, the adversary somehow managed to corrupt the systems of some of the senders, not only revealing their encrypted message, but also the internal randomness used to encrypt the message. Such attacks are known as 'Selective Opening Attacks' and we would like to ensure some notion of confidentiality for messages sent by uncorrupted users. Intuitively speaking, we do not want the encrypted messages to reveal any information beyond information already leaked by the messages of corrupted users.

Recent negative results show that selective opening security is indeed a strictly stronger security notion, meaning that it does not come for free assuming only standard security holds. We are interested in achieving selective opening security for public key encryption schemes, trying to tackle the problem from multiple directions:

Our first approach led to new proofs for well-known and practical public key encryption schemes (RSA-OAEP and a variant of DHIES) in an idealised model. We proved that these schemes fulfill a strong notion of selective opening security only relying on the same assumptions needed to show standard security for those schemes[1].

Keeping the negative results in mind, another interesting line of ongoing research studies the natural question if standard security plus some special properties might already imply a weak notion of selective opening security. We obtained the first non-trivial result and showed that standard security implies selective opening security for 'low-dependence' message distributions, e.g. if the messages for a Markov chain[2].

[1] F. Heuer, T. Jager, E. Kiltz, and S. Schäge, "On the selective opening security of practical public-key encryption schemes," *PKC 2015 - Lecture Notes in Computer Science*, vol. 9020, pp. 27–51, Mar. 2015.

[2] G. Fuchsbauer, F. Heuer, E. Kiltz, and K. Pietrzak, "Standard security does imply security against selective opening for markov distributions," *TCC 2016-A - Lecture Notes in Computer Science*, vol. 9562, pp. 282–305, Dec. 2015.

8.6 GPS Security

Kai Jansen (kai.jansen-u16@rub.de)
Supervisor/s: Prof. Dr. Christina Pöpper

With advancements in aerospace engineering, the United States Department of Defense (DoD) began to develop a global satellite-based positioning system for military purposes in the 1970s. The system that we know today as the Global Positioning System (GPS) started full operation in 1995 with an intentionally degraded civilian version. After the shutdown of the degrading Selective Availability (SA) in May 2000, the now enhanced version became the de facto standard for time synchronization and determining geolocations.

Today, GPS is an integrated component of various safety-critical and security-critical applications such as load balancing in power grids, stock market transaction synchronization, air traffic control, or position-specific services. From a security point of view, civilian GPS suffers under the absence of any authentication or confidentiality mechanisms making it prone to so-called spoofing attacks.

Prominent Countermeasures like plausibility checks or physical parameter tests are often not practicable due to the resource constraint nature of GPS receivers. Our approach is to develop a spoofing detection system that can be realized with already deployed standard receivers. The underlying idea is based on the usage of multiple receivers in a predefined formation. With carefully evaluated design parameters, a violation of this formation allows us to identify spoofing attacks with a high detection rate and a low false alarm probability.

So far, we were able to substantially improvement the underlying model. With our improved model of correlated error sources, we can shrink distances to approx. 5 meters making the countermeasure applicable to much broader range, e.g., placement small ships or trucks. The resulting detection and false alarm ratios were analyzed to be in the order of 10^6, which is the same level or less than what was previously considered. As a proof of concept, we built a prototype which encountered no missed detections as well as no false alarms.

8.7 Lattice-based cryptography

Elena Kirshanova (elena.kirshanova@rub.de)
Supervisor/s: Prof. Dr. Alexander May

The major goal of cryptography is the construction of 'secure' functions (one-way functions) that are hard to break on average under some standard worst-case complexity assumption. It was Ajtai's discovery (1996) that turned lattices from a cryptanalytic weapon to an attractive tool for various constructions: if there is an adversary that breaks a scheme (even with some small probability), then this adversary can solve any instance of a certain geometric problem on this lattice. In contrast, for constructions based on number-theoretic assumptions, e.g. factoring in RSA, one has to assume that it is hard to factor n not only in the worst-case, but also on average for some suitable distribution on n.

One bottleneck in all of the lattice-based cryptographic primitives (which currently precludes lattices from being widely deployed) is the huge size of the keys. The parameters one has to choose in order to achieve the above worst-case hardness guarantee are extremely impractical. Thus, it is reasonable to ask, what is the best known algorithm for a lattice-problem that underlines a cryptographic primitive instantiated with certain (relaxed) parameters. In particular, we consider the Learning with error (LWE) problem, a variant of the Bounded-distance decoding problem, introduced by Regev (2005). This is a promise version of the Closest Vector problem, known to be NP-hard. The best known algorithm for solving CVP has exponential (in the lattice- dimension) running time and memory complexity. However, one might wonder how the promise (the distance guarantee in LWE case) changes the complexity, and hence, how to choose parameters for a cryptosystem. This is the question we address in our research.

At the current state of the research, we understand the asymptotic complexity of LWE problem under all known to-date algorithms. This means we can argue about some suggested parameter-sets and provide a rough estimate on the security-level achieved by these parameters. It is vital to be able to answer the question 'how large should I choose my parameters to achieve some security-level?' as it arises at the very first stage of deployment. Here we emphasize that the question of estimating the security-level of LWE-based crypto-primitives attracts lots of attention in cryptographic community also partially due to recent progresses towards building quantum computer. The Learning with Errors Problem is believed to be hard even in the presence of quantum adversary. Settling parameters for both efficient and secure cryptosystem is crucial if one wants to migrate from number-theoretic constructions.

8.8 Privacy

Katharina Kohls (katharina.kohls@rub.de)
Supervisor/s: Christina Pöpper

As part of their daily routine, many people leave traces of personal information throughout the Internet. This information remains available for long periods of time, even after the initial relevance of information may fade. Even though many online services suggest the possibility of deleting published information, e.g., profile pictures in social media, users ultimately have no control of data that once was stored at the servers of service providers. This becomes even more critical in presence of Internet censorship, where published information is monitored and eventually controlled by the censor. My research focuses on privacy enhancing techniques that allow users to regain control over private and sensitive information.

Neuralyzer[1] allows for assigning a lifetime to online data that, as soon as expired, revokes the access to uploaded information. Other than previous work in this field, Neuralyzer is based on access heuristics that trigger the revocation of data based on the interest in the respective files (examples: interest fades over time, unexpected excessive access, or manual revocation). This is possible through encrypting data before uploading it to a service, while the encryption key is stored in an external and public infrastructure. To revoke the access to a file the encryption key is destroyed and hence the decryption of data becomes impossible. Neuralyzer is a starting point for more sophisticated revocation systems and the utlization of alternate infrastructures for distributing the encryption keys.

In context of Internet censorship, SkypeLine[2] provides a hidden communication channel within Skype. It allows users to hide secret information in legitimate VoIP conversations that is protected from blacklisting or further censorship activities. SkypeLine utilizes a modulation technique that hides single bits of the secret within sequences of noise which are added directly to the audio signal of the conversation. As VoIP is a legitimate service even under censorship, this allows users to secretly exchange information through a public and unblocked communication channel. My future projects in the field of anti censorship systems will focus on the utilization of steganography techniques, e.g., for enhancing the security and performance of pluggable transports. Such transports are deployed to obfuscate traffic to services that are blocked through censorship authorities. One prominent use case for this is the anonymity network Tor.

[1] A. Zarras, K. Kohls, M. Dürmuth, and C. Pöpper, "Neuralyzer: Flexible expiration times for the revocation of online data," *ACM CODASPY*, 2016.

[2] K. Kohls, T. Holz, D. Kolossa, and C. Pöpper, "SkypeLine: Robust hidden data transmission for VoIP," *ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS)*, 2016.

8.9 Design and Analysis of Symmetric Primitives in Cryptology

Thorsten Kranz (thorsten.kranz@rub.de)
Supervisor/s: Gregor Leander

My doctoral project is about design and analysis of symmetric cryptography. Cryptography can be defined as communication in the presence of an adversary. Famous applications of this mathematical field in our everyday life are data encryption, user identification or data authentication. As an example, each banking transfer is protected by cryptographic algorithms. One distinguishes between asymmetric and symmetric cryptography where the latter one is the field of cryptography in which the users share a pre-defined secret, for example, a password.

Famous examples for symmetric cryptography applications are the Advanced Encryption Standard (AES) and the Secure Hash Algorithm 3 (SHA-3).

Symmetric primitives like encryption schemes, hash algorithms, and message authentication schemes are constantly designed and analyzed by the cryptographic research community. This is a very important process for improving their security and preventing the employment of weak cryptographic schemes.

In our research, we mainly focus on the area of Substitution-Permutation Networks. In this context, we analyze the characteristics of linear transformations and Substitution Boxes. Those are the two main building blocks of modern symmetric primitives. For analyzing such building blocks we often consider the two famous attack techniques of linear and differential cryptanalysis. We are especially interested in gaining better understanding concerning these attacks.

A fundamental understanding will very likely improve the performance of symmetric primitives. This is a very vivid research area because nowadays also small devices with restricted resources are equipped with cryptographic algorithms. This area is called Lightweight Cryptography and also one of our main research areas[1].

Another example of our current research is the decomposition of an SPN that is only given as a blackbox[2]. This is closely related to the so-called Integral Attack which is one of the most powerful attacks currently known against AES.

A third topic is the design of a lightweight block cipher which is software-optimized on 16-bit microcontrollers. Those microcontrollers might for example be used in wireless sensor networks. In this context, we also practically implement encryption schemes on the MSP430 which is a well-known 16-bit microcontroller from Texas Instruments.

[1] C. Beierle, T. Kranz, and G. Leander, "Lightweight Multiplication in GF(2^n) with Applications to MDS Matrices." Cryptology ePrint Archive, Report 2016/119, 2016.

[2] I. Dinur, O. Dunkelman, T. Kranz, and G. Leander, "Decomposing the ASASA Block Cipher Construction." Cryptology ePrint Archive, Report 2015/507, 2015.

8.10 Big Data

Robert Kübler (robert.kuebler@rub.de)
Supervisor/s: Prof. Dr. Alexander May

My thesis is about how to deal with huge amount of memory that is required in cryptographic settings. I am not designing cryptographic systems that require low memory, but instead I try to break cryptographic systems with lower memory requirements. For example, there are many algorithms for hard problems that require exponential memory, which is often the real bottleneck for actually solving the problem.

While waiting 2^{50} steps for solving a problem might still be feasible, keeping 2^{50} objects in memory might be the real problem here. Of course one can write objects to a harddisk, but then the performance of the algorithm will collapse, since reading and writing will take much longer time.

For example there is the LPN problem, it goes like this: Given natural numbers n (dimension) and m (number of queries), a real number p between 0 and 1 (error probability) and a secret binary vector s of dimension n. Given m pairs of the form $(a, < a, s >)$ where a is a uniform binary vector of dimension n and the second component is correct with probability $1 - p$, find s. There are several approaches to this problem, brute-force just picks every s and does some statistical testing whether it's the right one or not, which can be done in polynomial time and space. The time complexity is 2^n, the space complexity is polynomial.

Then there is the more sophisticated BKW algorithm, who does some kind of Gauss reduction, but tries to eliminate many variables at once instead of a single one in each step. The time complexity here is $2^{(n/log(n))}$, which is much better than the brute-force time complexity, but unfortunately this is also the space complexity, which is much worse than before. This means, that this algorithm can't be carried out in practice for reasonable values of n. Also, the running time is independent of the error p, which might be a problem for security estimations, because some cryptographic protocols use small values for p, for which there are more efficient algorithms, depending also on n.

I could apply techniques from the Decoding Theory to the LPN problem, which yield still fully exponential running times, but lower (still exponential) space complexities for reasonable parameters of n. These algorithms also take the error p into account, which pays off for very small p, used for example in the HELEN public-key cryptosystem, proposed by Alexandre Duc and Serge Vaudenay.

8.11 Cryptography from Hard Learning Problems

Daniel Masny (Daniel.Masny@rub.de)
Supervisor/s: Prof. Dr. Eike Kiltz

Most Public Key Encryption (PKE) schemes used in practice rely on the assumption that factoring or the discrete logarithm problem (DLOG) are hard. As shown by Shor[1], it is feasible for a quantum computer to factor or compute discrete logarithms.

There are alternative problems like decoding random linear codes, which is also called Learning Parity with Noise (LPN), or the lattice problem Learning with Errors (LWE). There is no quantum algorithm known that solves them efficiently. Therefore, these problems are suitable for post-quantum cryptography.

Starting with the HB protocol[2], there has been a variety of scientific effort to provide secure authentication from LPN. The idea behind the HB protocol is that it consists of very simple operations such that even humans could carry them out. In[3], we have extended this protocol such that security holds even against Man-in-the-Middle attacks. This gives stronger security guarantees than previous HB-like protocols have.

In[4], we have constructed a simpler chosen ciphertext (CCA) secure PKE scheme from a variant of LPN. We used a similar approach in[5] to construct a CCA secure PKE from Subset Sum.

Regev has shown that Learning with Errors (LWE) is at least as hard as the shortest vector problem (SVP)[6]. In[7], we have extended previous results that base the hardness of Learning with Rounding (LWR) on LWE to a wider range of parameters. In particular for the construction of pseudorandom number generators and functions, LWR is better suited than LWE.

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999.

[2] N. J. Hopper and M. Blum, "Secure human identification protocols," in *Advances in cryptology - ASIACRYPT 2001, 7th international conference on the theory and application of cryptology and information security, Gold Coast, Australia, December 9-13, 2001, proceedings*, 2001, vol. 2248, pp. 52–66.

[3] V. Lyubashevsky and D. Masny, "Man-in-the-middle secure authentication schemes from LPN and weak PRFs," in *Advances in cryptology - CRYPTO 2013 - 33rd annual cryptology conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, part II*, 2013, vol. 8043, pp. 308–325.

[4] E. Kiltz, D. Masny, and K. Pietrzak, "Simple chosen-ciphertext security from low-noise LPN," in *Public-key cryptography PKC2014 - 17th international conference on practice and theory in public-key cryptography, Buenos Aires, Argentina, March 26-28, 2014. proceedings*, 2014, vol. 8383, pp. 1–18.

[5] S. Faust, D. Masny, and D. Venturi, "Chosen-ciphertext security from subset sum," *IACR Cryptology ePrint Archive*, vol. 2015, p. 1223, 2015.

[6] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, no. 6, 2009.

[7] A. Bogdanov, S. Guo, D. Masny, S. Richelson, and A. Rosen, "On the hardness of learning with rounding over small modulus," in *Theory of cryptography - 13th international conference, TCC 2016-a, Tel Aviv, Israel, January 10-13, 2016, proceedings, part I*, 2016, vol. 9562, pp. 209–224.

8.12 Acoustic CAPTCHAs for Network Security

Hendrik Meutzner (hendrik.meutzner@rub.de)
Supervisor/s: Prof. Dr.-Ing. Dorothea Kolossa

A common method to prevent automated abuse of Internet services is to utilize challenge-response tests that distinguish human users from machines. These tests are known as CAPTCHAs (Completely Automated Public Turing Tests to Tell Computers and Humans Apart) and should represent a task that is easy to solve for humans, but difficult for fraudulent programs[1].

To enable access for visually impaired people, an acoustic CAPTCHA scheme is typically provided in addition to the better-known visual CAPTCHAs by most websites. Acoustic schemes are generally based on a sequence of spoken words, often using a small vocabulary, where the audio signals have been artificially distorted to harden attacks.

A major problem of current acoustic CAPTCHAs arises from a bad trade-off between human usability and robustness against automated attacks. Recent security studies show that most acoustic CAPTCHAs, albeit difficult to solve for humans, can be easily solved by means of computers. The primary goal of this research project is the development of novel acoustic CAPTCHAs that are more usable and secure than currently available ones. For example, we conducted a security and usability study of Google's famous reCAPTCHA where we found that our utilized speech recognizer was able to outperform the human listeners by a factor of 3. Based on our findings, we proposed an alternative CAPTCHA design by exploiting the effect of auditory streaming of the human auditory system. The proposed CAPTCHA design turned out to exhibit a better trade-off between human usability and security as compared to reCAPTCHA[2].

Our most recent work[3] proposes a universally usable type of CAPTCHA that is solely based on the classification of acoustic sound events, rendering the CAPTCHA independent of language skills and making it thus suitable for a broader group of users.

[1] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using Hard AI Problems for Security," in *Proc. EUROCRYPT*, 2003.

[2] H. Meutzner, V.-H. Nguyen, T. Holz, and D. Kolossa, "Using Automatic Speech Recognition for Attacking Acoustic CAPTCHAs: The Trade-off between Usability and Security," in *Proc. ACSAC*, 2014.

[3] H. Meutzner and D. Kolossa, "A Non-speech Audio CAPTCHA Based on Acoustic Event Detection and Classification," in *Proc. EUSIPCO*, 2016, submitted.

8.13 Leakage-Resilient Cryptographic Implementations

Tobias Schneider (tobias.schneider-a7a@rub.de)
Supervisor/s: Prof. Dr. Christof Paar

Most modern ciphers cannot be successfully attacked by traditional cryptanalysis. In practice however, an attacker can exploit vulnerabilities in the implementation of such a cipher to recover the secret. One type of these implementation attacks is based on the physical characteristics of the targeted device, e.g., power consumption. So called side-channel analysis (SCA) is a relatively new and striving area of security research. Over the last years, many countermeasures and attacks have been proposed. A majority of these countermeasures is algorithm- and platform-specific. Given that some countermeasures result in non-negligible resource overheads, designers are reluctant to include these countermeasures in commercial products. Therefore, there is still need for further research in this area to improve the efficiency and security level of side-channel countermeasures.

So far, I together with my colleagues developed a novel approach to realize masked addition in hardware. Our idea can be used to design side-channel resilient circuits of ciphers that rely on addition, e.g., Addition-Rotation-Xor (ARX) constructions. Furthermore, we have been working on an efficient combined countermeasure against side-channel analysis and fault injection attacks. This countermeasure mixes the common threshold implementation approach with error detecting codes. Currently, we have developed a first working prototype. Regarding evaluation techniques, we have mostly focused on applying incremental computation methods to common side-channel evaluation schemes and attacks. This particular way of computation enables the fast and accurate calculation of results while only loading each measurement once. Therefore, it can be easily run in parallel to the measurement setup which provides another significant performance improvement. So far, we have applied these methods on Welch's t-test[1] and correlation-based attacks and security assessment techniques[2]. Besides improving the performance of existing techniques, we also worked on extending the popular information-theoretic security evaluation method. To this end, we proposed to use advanced density estimation techniques which enable a per moment evaluation of masked implementations.

[1] T. Schneider and A. Moradi, "Leakage Assessment Methodology - A Clear Roadmap for Side-Channel Evaluations," in *CHES*, 2015, vol. 9293, pp. 495–513.

[2] T. Schneider, A. Moradi, and T. Güneysu, "Robust and One-Pass Parallel Computation of Correlation-Based Attacks at Arbitrary Order." Cryptology ePrint Archive, Report 2015/571, 2015.

8.14 Multimodal Speaker Identification and Verification

Lea Schönherr (lea.schoenherr@rub.de)
Supervisor/s: Prof. Dr.-Ing. Dorothea Kolossa

Speaker recognition can be used to identify and verify an individual biometrically. For this purpose, the physical characteristics of speech are considered, which differ for every person. However, using only a single biometric feature has already been shown to be vulnerable to spoofing attacks that imitate the victim's biometrics[1]. On the other hand, the false rejection rate (rejecting a legitimate user) should be small as well. Furthermore, a biometric system must be robust enough for everyday life.

A solution to accomplish those requirements is to combine various biometric features and thus achieve greater robustness. In case of speaker recognition, an obvious combination is with face recognition. The advantages of audiovisual speaker recognition include the difficulty for an attacker to obtain the audio as well as the visual information of a speaker at the same time. Additionally, a multimodal biometric system can operate under various conditions, since the results of both components can be weighted adaptively.

For speaker recognition the i-vector method is state of the art, which recognizes a person by extracting the speaker-dependent part of an utterance (characteristics of a person's speech) and comparing it with a stored model of all enrolled speakers in a system[2]. Since only the speaker-dependent part is used, the i-vector method is text-independent. For face recognition, the eigenface method is used, which shows great robustness under different lighting conditions and poses of the head[3].

To take advantage of the text-independence property, the text for the verification can change for each identification process. This makes it harder for an attacker to imitate the necessary utterance. Additionally, audiovisual speech recognition can be used to verify the spoken text and to match the movements of the lips with the audio channel.

The intention of our work is to merge speech recognition with face recognition as described above. For this, the weighting of both components needs to be adaptive, depending on the environmental conditions. Furthermore, spoofing attacks against such a multimodal system should be prevented. This can be accomplished by combining the audio and the visual identification with audiovisual speech recognition to verify that an autogenerated, dynamic passphrase is uttered correctly.

[1] S. M. A. Hadid N. Evans, "Biometrics systems under spoofing attacks: An evaluation methodology and lessons learned," *IEEE Signal Processing Magazine*, vol. 32, pp. 20–30, 2015.
[2] H. Beig, *Fundamentals of speaker recognition*. Springer Science+Business Media, 2011.
[3] S. Z. L. A. K. Jain, *Handbook of face recognition*. New York: Springer, 2005.

8.15 Security Aspects of FPGA-Designs and Embedded Software

Pawel Swierczynski (pawel.swierczynski@rub.de)
Supervisor/s: Prof. Dr. Christof Paar

Our previous works have shown that the bitstream encryption scheme of Xilinx and Altera FPGAs can be broken by means of side-channel attacks making the straightforward cloning of an FPGA design possible. In addition to that, the integrity of the seemingly protected bitstream (containing a description of the hardware configuration) is lost. Since the hardware configuration can be changed by modifying a (revealed) bitstream, in theory, an attacker is able to alter the complete circuitry, e.g., to implant a malicious functionality in an AES core. Therefore, an unprotected bitstream can lead to the insertion of potential cryptographic Trojans and hence to the loss of confidentiality and privacy.

Since the bitstream file format is proprietary, which describes the configuration of a (complex) hardware circuitry, an attacker has to overcome two main hurdles for conducting a meaningful change of the internal hardware setup: first, the bitstream file format needs to be reverse-engineered. Second, the relevant primitives need to be identified, located, and replaced. Recent works, e.g. the one of[1] have shown that the bitstream file format can be reverse-engineered to a certain extent, but the attacker's real-world capabilities of manipulating unknown cryptographic 3rd-party FPGA designs are less explored and unclear.

In this work we evaluate how to detect the crucial components of cryptographic FPGA designs and demonstrate that the FPGA's system security using symmetric cryptography can be undermined by an attacker who has to perform changes at a very low level, cf..[2] As a proof-of-concept, we have demonstrated[3] that this kind of attack can be conducted on a publicly available high-security USB flash drive that is supposed to securely encrypt user data.

[1] Z. Ding, Q. Wu, Y. Zhang, and L. Zhu, "Deriving an NCD file from an FPGA bitstream: Methodology, architecture and evaluation," *Microprocessors and Microsystems - Embedded Hardware Design*, vol. 37, no. 3, pp. 299–312, 2013.

[2] P. Swierczynski, M. Fyrbiak, P. Koppe, and C. Paar, "FPGA Trojans through Detecting and Weakening of Cryptographic Primitives," *IEEE Transactions on CAD*, 2015.

[3] P. Swierczynski, M. Fyrbiak, P. Koppe, A. Moradi, and C. Paar, "Interdiction in practice – hardware trojan against a high-security USB flash drive." Cryptology ePrint Archive, Report 2015/768, 2015.

8.16 Differential Privacy and Cryptography

Filipp Valovich (filipp.valovich@rub.de)
Supervisor/s: Prof. Dr. Hans Ulrich Simon

In recent years, the notion of *differential privacy* (DP) has become an important field of research. In this framework we consider individual users storing sensitive data in statistical databases. Our concern is to find techniques protecting the privacy of these users against untrusted data analysts. Simultaneously, the data analyst should be able to perform accurate analyses over the database.

Our research aims at showing how cryptographic methods can provide positive impact to DP. Concretely, we investigate solutions for the so-called *distributed setting*, where we do not want to rely on a *trusted curator*, as in the *centralised setting*. This complicates the goal of achieving DP and accuracy at the same time, since the users independently have to make their own data private but to a certain extent available without the help of a second trusted party.

Therefore we study how a proper *differentially private perturbation process* can be performed by the users on their own. In order to achieve the same accuracy as provided by well-known techniques in the centralised setting, Shi et al.[1] introduce the *Private Stream Aggregation* (PSA) scheme, a cryptographic protocol which enables each user to securely send encrypted time-series data to a data analyst. The analyst then decrypts the aggregate of all data in each time step, but cannot retrieve any further information about the individual data. Using such a protocol, the perturbation task is split among the users, such that DP is preserved and high accuracy is guaranteed.

In[2], a PSA scheme for sum queries is provided and some security guarantees under the DDH assumption are shown. However, this instantiation has some limitations. First, the security only holds in the *random oracle model*; second, its decryption algorithm is not efficient in general; third, since a PSA scheme provides *computational security*, the perturbation mechanism in use can only provide *computational DP*. However, no connection between the security of a PSA scheme and DP is explicitly shown. In[3], we eliminate all three drawbacks by giving a general framework for constructing a secure PSA scheme in the *standard model*, providing a DDH-based example with efficient decryption and showing the missing reduction. In an upcoming work we provide furthermore a LWE-based PSA scheme with prospective security against quantum computers.

[1] E. Shi, T. H. Chan, E. G. Rieffel, R. Chow, and D. Song, "Privacy-preserving aggregation of time-series data," in *Proc. of NDSS '11*, 2011.
[2] E. Shi, T. H. Chan, E. G. Rieffel, R. Chow, and D. Song, "Privacy-preserving aggregation of time-series data," in *Proc. of NDSS '11*, 2011.
[3] F. Valovich and F. Aldà, "Private stream aggregation revisited," *CoRR*, 2015.

8.17 On the practical hardness of the LWE problem

Friedrich Wiemer (friedrich.wiemer@rub.de)
Supervisor/s: Prof. Dr. Alexander May

In our today's digital world cryptography is in wide-spread use to secure our daily actions. Asymmetric cryptography is needed for secure communications, e.g., when doing bank transactions or shopping on websites. Latest progress in quantum computer research and the advent of such computers in the not so distant future poses a major threat to some important (asymmetric) cryptographic primitives. To replace these primitives with so called post-quantum cryptographic (PQC) ones, these new primitives need to undergo close scrutiny.

One of the three major candidates for PQC are lattice based schemes, which can be based on the theoretical hardness of the Learning With Error (LWE) problem. Regev introduced the LWE problem as a variant of the Bounded-distance decoding (BDD) problem in 2005. It is a variant of the Closest Vector Problem in lattices, which is known to be NP-hard. Several algorithms are known to solve LWE, in practice BDD enumeration algorithms seem to result in the best running times for solving LWE. But a gap between practical and theoretical runtime remains. Thus it is important to implement these algorithms and evaluate them practically.

We have implemented several variants of BDD enumerations in both, single- and multi-threaded versions, the code is online available[1]. With these implementations the running time of a practical attack on various proposed parameter sets for LWE based cryptosystems were checked. For benchmarking, we used a computer cluster, thus one attack instance could use up to 64 cores for computations.

The eventual aim is, to report our findings and publish the results on the practical evaluation[2].

[1] E. Kirshanova and F. Wiemer, "Github Project: Parallel Implementation of BDD enumeration for LWE," Feb-2016. [Online]. Available: https://github.com/pfasante/cvp-enum.
[2] E. Kirshanova and F. Wiemer, "Parallel Implementation of BDD enumeration for LWE," 2016.

8.18 FPGA Security

Alexander Wild (alexander.wild@rub.de)
Supervisor/s: Prof. Dr. Christof Paar

A Field Programmable Gate Array (FPGA) is basically a programmable hardware device which is employed in a wide range of commercial products, e.g. satellite receivers or secured USB sticks but also infrastructures such as network backbones. The popularity of this device family bases on its flexibility and programmability combined with the advantages of hardware (w.r.t. high performance, low energy consumption, and security through integration). Hence, the hardware structure of FPGAs provides a quite reasonable plattform for fast and efficient applications with minimal development cost. Nonetheless, FPGA manufacturer provide only minimal support to secure the device against various attack scenarios.

My research focuses on FPGA devices and combines it with the extensive definition of security aspects. This includes, on the one hand, the security of the FPGA itself (i.e., configurations, trust zones, key management, design tools) for which only minimal support by FPGA manufacturers is available. Especially a secure key management is hard to achieve on recent SRAM based FPGA devices, which lose their configuration and content after power-down. Therefore, cryptographic secret keys must either be securely stored and reloaded from external sources or can be created device internal. The latter uses device specific properties that are inherently available due to manufacturing differences. Hardware circuits extracting such device specific characteristics are called Physical Unclonable Functions (PUF) and are a big research topic in the hardware security area[1,2,3].

Furthermore, FPGAs are often used for security applications and thus might be subject of a wide range of physical and logical attacks. One major physical threat are the so-called side-channel attacks, that extract secret information from a cryptographic device by exploiting information leaked over a side-channel like; processing time, power consumption or electromagnetic emission. My PhD thesis also aims to provide a solution to harden cryptographic applications against those attack vectors[4,5,6].

[1] A. Wild and T. Güneysu, "Enabling SRAM-PUFs on Xilinx FPGAs," in *FPL 2014*, 2014, pp. 1–4.
[2] G. T. Becker, A. Wild, and T. Güneysu, "Security Snalysis of Index-Based Syndrome Coding for PUF-Based Key Generation," in *HOST 2015*, 2015, pp. 20–25.
[3] A. Wild, G. T. Becker, and T. Güneysu, "On the Problems of Realizing Reliable and Efficient Ring Oscillator PUFs on FPGAs," in *HOST 2016*, 2016.
[4] A. Wild, A. Moradi, and T. Güneysu, "Evaluating the Duplication of Dual-Rail Precharge Logics on FPGAs," in *COSADE 2015*, 2015, vol. 9064, pp. 81–94.
[5] A. Wild, A. Moradi, and T. Güneysu, "GliFreD: Glitch-Free Duplication - Towards Power-Equalized Circuits on FPGAs," *IACR Cryptology ePrint Archive*, vol. 2015, p. 124, Preprint, 2015.
[6] A. Moradi and A. Wild, "Assessment of Hiding the Higher-Order Leakages in Hardware - What Are the Achievements Versus Overheads?" in *CHES 2015*, 2015, pp. 453–474.

9 RTG 1855: Discrete Optimization of Technical Systems under Uncertainty

Prof. Dr. Peter Buchholz (peter.buchholz@cs.tu-dortmund.de)
University of Dortmund
http://grk1855.tu-dortmund.de

The development and operation of technical systems like production systems, logistics networks or large IT systems has to be based on a large number of design and configuration decisions to meet the performance requirements with a limited amount of resources and costs. Necessary decisions are often based on the solution of optimization problems with discrete or mixed discrete-continuous parameters describing the available alternatives.

Optimization problems of this kind are hard to solve as the number of available solutions exponentially increases with the number of decisions between discrete alternatives due to the "combinatorial explosion". Most practical problems are simplified significantly to allow an algorithmic solution. Furthermore, in practice, decisions often have to be made with incomplete knowledge. The resulting uncertainty is usually not considered in existing optimization approaches even if this may result in considerable differences between the computed and real solution of the optimization problem. In some cases computed solutions may not even be feasible in practice.

Another yet not deeply considered aspect of the optimization of technical systems is the role of people in the decision process. Mathematical methods and algorithms may compute optimal parameter values but the final solution must be accepted by a person and must be translated into concrete plans and instructions. To increase the applicability of optimization methods in practice, people must be regarded as part of the decision process. This implies that the process of optimization and result representation must take into account the requirements of users.

The topic of the graduate school is optimization under uncertainty with the incorporation of people in the optimization process. Application scenarios that will be considered occur the areas of logistics, chemical production systems and IT systems. Topics of the graduate school are interdisciplinary since the school combines research on methods from optimization, algorithms, statistics, applications and psychology.

9.1 Robust Perfect Matchings

Viktor Bindewald (viktor.bindewald@math.tu-dortmund.de)
Supervisor/s: Jun.-Prof. Dr. Dennis Michaels

We consider a robustness concept that models structural uncertainty in combinatorial optimization problems. Concretely, in the considered model, the set of feasible solutions itself can change depending on the emerged scenario, while the cost structure of resources is not subject to uncertainty. The uncertainty in the feasible set is modelled via the failure of certain subsets of resources (edges or nodes in a graph) that are specified in the input. Each set of vulnerable resources defines a scenario of our robust optimization problem. The goal is to find a set of resources (e.g., edges or nodes) containing a solution to the underlying problem (e.g., an s-t path, or a perfect matching), no matter which scenario emerges, namely no matter what specified set of resources comprising a single scenario is removed from the solution. The goal is to find a robust solution of the latter type with minimum cost. For details on this model we refer to[1]. We consider the described approach with the Perfect Matching Problem as the underlying combinatorial optimization problem. This question can be then formulated as follows. Consider a graph $G = (V, E)$. The set of resources R can be either the node set V or the edge set E. The vulnerable resources are given by the scenario set $\Omega \subseteq 2^R$. The costs are represented by a function $c : 2^R \to \mathbb{R}$. Our robust optimization problem can be then stated as follows:

$$\begin{array}{ll} \min & c(Y) \\ \text{s.t.} & \forall F \in \Omega \text{ the induced graph } G[Y \setminus F] \text{ admits a perf. matching of } G \\ & Y \subseteq R \end{array} \qquad (\mathcal{RPM})$$

In a joint work with Dr. Adjiashvili we focus on the (RPM)-variant with the edge set as the possibly vulnerable resources.

Even under additional assumptions we were able to prove that our problem is NP-hard for the simplest cases of the uncertainty set. Moreover we obtained, under mild assumptions, results on hardness of approximation for the general and some restricted cases. The algorithms we developed are asymptotically tight.

[1] D. Adjiashvili, S. Stiller, and R. Zenklusen, "Bulk-robust combinatorial optimization," *Mathematical Programming*, vol. 149, no. 1, pp. 361–390, 2014.

9.2 Stochastic Bilevel Programming

Matthias Claus (matthias.claus@uni-due.de)
Supervisor/s: Prof. Dr. R. Schultz

Bilevel programming problems form a special class of hierarchical optimization problems where the set of decision variables is partitioned into upper and lower level variables. The lower level variables are to be chosen as an optimal solution of an optimization problem which is parametrized in the upper level variables and referred to as the lower level problem. Among many others, applications of such models include problems in the domain of economics (e.g. Stackelberg games), transportation (e.g. toll setting problems) and energy (e.g. the modeling of day-ahead electricity markets).

Real-world applications usually have to deal with uncertain data. Stochastic and purely exogenous uncertainty and an interplay between decision and observation where the upper level variables have to be decided without knowledge of the realization of the randomness while the lower level problem is solved under complete information is assumed. In this setting, each decision of the upper level variables results in a random variable describing the possible outcomes for the objective function. Applying a weighted sum of the expectation and some quantification of risk imposes a preorder on this family of random variables that allows for optimization. This gives rise to a class of problems that includes 2-stage mean risk models as a special case where upper and lower level have a common objective function allowing to take only the optimal value of the lower level problem into account. In general, the objective functions do not coincide and the lower level problem has no unique solution which results in weaker structural properties and motivates an investigation of the stability of the models. Such considerations are indispensable preliminary work for the analysis of the behavior of solution algorithms under perturbations of the underlying probability measure motivated by the fact even the distribution of the randomness itself might originate from an approximation in real-world problems. In addition, the choice of the quantification of risk allows for considering various notions of risk aversion and the question of which risk measure lead to stable and traceable models arises naturally.

In 2-stage mean risk models, assuming the uncertainty to be given by a random vector with finitely many realizations often results in a large-scale MILP that can be tackled using algorithms based on scenario decomposition. It seems promising to analyze to what extend such methods can be applied for stochastic bilevel problems as well.

9.3 Dynamic management of logistic facilities under uncertainty

Lars Eufinger (eufinger@itl.tu-dortmund.de)
Supervisor/s: Prof. Dr.-Ing. Uwe Clausen

Freight forwarding companies in the less-than-truckload (LTL) industry are under strong competitive pressure. Due to this pressure companies are trying to gain a competitive advantage by systematically optimizing the processes and the implementation of logistics innovations. We want to investigate LTL terminals, which are the hubs of the LTL transportation networks and operate as distribution centers with collection and distribution function of goods, e.g. cross docking. The task of a LTL terminal is the accurate and in time handling of shipments between vehicles on short-distance traffic and transport vehicles on long-distance traffic. The performance of a LTL terminal is largely determined by the proper use of the gates. A gate assignment plan should minimize the waiting times of the trucks while having short transportation distances for the goods inside the terminal. However, many uncertain factors influence the planning. Especially fluctuations in the arrival times of vehicles have great impact on the planning process. Thus it is reasonable to use stochastic optimization to create a gate assignment plan which can handle the occurring uncertainties.

The developed MILP optimization model is based on two-stage stochastic optimization using scenario decomposition. The basic idea of the two stage process is the following. At the first stage, before a realization of the corresponding variables becomes known, one chooses the first-stage decision variables to optimize the expected value of an objective function which in turn is the optimal value of the second-stage optimization problem. A finite number of realizations of the random data, called scenarios, are considered to model the uncertainties.

In the two-stage model for the gate assignment problem, the assignments of the trucks to the gates are used as the first-stage decision variables. All remaining variables, e.g. the assignment times of the trucks, are the second-stage decision variables. Which means, in the first stage, a gate assignment is determined. The quality of the assignment is evaluated in the second stage, where the assignment times and the transports of the goods inside the facility are determined for the given scenarios.

To handle the problem in practice a matheuristic is developed. In the first stage gate assignments are determined using a metaheuristic, e.g. local search or evolutionary algorithms. For each assignment the second stage is solved via CPLEX for each scenario. By this the objective value of a given gate assignment can be derived. The information of the second stage can now be used to find better assignments in the first stage. This way, one gets an iterative procedure to determine good gate assignments, which takes the occurring uncertainties into account.

9.4 Stochastic Graph Models with Phase Type Distributed Edge Weights

Iryna Felko (iryna.felko@cs.tu-dortmund.de)
Supervisor/s: Prof. Dr. Peter Buchholz

Most stochastic shortest path problems include an assumption of independent weights at edges. For many practical problems, however, this assumption is often violated indicating an increased number of applications with stochastic graphs where edge weights follow a distribution that has possible correlation with weights at adjacent edges. Particularly, real-world information in conjunction with stochastic dependencies in networks can significantly contribute for computation of the optimal shortest path. E.g., the knowledge of a congestion arising on the current road result in a better traveler's choice of an alternative route. In this thesis, an innovative model class for stochastic graphs with correlated weights at the edges is introduced. In the developed PH-Graph model edge weights are modeled by PH distributions and correlations between them can be encoded using transfer matrices for PH distributions of adjacent edge weights. Stochastic graph models including correlations are important to describe many practical situations where the knowledge about system parameters like travelling times and costs is incomplete or changes over time. Based on PH-Graphs efficient solution methods for Stochastic Shortest Path Problems with correlations can be developed. Competing paths from origin to destination in a PH-Graph can be interpreted as CTMDP. Optimal solutions to many realistic shortest path problems can be obtained from finding an optimal policy in a CTMDP. E.g., the problem of finding reliable shortest path to maximize the probability of arriving on time under realistic assumptions can be efficiently treated. Formulations of different shortest path problems with correlations as well as solution methods from the CTMDP field are presented. We adress the parameterization of PH-Graphs based on measured data from some real-world and simulated systems. Fitting methods for parameterization of transfer matrices are adopted from MAP fitting approaches. Furthermore, we consider similarity transformations of PHDs when modeling correlation between two PHDs. For order 2 acyclic PHDs, optimal representations maximizing the first joint moment that can be reached when two PHDs are combined in composition are investigated. We derived transformation methods to increase the range of correlation that can be modeled by the novel PH-Graph model. By means of a real-world example using a vehicle mobility trace based on 24-hour car traffic simulation data of the city of Cologne it is shown that the new PH-Graph model is able to capture existing correlations. Based on realistic representation of traveling time durations car traffic on road networks with congestion effects can be represented. Our experiments and examples show that correlation has a significant impact on shortest paths in stochastic weighted networks and that our solution methods are effective and usable when, e.g., optimal traveler route choice decision should be determined.

9.5 Black-box optimization of mixed discrete-continuous optimization problems

Momchil Halstrup (halstrup@statistik.tu-dortmund.de)
Supervisor/s: Prof. Dr. Sonja Kuhnt

In many industrial applications it is becoming standard practice to study complex processes with the help of computer experiments. The increasing computing capabilities have made it possible to perform cheap simulation studies beforehand, where the desired process characteristics can be optimized. Computer simulations may have only continuous inputs, or also mixed discrete-continuous input variabless. Simulations take a very long time to run, making it impossible to perform direct optimization on the computer code. Instead, the simulator can be considered as a black-box function and an analytical model, much cheaper to evaluate, is used to interpolate the simulation.

Model-based optimization of black-box functions has a long history and has become a classical tool in the analysis of computer experiments. This work explores the capabilities of current black-box optimization procedures, many of which are based on a well known metamodel - the Kriging model, and also proposes some new methods which improve the existing theory. This thesis considers two separate classes of black-box experiments - simulations with continuous inputs and mixed-input simulations.

For experiments with only continuous inputs, this work proposes a robust version of the Kriging-based efficient global optimization (EGO) algorithm. The novel method, called KeiEGO is able to correct some of the flaws of EGO, stemming from the restrictive assumptions which EGO and the Kriging model make. First of all, an alternative metamodel - the kernel interpolation (KI) is used instead of Kriging and a robust search criterion is implemented. It is shown that KeiEGO works better than EGO in some situations, including a simulation study. Furthermore in this work a parallelization procedure is proposed - the ParOF (parallel optimization based on FANOVA) algorithm. The ParOF method gathers information about the structure of the black-box function and uses that information for parallel computations and dimensionality reduction. It is shown that this procedure works well on a simulation example.

Although the mixed case is of interest for various applications, only a handful of model-based optimization procedures exist, able to produce solutions for mixed-input experiments. The biggest problem for model-based optimization is being able to define a model for mixed-inputs. For example, the Kriging method is based on distance calculations and this proves to be problematic in the mixed case. In this thesis a special class of kernels for Kriging are introduced, based on the Gower distance for mixed inputs. With the help of this Kriging modification, the EGO procedure is transformed to work for mixed inputs. This new method scales excellently in comparison to existing methods and it is shown, that the procedure is able to tackle mixed problems very well.

9.6 Min-max-min Robust Combinatorial Optimization

Jannis Kurtz (jannis.kurtz@math.tu-dortmund.de)
Supervisor/s: Prof. Dr. Christoph Buchheim

The robust optimization approach, designed for tackling the uncertainty that is present in the parameters of many optimization problems has a variety of practical applications in industry, finance or even medicine. The original idea of the robust optimization approach is to ask for a worst-case optimal solution and can be modeled by a min-max problem. Since this solution can be very conservative and hence far from optimal in the actual scenario, in the last decades the focus of research has moved to the development of new approaches that try to avoid, or at least reduce, the so-called *price of robustness*.

One of these approaches is the idea of k-adaptability in two-stage robust optimization. Here the aim is to calculate a fixed number k of second-stage policies here-and-now. After the actual scenario is revealed, the best of these policies is selected. This idea leads to a min-max-min problem. In my thesis, we consider the case where no first stage variables exist and propose to use this approach to solve combinatorial optimization problems with uncertainty in the objective function. More precisely we study the problem

$$\min_{x^{(1)},\dots,x^{(k)}\in X} \max_{(c,c_0)\in U} \min_{i=1,\dots,k} c^\top x^{(i)} + c_0 \ . \tag{M^3}$$

where $X \subseteq \{0,1\}^n$ contains the incidence vectors of all feasible solutions of the given combinatorial problem and U is the so called *uncertainty set* which contains all possible cost functions.

The main objective of my thesis is to determine the computational complexity of Problem (M^3). The complexity of course depends on the underlying set X and on the uncertainty set U.

We first show that for convex uncertainty sets U the min-max-min problem is as easy as the underlying certain problem if k is greater than the number of variables and if we can optimize a linear function over the uncertainty set in polynomial time. We also provide an exact and practical oracle-based algorithm to solve the latter problem for any underlying combinatorial problem. On the other hand, we prove that the min-max-min problem is NP-hard for every fixed number k, even when the uncertainty set is a polyhedron, given by an inner description. For the case that k is smaller or equal to the number of variables, we finally propose a fast heuristic algorithm and evaluate its performance.

For the case of discrete uncertainty sets U, i.e. U is a finite set, we prove that for several classical combinatorial optimization problems the min-max-min problem (M^3) is NP-hard for a fixed number of scenarios and strongly NP-hard otherwise for any fixed k. Additionally we propose a pseudopolynomial algorithm for the case of a fixed number of scenarios which reduces (M^3) to the well known min-max problem. Finally, we consider approximation schemes for (M^3).

9.7 Linear Programming Formulations for Stochastic Routing Problems

Denis Kurz (denis.kurz@tu-dortmund.de)
Supervisor/s: Prof. Dr. Petra Mutzel

In a first phase, we consider stochastic shortest path problems. We discovered a close connection to the Constrained Shortest Path problem (CSP), and studied algorithms for CSP extensively. We found that the best and most widely used way to tackle this problem is a two-stage approach. First, the problem size is reduced massively. A method called Aggressive Edge Elimination (AEE) by Muhandiramge and Boland achieves the best reduction results, and uses Lagrange relaxation tools repeatedly. We found that, although AEE results in very small graphs, it is very slow and can be accelerated considerably when applying certain other reduction tests prior to AEE.

As a side product, every known reduction technique gives both an upper and a lower bound for the length of a shortest constrained path. Another algorithm is then used to close the gap between the upper and lower bound. Common gap-closing approaches are k-best enumeration, label setting, and label correcting algorithms. In this context, we developed a new algorithm for the k Shortest Simple Path problem (kSSP) that is based on an optimal algorithm for the k Shortest Path problem due to David Eppstein. In contrast to existing kSSP algorithms, our algorithm is not based on the Replacement Path problem and may find multiple relevant solutions during a single shortest path tree computation.

In a second phase, we consider variants of the Stochastic Vehicle Routing problem (SVRP). Specifically, we want to explore possible ways to solve SVRPs by common means of Linear Programming like Branch and Price. We expect to benefit heavily from our experience with CSP because of existing column generating approaches for SVRP where the pricing step is equivalant to solving CSP instances.

9.8 The effect of mental representations on visual search behavior under uncertainty

Johanna Renker (renker@ifado.de)
Supervisor/s: PD Dr. phil. Gerhard Rinkenauer

Users develop mental representations during the interaction with technical systems. These representations are also called mental models and can be defined as long-term knowledge structures, which represents a users understanding of situation-specific system functioning. In order to investigate the development of mental models and to find indicators for uncertainty we recorded eye movements while participants performed the occluded visual spatial search task. Within this task different stimuli appeared with a certain probability at defined locations in the display and participants had to predict these locations as accurately as possible. For this paradigm we distinguish between exogenous (task) uncertainty and endogenous (subjective) uncertainty. Results of the experiment showed that eye movement patterns change over time with increasing expertise and thus decreasing endogenous uncertainty: fixation durations, fixation frequency as well as the number of gaze shifts decreased. At the beginning of the experiment, endogenous uncertainty was high and participants showed extensive visual search behavior, which became more focussed with decreasing endogenous uncertainty[1]. In a further study we assessed eye movement patterns during relearning uncertain task concepts. Former results could be replicated and extended: during relearning eye movement patterns possessed specific distinctiveness and provided different information about the stage of learning. Fixation frequency signalized the beginning of the relearning phase whereas fixation duration responded to this phase with a time delay[2]. In addition, our findings indicated that the efficiency in developing mental representations also depended on the characteristics of the user interface. In future studies, we are going to investigate the way eye movement patterns change with different task probabilities. Finally, theoretical and applied research are combined in a cooperation project with the Robotics Research Institute. We developed a new questionnaire QUHCC to investigate user behavior and satisfaction in High Performance Computing[3]. Collected data from the QUHCC are used to model users and to run scheduler simulations.

[1] J. Renker and G. Rinkenauer, "The acquisition of mental representation under uncertainty: An eye movement study." in *5. Interdisziplinärer Workshop Kognitive Systeme - Mensch, Teams und Automaten, 14th - 16th March 2016, Bochum, Germany*, submitted.

[2] J. Renker and G. Rinkenauer, "Umlernen von unsicheren Konzepten - Wie verändern sich Augenbewegungsmuster parallel zum Lernprozess?" in *Arbeit in komplexen Systemen. Digital, vernetzt, human?! - 62. Kongress der Gesellschaft für Arbeitswissenschaft, 2nd - 4th February 2016, Aachen, Germany*, 2016.

[3] J. Renker, S. Schlagkamp, and G. Rinkenauer, "HCI international 2015 - posters' extended abstracts: International conference, HCI international 2015, Los Angeles, CA, USA, August 2-7, 2015. proceedings, part II," Springer International Publishing, 2015, pp. 697–702.

9.9 Markov decision processes with uncertain parameters

Dimitri Scheftelowitsch (dimitri.scheftelowitsch@tu-dortmund.de)
Supervisor/s: Prof. Dr. Peter Buchholz

This PhD project deals with uncertainty in Markov decision processes. Its main motivation lies in the constraints of the Markov modeling paradigm and real-world systems that cannot be captured by it.

One major topic in this project concerns with introducing a set of possible Markov decision processes, given by sets of transition probabilities, and considering perspectives of robust optimization in this and related scenarios. It has been possible to show limits w.r.t. computational lower bounds for this model as well as some related formalisms. Furthermore, multi-objective approaches to parameter uncertainty have been explored, and it was possible to create algorithms for the arising problems such as the Pareto front enumeration problem.

Another topic of this work is the consideration of transition time uncertainty, i.e., incorporating semi-Markov processes into the MDP model. In particular, the concept of hidden clocks that govern transition times has been explored. While it is possible to view this problem as a partially observable Markov decision process, the known lower bounds for solving POMDPs are large; thus, it seems intuitive to consider a special case in the hope to apply problem-specific techniques. We have developed a framework that captures transition time uncertainty in Markov decision processes and have solved several problems within this framework with methods from stochastic game theory.

9.10 User Modeling in High Performance Computing

Stephan Schlagkamp (stephan.schlagkamp@udo.edu)
Supervisor/s: Prof. Dr. Schwiegelsohn

The performance of parallel computer systems can be evaluated with representative workloads. These workloads can derive from workload traces (logs of actual computing systems) or statistical models generating workloads with certain aspects (e.g., distribution of the number of submitted jobs per time interval, etc.). This may not suffice due to feedback effects in the interaction of users and computer systems. Users might change their behavior when facing slow or limited resources. By means of this interpretation, a workload trace represents only one instantiation of an interaction process of users and a computing system. Therefore, we aim to model user behavior more generally to provide better insights to rate and improve system performances. We want to focus on aspects such as working habits or patterns, the influence of waiting and response times (the time a system needs until a job is started or until a job is completed, respectively), etc., instead of learning user models from actual workload traces. Additionally, this modeling can help to obtain further insights to different criteria of evaluation. Quantifiable aspects like system utilization, power consumption, or heat management can be considered. All aspects can be analyzed better if a system can be simulated under realistic conditions. Another important aspect is user satisfaction. We aim to find measures optimizing parallel computing systems towards user satisfaction to give them a supportive character. Further aspects of user-system interaction might be found in cloud computing scenarios where service level agreements (SLA) have to be met (e.g., Amazon EC2, Google Cloud, etc.). A provider of computing instances guarantees for availability and response times of a system. The user pays a certain fee to use the resources under the negotiated SLA. Providers face uncertain and volatile requests. For instance, they have different approaches to deal with situations of low resource demands. While Google can run background jobs of its own interest (e.g., indexing of large data sets), Amazon established a spot market. Within this spot market, spare resources are offered in an auction-based way. In how far these cloud computing scenarios are influenced by user behavior is of great interest. It might be possible to exploit results on such behavior to design and implement better algorithms to deal with the sketched problems.

9.11 Heuristic methods for solving two-stage stochastic chemical batch scheduling problems

Thomas Siwczyk (thomas.siwczyk@bci.tu-dortmund.de)
Supervisor/s: Prof. Dr.-Ing. Sebastian Engell

Chemical batch scheduling problems in the literature in most cases are solved for nominal problems where the equipment, recipes and production orders are given and fixed. In reality, however, scheduling has to be done under significant uncertainty about yields, availability of equipment and personnel, and especially varying demands, rush orders, cancellations etc. Scheduling problems can be modeled by two-stage stochastic mixed-integer linear programs (2SSP), where the uncertainty is modeled by a discrete set of scenarios and the option of recourse decisions that react to the actual evolution is represented. If several uncertainties are included, the number of scenarios grows rapidly. With an increasing number of scenarios the resulting MILP problems become computationally very hard to solve in a monolithic fashion, making it impossible to apply this approach to realistic problem sizes. Decomposition techniques and/or (semi)heuristic approaches can then be used to find good solutions in reasonable computation times.

In a previous approach stage decomposition was successfully applied to solve 2SSP scheduling problems, where the first stage problem is solved by an evolutionary algorithm, while the second stage subproblems are solved exactly by a solver for MILPs. This implies that for each tested solution for the first-stage variables, all scenario subproblems are solved to optimality, so the computation time increases at least proportional to a multiple of the number of scenarios.

In this project, a new idea for solving large-scale 2SSP that arise from chemical batch scheduling under uncertainty is being researched based on stage decomposition and the principles of Ordinal Optimization (OO): 'Order is easier than Value' and 'Nothing but the best is very costly'. According to OO it is easier to create a ranking of multiple solutions than evaluating their exact values. Hence a heuristic evaluation might be used to find a correct ranking of solutions (with a small error). Applying this idea to two-stage stochastic programming solved by stage decomposition, the time consuming calculation of exact solutions for all scenario-related subproblems, which were used before to rank different first-stage solutions, is replaced by a non-exact evaluation, which allows finding good solutions for very large problems with a large amount of scenarios in relatively short computation times. This approach is evaluated by a case study of a chemical batch plant for the production of expandable polystyrene. Different evaluation methods for the ranking of the solutions are being considered in order to find a method that provides a ranking that is comparable to the true ranking achieved by an exact evaluation method.

10 RTG 1906: Computational Methods for the Analysis of the Diversity and Dynamics of Genomes

Jens Stoye (jens.stoye@uni-bielefeld.de)
Bielefeld University and Simon Fraser University, Vancouver, Canada
http://didy.uni-bielefeld.de

This International DFG Research Training Group at Bielefeld University started October 2013. It is in close cooperation with the NSERC-CREATE funded graduate program at Simon Fraser University, and further researchers at BC Cancer Agency and Vancouver Prostate Centre in Burnaby/Vancouver, Canada.

Both universities are young, research-oriented universities, among the leading institutions in their countries with respect to the development of bioinformatics algorithms and software. Still, there are a number of individual points where we have identified a clear gain by joining forces and bringing together expertise from both sides.

Our program aims at training specialists in handling big data related to genomics and molecular biology. The main focus of the international cooperation are exchange of both students and senior researchers, joint workshops and co-teaching. In particular, the program involves extensive research stays of the PhD students in Vancouver[1].

Research focuses on the development of methods of high importance for the practical comparative analysis of genomes. Since the development of genome sequencing, a high potential was seen in the benefits of a better understanding of the molecular mechanisms underlying life. Through the technological advances not only more genomic data are produced, but also new scientific questions can be addressed, regarding the relationship of individuals within larger populations. Understanding both the variation between individuals *(diversity)* and the change in populations over time *(dynamics)* are essential to fully comprehend biological systems.

Website of partner program: http://www.sfu.ca/madd-gen.html

Spokesperson of partner program: Prof. Dr. Martin Ester

[1] A. Tung, "Summer sojourns: SFU welcomes four students from Germany's Bielefeld University," *SFU News*, Sep. 2015.

10.1 Ancestral lines under selection: Linking population genetics and phylogenetics

Nicole Althermeler (altherme@cebitec.uni-bielefeld.de)
Supervisor/s: Ellen Baake

Ancestral processes are driven by biological forces such as mutation, recombination, natural selection and random transmission of genetic material. These forces are largely of random nature, thus statistical models support inferring and predicting genetic patterns created by them. A collection of statistical models is offered by coalescent theory, which describe the demographic history of species. The *n-coalescent* by Kingman (1982) marks a milestone in the field[1]. It is a tree-structure that describes the history of a sample of individuals from one species. The corresponding mathematical process describes the neutral case, in which no selection is present. A graph structure that does take selection into account is the *ancestral selection graph*[2]. Here, one individual and all its potential ancestors are described in one graph. This graph can be constructed by random poisson processes and models not only different reproduction and mutation rates, but also the effects of selection.

Several important question arise in this field of research, for instance: Given an initial frequency x of a beneficial type in a population in the distance past, what is the probability that the ancestor of today's population had the beneficial type?

It is possible to analytically derive these probabilities for simpler, restricted cases[3]. However, as studied scenarios become more complicated, analytical results become nearly impossible. Here, a solution are simulations of ancestral processes via Markov chains. These should result to close approximations of the underlying probabilities.

The project is devoted to the simulation and thorough understanding of random genealogies and ancestral lineages under various models of mutation and selection. Particular emphasis will be on the single ancestral line that leads back into the distant past and also connects with other species, thus building the bridge to phylogenetics, the evolutionary relationship of species. This may, for example, help to understand the large discrepancy between mutation rates estimated from species trees and those estimated from population samples.

[1] J. Kingman, "The coalescent," *Stochastic Processes and their Applications*, vol. 13, no. 3, pp. 235–248, 1982.

[2] C. N. S.M. Krone, "Ancestral processes with selection." *Theor. Popul. Biol.*, vol. 51, pp. 210–237, 1997.

[3] U. Lenz, S. Kluth, E. Baake, and A. Wakolbinger, "Looking down in the ancestral selection graph: A probabilistic approach to the common ancestor type distribution," *Theoretical Population Biology*, vol. 103, pp. 27–37, 2015.

10.2 Assembling the Microbial Dark Matter

Andreas Bremges (andreas@cebitec.uni-bielefeld.de)
Supervisor/s: Alex Sczyrba, Jens Stoye

The vast majority of microbial species found in nature has yet to be grown in pure culture, turning metagenomics and – more recently – single cell genomics into indispensable methods to access the genetic makeup of microbial dark matter[1,2]. We develop new tools and algorithms that naturally exploit the complementary nature of single cells and metagenomes.

Frequently, single amplified genomes (SAGs) and shotgun metagenomes are generated from the same environmental sample. Our software *MeCorS* uses sequence information derived from accompanying metagenome sequencing to accurately correct SAG sequencing reads, even from ultra-low coverage regions[3]. Pushing this concept even further, we developed *kgrep*, a fast k-mer based recruitment method to sensitively identify metagenomic "proxy" reads representing the single cell of interest, using the raw single cell sequencing reads as recruitment seeds. By assembling largely unbiased metagenomic reads (instead of SAG reads), we circumvent most challenges of single cell assembly, and can significantly improve the completeness and contiguity of single cell genome assemblies.

The increase in scientists using single cell genomics for their studies – often in conjunction with metagenomics – goes hand in hand with the broad application of *MeCorS* and *kgrep*, and their utility to improve the quality of single cell genome data.

[1] C. T. Brown and others, "Unusual biology across a group comprising more than 15% of domain Bacteria," *Nature*, 2015.
[2] C. Rinke and others, "Insights into the phylogeny and coding potential of microbial dark matter," *Nature*, 2013.
[3] A. Bremges and others, "MeCorS: Metagenome-enabled error correction of single cell sequencing reads," *Bioinformatics*, 2016.

10.3 Polyomics Visualization

Benedikt G. Brink (bbrink@cebitec.uni-bielefeld.de)
Supervisor/s: Stefan Albaum, Ryan R. Brinkman, Tim W. Nattkemper

Cells are living systems full of various functional molecules, which eventually determine the phenotype of the cells. Such molecules include mRNA transcribed from DNA, proteins translated from mRNA, and various metabolites generated by various enzymatic activities. Obviously, only analyzing the DNA sequences of genomes is not enough to obtain crucial information regarding the regulatory mechanisms involved in a cells metabolism, e.g. responses to environmental factors and other stresses or the production of metabolites. To understand the diversity and dynamics of a biological system, data from more than one *omics* approach is needed[1].

Surprisingly, to date a great deal of information regarding cellular metabolism is being acquired through application of individual omics approaches. There are powerful tools for analyzing mRNA expression profiles, visualizing interaction networks or investigating metabolic pathways. But only little effort has been made to develop tools for a comprehensive, integrative analysis of data from multiple omics-experiments[2]. A new, integrative approach to visualize these data at different levels, creating a state-of-the-art, data driven tool can potentially provide new insights into biology, or at least simplify gathering of information and analyzing data from experiments with more than one omics-approach.

To achieve all this, a new framework for polyomics data integration called Fusion is being developed. It shall become a center for all kinds of data-rich high-throughput experiments and offer convenient data management, powerful analysis tools, including established methods for analyzing and visualizing single omics data, as well as new features for an integrative analysis of data from multiple omics platforms. Fusion focuses on the three classical fields in omics: transcriptomics, proteomics and metabolomics and offers connections to other platforms like EMMA or QuPE, all developed and hosted at the Center for Biotechnology (CeBiTec) in Bielefeld. It is a web based service, completely written in Java and JavaScript using the popular D3.js library and is supposed to supersede ProMeTra[3].

[1] W. Zhang, F. Li, and L. Nie, "Integrating multiple 'omics' analysis for microbial biology: Application and methodologies," *Microbiology (Reading, England)*, vol. 156, no. Pt 2, pp. 287–301, 2010.

[2] N. Gehlenborg, S. I. O'Donoghue, N. S. Baliga, A. Goesmann, M. A. Hibbs, H. Kitano, O. Kohlbacher, H. Neuweger, R. Schneider, D. Tenenbaum, and A.-C. Gavin, "Visualization of omics data for systems biology," *Nature methods*, vol. 7, no. 3 Suppl, pp. S56–68, 2010.

[3] H. Neuweger, M. Persicke, S. P. Albaum, T. Bekel, M. Dondrup, A. T. Hüser, J. Winnebald, J. Schneider, J. Kalinowski, and A. Goesmann, "Visualizing post genomics data-sets on customized pathway maps by ProMeTra-aeration-dependent gene expression and metabolism of Corynebacterium glutamicum as an example," *BMC systems biology*, vol. 3, p. 82, 2009.

10.4 Practical evaluation of family-free common intervals methods for comparing genomes

Omar de Jesus Castillo Gutierrez (castillo@cebitec.uni-bielefeld.de)
Supervisor/s: Jens Stoye

Comparing gene order in related genomes is beneficial for the understanding of genome evolution and function. Considering the genome as a sequence of characters representing each individual gene, common character set intervals between two or more genomes constitute gene clusters as seen in the operons in prokaryotes. This approach generally requires previous gene family identification. However, there are family-free methods for identifying gene clusters[1], measure breakpoint distance and finding the median genome without precomputing gene families. In this project we evaluate the predictive capabilities of these approaches by comparing them against other approaches and testing them using different clades; for validation we use public cluster and pathway databases.

[1] D. Doerr, J. Stoye, S. Böcker, and K. Jahn, "Identifying gene clusters by discovering common intervals in indeterminate strings," *BMC genomics*, vol. 15, no. Suppl 6, p. S2, 2014.

10.5 Pan-genome Storage and Search

Holley Guillaume (gholley@cebitec.uni-bielefeld.de)
Supervisor/s: Jens Stoye, Roland Wittler, Cenk Sahinalp

The advent of High Throughput Sequencing (HTS) technologies offered to the scientific community an opportunity to fully study the dynamics and diversity of genomes by sequencing multiple strains of the same species. introducing the *pan-genome* concept. A pan-genome is composed of the *core genome* and the *dispensable genome*. The first contains all the genes shared by all the strains of the same species meanwhile the the second contains genes specific to one or mutiple strains but not part of the core genome.

In this project, we aim to provide methods and data structures enabling the storage and the indexing of pan-genomes at the DNA level. A data structure for pan-genome storage and search should provide easy and fast access to any part of it by indexing its content and taking advantage of the data redundancy for compression. It should allow the insertion of newly produced data such that its performance does not degrade with the amount of data added.

In the first and second year of this project, an alignment-free and reference-free data structure for compressing and indexing a pan-genome has been developed. A pan-genome is represented as a *colored de-Bruijn graph*[1] in which vertices represent colored k-mers, words of length k associated with the identity of the strains in which they occur. We proposed for storing and traversing such a graph the *Bloom Filter Trie* (BFT)[2], a trie that compress and index strings of fixed-length k and their colors. BFT is based on the *burst trie*[3] and includes mutiple *Bloom filters*[4] to accelerate the traversal. Experimental results prove better performance compared to another state-of-the-art data structure.

During the third year, a pan-genome sequencing reads compression algorithm based on the BFT, named BFT-Comp, was developed. Indeed, pan-genome sequencing reads are often compressed as soon as they are produced, resulting in mutiple redundant compressed archives. HTS-specific compression tools do not offer the possibility to edit these archives with newly produced data. BFT-Comp tackles the problem of pan-genome compression by encoding the sequences of a pan-genome as a guided de-Bruijn graph. Sequencing reads can be added to a BFT-Comp archive without the need to decompress it entirely.

[1] Z. Iqbal, M. Caccamo, I. Turner, P. Flicek, and G. McVean, "De novo assembly and genotyping of variants using colored de Bruijn graphs," *Nat. Gen.*, vol. 44, no. 2, pp. 226–232, 2012.

[2] G. Holley, R. Wittler, and J. Stoye, "Bloom Filter Trie–A Data Structure for Pan-Genome Storage," in *Proceedings of 15th international workshop on algorithms in bioinformatics*, 2015, vol. 9289, pp. 217–230.

[3] S. Heinz, J. Zobel, and H. E. Williams, "Burst tries: a fast, efficient data structure for string keys," *ACM Trans. Inf. Syst.*, vol. 20, no. 2, pp. 192–223, 2002.

[4] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422–426, 1970.

10.6 Interpretation and visualisation of molecular dynamics in complex bioimage data

Georges Hattab (ghattab@cebitec.uni-bielefeld.de)
Supervisor/s: Tim W. Nattkemper

With the advent of technologies that permit advancements in microscopy, either for high-resolution data acquisition or automation of processes, the volume and complexity of image data has increased to the point that it is no longer feasible to retain relevant information without the use of a computer[1]. Even though major technological improvements and breakthroughs have been made[2], the continuous acquisition and analysis of high-resolution time-lapse microscopy images remains a complex task. Yet various venues have been successful in developmental biology[3,4], in synthetic and systems biology[5]. This is due to the coupling of key advances in fluorescence light microscopy, computational image processing, data management and visualisation. This work inscribes itself in synthetic biology, with the main objective of analysing the history of a single-cell bacteria, *Sinorhizobium meliloti*, throughout its life. Its novelty relies not only on tackling image data where each pixel represents 0.06 µm but also at attempting to assess bacterial fitness using cell-lineage, where an individual bacteria at t(0) evolves into a colony. The originality of this work is that cell-lineage is tackled in an unexplored field in bioimaging, where the data at hand are both non trivial and difficult (e.g. low signal-to-noise ratio, spatial shift, etc). Achieving the design of a reliable system encompasses handling such factors. In light of this high-dimensional data, novel algorithmic and representation venues have been sought. First, a novel and adaptive algorithm was developed to correct for spatial shift. Second but not last, an enhanced 3D visualisation coupled with an automated segmentation-free pipeline enabling us to gain quick insight into the pedigree of each cell in every temporal development. The mutual dependencies of the bacteria remain to be tackled. In addressing both biological (e.g. targeted gene expression) and informatics questions (feature detection, single-cell tracking, birth/deaths events, etc), this permits a quantitative and qualitative investigation of the data, which could in turn be subject to a posterior statistical analysis.

[1] H. Peng, A. Bateman, A. Valencia, and J. Wren, "Bioimage informatics: A new category in *bioinformatics*," *Bioinformatics*, vol. 28, p. 1057, Mar 2012.
[2] F. Amat and J. Keller, "Towards comprehensive cell lineage reconstructions in complex organisms using light-sheet microscopy," *Develop. Growth Differ.*, March 2013.
[3] A. McMahon, W. Supatto, S. Fraser, and A. Stathopoulos, "Dynamic analyses of drosophila gastrulation provide insights into collective cell migration," *Science*, no. 322, pp. 1546–1550, 2008.
[4] J. Swoger, M. Muzzopappa, H. Lopez-Schier, and J. Sharpe, "4D retrospective lineage tracing using SPIM for zebrafish organogenesis studies," *J. Biophotonics*, vol. 4, pp. 122–134, 2011.
[5] Q. Wang, J. Niemi, C.-M. Tan, L. You, and M. West, "Image segmentation and dynamic lineage analysis in single-cell fluorescence microscopy," *Cytometry A.*, vol. 1, no. 77, pp. 101–110, Jan 2010.

10.7 A bioinformatics framework for easy setup and scale metagenomics analysis pipelines

Liren Huang (huanglr@cebitec.uni-bielefeld.de)
Supervisor/s: Alexander Sczyrba

Over the last decade, advanced next-generation sequencing (NGS) technology for metagenomics and single cell genomics have unraveled the mysteries of extremophile "microbial dark matter"[1]. Although, a handful of tools were developed for particular parts of the bioinformatics analysis, there are still bottlenecks on how to build case specific analysis pipelines to efficiently process those gigantic amounts of metagenomics sequencing data. We introduce a bioinformatics framework for easy setup of personalized metagenomics analysis pipelines. In this framework, most of the commonly used tools were collected. Their interfaces were standardized, modulated and can be dispatched by users for pipeline assembling. All modules were built into Docker containers and can be easily replaced by other containers or shipped to other machines and clusters. We also integrated MapReduce framework, which allow us to distribute pipelines on most high performance clusters (HPCs) , as well as to scale-out on multiple instances of Openstack clouds.

[1] W. L. et a. Wang, "Application of metagenomics in the human gut microbiome," *World J Gastroenterol*, vol. 21, pp. 803–814, 2015.

10.8 Analysis and Visualization of MSI Data

Jan Kölling (koelling@cebitec.uni-bielefeld.de)
Supervisor/s: Tim W. Nattkemper, Karsten Niehaus

The basic workings of any organism as well as specific processes like the growth of a tumor can be seen as biological systems. To understand them it is not only required to know which components they are comprised of, but also how, when and where they interact with each other. Therefore researchers have always tried to get as good of a view as possible of their targets by building better imaging systems and other analytical techniques. Many methods now reach a very high resolution when focusing on a single property of the system in question: The molecular composition of a sample can be studied in detail with techniques from the fields of spectrometry or spectroscopy and the spatial organization can be studied with a wealth of methods from the field of microscopy.

Mass spectrometry imaging (MSI) builds a bridge between the long established analytical techniques of mass spectrometry and microscopical imaging. It generates a series of mass spectra from discrete sample positions on a tissue, thereby providing high-resolution information on molecular composition and spatial distribution in a single high-throughput experiment. This allows for an untargeted and simultaneous measurement of a wide variety of molecules, including proteins, peptides, lipids and metabolites. This wide range of possible targets makes it a suitable analysis method for many research questions from plant metabolism to biomarkers for human diseases[1]. However, due to the size and complexity of the resulting data, automated processing and tools to augment the researchers capabilities for data analysis become necessary.

Therefore the goal of this project is the design and development of a new integrative approach to analyze MSI data sets to aid the MSI analyst. For this purpose a set of analysis strategies and software tools is being developed and integrated with existing complimentary data sources and omics tools. Furthermore, the wealth of information in the data sets can be better accessed if computational analysis is supplemented with interactive visualization tools to leverage the human capability for pre-attentive visual processing.

So far several tools[2] have been developed in close collaboration with biologists and biochemist and the results have been directly applied to their research on industrially relevant processes like cereal germination[3], but also human diseases like glioblastoma and artheriosclerosis.

[1] M. M. Gessel, J. L. Norris, and R. M. Caprioli, "MALDI imaging mass spectrometry: Spatial molecular analysis to enable a new age of discovery," *Journal of Proteomics*, vol. 107, pp. 71–82, 2014.

[2] J. Kölling, D. Langenkämper, S. Abouna, M. Khan, and T. W. Nattkemper, "WHIDE - A web tool for visual data mining colocation patterns in multivariate bioimages," *Bioinformatics*, vol. 28, no. 8, pp. 1143–1150, 2012.

[3] K. Gorzolka, J. Kölling, T. W. Nattkemper, and K. Niehaus, "Spatio-Temporal Metabolite Profiling of the Barley Germination Process by MALDI MS Imaging." *PloS one*, vol. 11, p. e0150208, 2016.

10.9 Computational Determination of New Functional RNAs from Viral Genomes

Benedikt Löwes (bloewes@uni-bielefeld.de)
Supervisor/s: Robert Giegerich, Peter Unrau

Viral interactions are essential for the infection of host organisms and the subsequent replication of the viral genome in the host cell. These interactions are often based on specific RNA motifs shared between different evolutionary distant viruses. We observe that convergent evolution is a potential mechanism that explains similar motifs in phylogenetically distant viruses that infect common hosts by interacting with their cellular components. This is supported by the fact that for those specific RNA motifs similar selection criteria prevail. In this regard, the Hammerhead ribozyme is a well-studied example[1].

We focus on identifying new functional RNAs from viral genomes based on structural agreement of the RNA secondary structure, in order to find new examples of viral interactions with their host cells which are essential for the infection of the host and the replication of the virus. Previous approaches for identifying viral ncRNAs often strongly relied on sequence homology as well as pre-annotated RNA families in databases, i.e. *Rfam*[2]. Our approach, on the other hand, for the detection of the aforementioned convergent evolution uses conservation and convergence on the secondary structure level as primary information and the primary sequence only as additional source of information. This is based on the assumption that agreement on the level of secondary structure is the primary criterion for different viral RNA molecules to interact in a similar fashion with cellular components.

After identifying clusters of similar RNA elements by either only RNA structure matching, or a fast seed-based approach that takes structure and part of the sequence into account, or hierarchical RNA matching that uses an abstraction of the secondary structure, we incorporate phylogenetic information[3] to ensure that the candidates that form a cluster with similar secondary structure stem from phylogenetically distant viruses. The most promising candidates of convergent evolution can be used as evidence to show that RNAs from phylogenetically distant viruses "look and behave" the same way, but evolved completely independent from one another by a subsequent manual analysis in the laboratory.

[1] C. Hammann, A. Luptak, J. Perreault, and M. de la Pena, "The ubiquitous hammerhead ribozyme," *RNA*, vol. 18, no. 5, pp. 871–885, May 2012.

[2] S. W. Burge, J. Daub, R. Eberhardt, J. Tate, L. Barquist, E. P. Nawrocki, S. R. Eddy, P. P. Gardner, and A. Bateman, "Rfam 11.0: 10 years of RNA families," *Nucleic Acids Res.*, vol. 41, no. Database issue, pp. D226–232, Jan 2013.

[3] Y. Bao, S. Federhen, D. Leipe, V. Pham, S. Resenchuk, M. Rozanov, R. Tatusov, and T. Tatusova, "National center for biotechnology information viral genomes project," *J. Virol.*, vol. 78, no. 14, pp. 7291–7298, Jul 2004.

10.10 Reconstructing ancestral genomes including aDNA

Nina Luhmann (nluhmann@techfak.uni-bielefeld.de)
Supervisor/s: Cedric Chauve, Jens Stoye, Roland Wittler

Reconstructing ancestral genomes is a long-standing computational biology problem with important applications to large-scale sequencing projects. Informally, the problem can be defined as follows: Given a phylogenetic tree representing the evolutionary history leading to a set of extant genomes, we want to reconstruct the structure of the ancestral genomes corresponding to the internal nodes of the phylogeny. Global approaches simultaneously reconstruct ancestral gene orders at all internal nodes of the considered phylogeny, generally based on a parsimony criterion. However while complex rearrangement models can give insights into underlying evolutionary mechanisms, from a computational point of view, this problem is NP-hard for most rearrangement distances.

Besides the phylogeny and the extant genome sequences, a third source of data for reconstruction became available recently. Due to the progress in sequencing technologies, ancient DNA (aDNA) found in conserved remains can be sequenced. One example is the genome of the ancestor of *Yersinia pestis* strains that is understood to be the cause of the Black Death pandemic[1]. However, enviromental conditions influence sources for such paleogenomes and result in degradation and fragmentation of DNA molecules over time. This entails the reconstruction of the genome to be specifically challenging and leads only to a fragmented solution requiring additional scaffolding.

The goal of this project is to integrate new ancient sequencing information in the reconstruction of ancestral genomes. The comparison with extant genomes in the phylogeny can scaffold the fragmented assembly of the aDNA data while offering a lot of questions regarding the modeling of the genomes and the rearrangement model applied. This project aims to develop algorithms addressing these problems in reconstruction and scaffolding with the focus on the fragmented ancient assembly. So far, we developed an extension of the exact algorithm to reconstruct genomes under the Single-Cut-or-Join rearrangement distance[2]. It includes ancient DNA sequencing information in the reconstruction of ancestral genomes and also scaffolds the fragmented aDNA assembly while minimizing the SCJ distance in the tree[3]. We then generalized this result in an approach combining the evolution under the SCJ model with prior information of the genome structure at internal nodes of the tree, e.g. derived from the available aDNA data. We developed an exact algorithm under this objective and applied it to the *Yersinia pestis* data.

[1] K. I. Bos, V. Schuenemann, and others, "A draft genome of yersinia pestis from victims of the black death," *Nature*, vol. 478, pp. 506–510, 2011.

[2] P. Feijão and J. Meidanis, "SCJ: A breakpoint-like distance that simplifies several rearrangement problems," *IEEE/ACM TCBB*, vol. 8, pp. 1318–1329, 2011.

[3] N. Luhmann, C. Chauve, J. Stoye, and R. Wittler, "Scaffolding of ancient contigs and ancestral reconstruction in a phylogenetic framework," in *BSB 2014*, vol. 8826, Springer, 2014, pp. 135–143.

10.11 Efficient Grouping and Cluster Validity Measures for NGS Data

Markus Lux (mlux@techfak.uni-bielefeld.de)
Supervisor/s: Barbara Hammer

Modern high-throughput technologies allow for sequencing of vast amounts of DNA and RNA. Single-cell sequencing and metagenomics deliver exciting data sources that are beneficial in a multitude of domains, most prominently biomedical research and the analysis of complex disease pathways. A major problem in single-cell sequencing is sample contamination with foreign genetic material. Here, it is desirable to be able to automatically detect the number of genomes in a given sample. Metagenomics is confronted with a similar problem, namely the detection of clusters representing the involved species in a sample. Automated binning methods would greatly speed up the analysis process of such, opening the door for sophisticated research in affected fields. Albeit powerful technologies exist for the identification of known taxa, de novo binning is still in its infancy. This research project focuses on efficient grouping and cluster validity measures where we adapt, compare and evaluate novel machine learning techniques in the context of such data.

Typically, genomic data can be represented in a high-dimensional vector space, making it inherently difficult for classical learning techniques as they suffer from the curse of dimensionality. Thus, it is crucial to use subspace projections or strong regularization. Additionally, the number of clusters is unknown and clustering results heavily depend on the chosen set of parameters which can be large. In order to generate useful results, it is also beneficial to incorporate side information such as coverage data. This is accompanied by the fact that such data sets are often large, making standard algorithms inapplicable because of quadratic or worse runtime or memory complexity.

10.12 Towards the analysis of mixture effects in interactive metabolomics research

Lukas Pfannschmidt (lpfannschmidt@techfak.uni-bielefeld.de)
Supervisor/s: Barbara Hammer

One of the main goals of biology is to understand all components in a cell, the connections between them and their function. While genomic and proteomic data made great strides in recent years, it was not enough to get a complete understanding of the internal structure and behavior of a cell. To get the whole picture, metabolomics research is a necessary tool to fill in missing information between the genotype and phenotype[1,2].

The metabolome itself is a metabolite snapshot of the organism at the time of sample retrieval. Unlike the genome, the metabolome is highly variable over short periods of time and in different contexts of the organism. By comparing samples from different experimental conditions one can learn about the reaction of the organism to external influences. It is possible to observe direct effects of a substance, specifically harmful effects in the case of toxicants. Toxicometabolomics[3] look at these effects and try to get knowledge of the underlying metabolism.

One example is to study pesticides, fungicides and insecticides in the farming and food industry. This is done to rule out any negative health effects on the consumer. Testing of harmfulness is mostly done with help of in-vivo animal testing[4]. Normally these risk assessment studies are concerned with a singular toxicant. Because of widespread use of pesticides and others, it is very likely for the consumer to ingest multiple different combinations of them in small dosages. To rule out any health risks, all possible combinations would need to be tested. If one can determine the behavior of multiple toxicants at the same time, the critical dosage of toxicants could be inferred without the need for widespread animal testing.

In our work, we focus on the analysis of mixture effects which are differences in metabolite levels between samples coming from experiments in isolated conditions and their mixture. We try to improve the preprocessing and dimensionality reduction steps to find features which explain the observed mixture effects and create models to infer mixture effects.

[1] O. Fiehn, "Combining genomics, metabolome analysis, and biochemical modelling to understand metabolic networks," *Comparative and Functional Genomics*, vol. 2, no. 3, pp. 155–168, 2001.

[2] O. Fiehn, "Metabolomics – the link between genotypes and phenotypes," *Plant Molecular Biology*, vol. 48, no. 1, pp. 155–171.

[3] M. Bouhifd, T. Hartung, H. T. Hogberg, A. Kleensang, and L. Zhao, "Review: Toxicometabolomics," *Journal of Applied Toxicology*, vol. 33, no. 12, pp. 1365–1383, 2013.

[4] S. Scholz, E. Sela, L. Blaha, T. Braunbeck, M. Galay-Burgos, M. Garcia-Franco, J. Guinea, N. Kluever, K. Schirmer, K. Tanneberger, and others, "A european perspective on alternatives to animal testing for environmental hazard identification and risk assessment," *Regulatory Toxicology and Pharmacology*, vol. 67, no. 3, pp. 506–530, 2013.

10.13 New insights into metagenomes through metadata

Madis Rumming (mrumming@cebitec.uni-bielefeld.de)
Supervisor/s: Alexander Sczyrba, Barbara Hammer, Fiona Brinkman

The advent of new sequencing technologies opened up the new promising field of studying whole environmental samples and the organisms living within them. The research field of metagenomics offers insights into environmental microbial communities. Two widely used methods are 16s rDNA based analysis of the phylogenetical composition of a metagenomic sample[1] and the analysis of all genomic sequences found in a sample using high throughput sequencing technologies[2]. The analytical results from metagenomic studies can be heterogeneous caused by the applied analytical and computational methods. Consequently comparison of metagenomic studies is a challenging task. The use of interpretable project comparison rules and the interpretation of those comparisons itself are not sufficiently investigated.

The main goal of this PhD project is to enhance the analysis of metagenome studies through the use of metadata. Project and its sample related metadata are acquired during sample collection and is to be compared to other metagenomes using the embodied metadata and the metadata of the contained genomes in each sample, coupled with metadata-enrichment studies. A subsequent task is automatic metadata acquisition, processing the heterogenous project data and metadata, genomic data and metadata respectively, and further data analysis with data mining techniques bridging to a controlled vocabulary.

For this purpose, MetaStone — Metagenomic Storage of novel entities — is under development; A data warehouse-driven online tool for metadata-based association studies for metagenomes and 16s rRNA community profiles: cross-comparison, metadata-enrichment studies, visualization, and annotation validation of metagenomic studies. The underlying data warehouse contains metadata on the genome level for 33,000+ bacterial / 650+ archaeal genomes, and 4000+ metagenomes, which is initially filled with data taken from Integrated Microbioal Genommes[3] system. Analyzed metagenomes unknown to MetaStone can be used to enhance the knowledgebase, if desired by the researcher. The metadata contains e.g. information about environmental conditions at host / sampling site (temperature, oxygen, primary energy source), pfams, and/or metabolic pathways. A set of classifiers on categorized metadata is used to compare metagenomes.

[1] J. E. Clarridge, "Impact of 16S rRNA gene sequence analysis for identification of bacteria on clinical microbiology and infectious diseases," *Clinical microbiology reviews*, vol. 17, no. 4, pp. 840–862, 2004.
[2] J. C. Wooley, A. Godzik, and I. Friedberg, "A primer on metagenomics," *PLoS Comput Biol*, vol. 6, no. 2, p. e1000667, 2010.
[3] V. M. Markowitz, I.-M. A. Chen, K. Palaniappan, K. Chu, E. Szeto, Y. Grechkin, A. Ratner, B. Jacob, J. Huang, P. Williams, and others, "IMG: The integrated microbial genomes database and comparative analysis system," *Nucleic acids research*, vol. 40, no. D1, pp. D115–D122, 2012.

10.14 Reconstructing the Subclonal Composition of Cancer Samples

Linda K. Sundermann (lsundermann@uni-bielefeld.de)
Supervisor/s: Quaid Morris, Gunnar Rätsch, Jens Stoye

Cancer samples are often genetically heterogeneous, which means that the cells involved in a tumor have different mutations in the DNA. Typical mutations are copy number variations (CNVs) where a segment of DNA is amplified or deleted and simple somatic mutations (SSMs) where a single brink of the DNA is exchanged, inserted or deleted. Cells with the same set of mutations can be described as a subclonal population (subpopulations). Information about the mutations in the subpopulations can help to identify the mutations that are responsible for the progress of cancer, or to choose targeted therapies. To analyze the mutations, the DNA of parts of the tumor is sequenced, often in an approach called "bulk-sequencing". Here, the result is not yet the complete DNA-sequence of the individual cells but a set of reads, short segments of the DNA. These reads are now mapped to a reference sequence of the human genome to find mutations.

Recently, several methods that attempt to infer the set of mutations for subpopulations using detected CNVs, SSMs, or both have been published[1,2]. Here, we present *Onctopus*, a new approach to jointly model and reconstruct the subclonal composition of a bulk tumor sample utilizing SSMs and CNVs.

Given the frequency of SSMs and heterozygous germline SNPs, which are structually equal to SSMs but which were already inherited from the parents and appear in a much higher number, as well as information about the position and number of reads of segments affected by CNVs, Onctopus assigns a frequency, CNVs and SSMs to subclonal lineages (sublineages). Each of these lineages is defined through the CNVs and SSMs that arose in this lineage. SNPs, which are needed to identify copy number changes in sublineages, are assigned to the normal lineage.

We build a joint likelihood model and model the tumor as consisting of a mixture of lineages on which we infer a partial order. We choose sublineages to avoid ambiguous solutions that can occur when copy numbers are determined for subpopulations. We developed a linear relaxation of our model as a mixed integer linear program that can be solved with state-of-the-art solvers.

The goal of this project is to develop a method for the resonstruction of the subclonal composition of a tumor sample that is more accurate than recent methods.

[1] A. Fischer, I. Vázquez-García, and others, "High-definition reconstruction of clonal composition in cancer," *Cell Reports*, vol. 7, no. 5, pp. 1740–1752, 2014.

[2] P. Deshwar A.G., S. Vembu, and others, "PhyloWGS: Reconstructing subclonal composition and evolution from whole-genome sequencing of tumors," *Genome Biology*, vol. 16, p. 35, 2015.

10.15 High performance cloud computing for comparative genomics

Jia Yu (yujia@techfak.uni-bielefeld.de)
Supervisor/s: Jochen Blom, Alexander Goesmann

Recently, the rapid developments in different fields such as biology, chemistry and physics have led the sequencing technology into the *next generation*. It not only accelerates the speed of sequencing a whole genome but also reduces its expense. With the enormous advantage of NGS technology, researchers now have the potential to analyze multiple genomes of several related bacterial strains at once to answer complex biological questions. However, the massive genome data are not feasible to analyze manually on a commodity computer. In order to efficiently tackle with multiple genomes at once, one idea is to use *cloud computing*.

EDGAR is the abbreviation of Efficient Database framework for comparative Genome Analysis using BLAST score Ratios[1] currently maintained by Justus Liebig University Giessen (JLU). It is a cloud framework that combines popular features of prokaryotic comparative genomics. However, with the rapidly growing efficiency of sequencing technology as well as research demands, EDGAR meets the bottle neck of data flood. Therefore it is urgent to improve the efficiency of EDGAR with regard to massive genome data.

The goal of this project is to propose a high performance back end of EDGAR. The improvements can be split into three levels. On the algorithmic level, we will test several recently released alignment algorithms to replace BLAST[2] in the framework based on their performances and accuracies. On the computational model level, we implement Apache Hadoop MapReduce[3] algorithm to parallelize heavy computations. Lastly on the database level, the Hadoop[4] compatible database model Apache HBase[5] will replace MySQL[6] because it is distributed and highly available. A new query scheme will also be designed for the new database. Hopefully, with the combination of these improvements, EDGAR will overcome the obstacle of massive data volume.

[1] J. Blom, S. P. Albaum, D. Doppmeier, A. Puhler, F. J. Vorholter, M. Zakrzewski, and A. Goesmann, "EDGAR: a software framework for the comparative analysis of prokaryotic genomes," *BMC Bioinformatics*, vol. 10, p. 154, 2009.
[2] W. J. Kent, "BLAT–the BLAST-like alignment tool," *Genome Res.*, vol. 12, no. 4, pp. 656–664, Apr 2002.
[3] T. White, *Hadoop: The definitive guide*, 1st ed. O'Reilly Media, Inc., 2009.
[4] T. White, *Hadoop: The definitive guide*, 1st ed. O'Reilly Media, Inc., 2009.
[5] The Apache Software Foundation, "Apache HBase^{TM} reference guide." 2016.
[6] M. Widenius and D. Axmark, *Mysql reference manual*, 1st ed. O'Reilly & Associates, Inc., 2002.

10.16 Functional Analysis of a Pan-genome

Tina Zekic (tzekic@techfak.uni-bielefeld.de)
Supervisor/s: Jens Stoye, Stephan Albaum

As the advances in DNA sequencing technologies lead to a decrease in sequencing time and costs, the number of completely sequenced genomes continues to grow. Therefore, the number of genomes belonging to different strains of the same species also increased, enabling the analysis of species-related characteristics. As a result, the concept of a *pan-genome*[1] arised, representing a set of genomes belonging to different strains of a species. A pan-genome is composed of three parts, the *core* genome, representing sequences shared among all strains of a species, the *dispensable* genome, containing sequences shared among a subset of strains and the *singleton* genome, representing strain-specific sequences.

Recently, a data structure for a memory efficient storage of a pan-genome has been developed[2]. The so-called Bloom Filter Trie (BFT) stores a pan-genome as a colored de Bruijn graph, by storing all k-mers of the input sequences and the set of genomes they originate from. The nodes in a de Bruijn graph represent k-mers, where two nodes are connected by an edge if their k-mers overlap on $k-1$ characters. The nodes can be colored by the annotation, denoting the genome(s) a k-mer comes from. The BFT does not store the edges explicitly.

The goal of this project is to extend this basic data structure by methods for the functional analysis of a pan-genome. The first step is the identification of the pan-genome, i.e. the core, dispensable and singleton genomes. The core genome with 100% sequence identity would represent a simple path in a de Bruijn graph, with each node containing all annotations. However, matching sequences can be interrupted by SNPs or other structural variations, resulting in branching nodes and additional paths in the graph. For this, we developed an alignment-free algorithm for core genome identification based on a seed-and-extend approach. A seed represents paths in the graph annotated with a predefined number of genomes. Reaching branching nodes in the graph, the traversal continues up to a given limit in order to extend the seed with another. Like this, also possible sequence varations will be included in the core sequences. We further plan on extending this algorithm as well as introducing functionalities such as listing genes contained in the identified core region.

[1] H. Tettelin, V. Masignani, M. Cieslewicz, and others, "Genome analysis of multiple pathogenic isolates of streptococcus agalactiae: Implications for the microbial "pan-genome"," *Proceedings of the National Academy of Sciences USA*, vol. 102, no. 39, pp. 13950–13955, 2005.

[2] G. Holley, R. Wittler, and J. Stoye, "Bloom filter trie–a data structure for pan-genome storage," in *Algorithms in bioinformatics*, Springer, 2015, pp. 217–230.

10.17 Protein subcellular localization analysis based on protein-protein interaction data

Lu Zhu (lzhu@techfak.uni-bielefeld.de)
Supervisor/s: Ralf Hofestädt, Martin Ester

The function of a protein is highly associated with its corresponding subcellular localization (SCL). Proteins can only find their correct interacting molecules at the right place and right moment. Thus, protein SCL is an essential part to interpret and to identify the functions of the proteins of interest that helps to suggest hypotheses on the mechanisms of a cell. Therefore meaningful data and methods to reliably and systematically study protein SCL and hence their mislocalization and the disruption of protein trafficking that are relied upon by the cell biology community are essential[1].

Physical interactions between proteins play an essential role in the proper functioning of living cells. To interact, proteins (or any other molecules) must necessarily share a common subcellular location (SCL), or an interface between physically adjacent SCLs, at least transiently or conditionally[2]. A reliable protein-protein interaction network could improve SCL prediction under a particular biological context. The analysis of the changes of PPI network over time or different conditions together with the changes of SCL over time could be very helpful for the generalization of the hypotheses in system biology research.

The motivation of this project is not only to predict the SCL for unannotated protein and also to help users to 'select' one SCL of protein from many when this protein is annotated by multiple SCL for the further analysis. The method we propose here is to apply PPI data to a MRF model to 'score' these multiple SCL and then give the best scored SCL to query proteins. We introduce the translocation matrix in this model that gives scores to SCL pairs according to the occurrence of the interacting proteins present in a particular SCL. Finally, the query network will be visualized in CELLmicrocosmos PathwayIntegration(CmPI)[3] in a virtuel cell in 3D.

[1] M.-C. Hung and W. Link, "Protein localization in disease and therapy." *Journal of cell science*, vol. 124, no. Pt 20, pp. 3381–92, Oct. 2011.

[2] J. R. Perkins, I. Diboun, B. H. Dessailly, J. G. Lees, and C. Orengo, "Transient protein-protein interactions: structural, functional, and network properties." *Structure (London, England : 1993)*, vol. 18, no. 10, pp. 1233–43, Oct. 2010.

[3] B. Sommer, B. Kormeier, P. S. Demenkov, P. Arrigo, K. Hippe, Ö. Ates, A. V. Kochetov, V. a Ivanisenko, N. a Kolchanov, and R. Hofestädt, "Subcellular localization charts: a new visual methodology for the semi-automatic localization of protein-related data sets." *Journal of bioinformatics and computational biology*, vol. 11, no. 1, p. 1340005, Feb. 2013.

11 RTG 1907: Role-based software infrastructures for continuous-context-sensitive systems

Prof. Dr.-Ing. Wolfgang Lehner (wolfgang.lehner@tu-dresden.de)
Technische Universität Dresden
http://wwwdb.inf.tu-dresden.de/rosi

Software with long life cycles is faced with 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. Only then, software can be called consistently context-sensitive.

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.

11.1 Formal Semantics for Models with Meta-Predicates

Stephan Böhme (stephan.boehme@tu-dresden.de)
Supervisor/s: Prof. Dr.-Ing. Franz Baader

When modeling a domain using concepts like *rôles*, *phases*, etc. it is important that all these so called meta-predicates have a formal definition and a well-defined semantics. To be able to express them in a suitable logic has several advantages. Stronger inferences can be drawn and inconsistencies can be found that would have stayed undetected otherwise. All the properties of these meta-predicates might be expressible in full first-order logic, but since reasoning in this logic is undecidable, automatic reasoning is not possible. Another family of knowledge representation formalisms are *Description Logics* (DLs) which are very expressive, but still provide decidable reasoning tasks.

Examining the properties of the meta-predicate rôle it becomes apparent that the notion of *context* is crucial for defining how a rôle behaves. DLs are well-suited to describe contexts as formal objects with formal properties that are organized in relational structures. However, classical DLs lack expressive power to formalize furthermore that some individuals satisfy certain concepts and relate to other individuals depending on a specific context. Therefore, often two-dimensional DLs are employed. Based on approaches by Klarman et al.[1], I investigated a family of two-dimensional *Description Logics of contexts*[2] (CDLs) that stay decidable even in the presence of rigid roles, i.e. DL roles that are required to be interpreted the same in all contexts.

Another key property of rôles is their dynamic behaviour. One does not only change playing a rôle depending on the context, but also on a certain time. Until now that dynamic aspect of roles is neglected, but I will study combinations of DLs of context and temporal logics. Apart from choosing a suitable temporal logic, a main research question will be how different combinations affect the expressiveness and computational complexity. Prior work on temporal DLs by Baader et al.[3] will serve as a starting point.

To my best knowledge, up to now there exists no DL reasoner that can handle DLs of context. So in order to use such systems, an appropriate calculus must be developed and implemented. There exist highly optimized DL reasoners, which are based on tableau or hypertableau[4] calculus. Investigation and adaption of these calculi will result in a prototypical implementation of a CDL reasoner.

[1] S. Klarman and V. Gutiérrez-Basulto, "Two-dimensional description logics for context-based semantic interoperability," in *Proceedings of AAAI-11*, 2011.

[2] S. Böhme and M. Lippmann, "Decidable description logics of context with rigid roles," in *Proceedings of FroCoS-15*, 2015, vol. 9322, pp. 17–32.

[3] F. Baader, S. Ghilardi, and C. Lutz, "LTL over description logic axioms," *ACM Transactions on Computational Logic*, vol. 13, no. 3, 2012.

[4] B. Motik, R. Shearer, and I. Horrocks, "Hypertableau Reasoning for Description Logics," *Journal of Artificial Intelligence Research*, vol. 36, pp. 165–228, 2009.

11.2 Context-based Reasoning in Ontologies

İsmail İlkan Ceylan (ceylan@tcs.inf.tu-dresden.de)
Supervisor/s: Prof. Dr.-Ing. Franz Baader

Description Logics (DLs) constitute a family of knowledge representation formalisms that has been successfully employed in various application domains. The particular syntax of a DL allows one to form axioms, which in turn, are used to encode the knowledge of a particular domain. Intuitively, a DL ontology is a (finite) set of such axioms, which restricts the possible set of interpretations over a knowledge domain.

The motivation behind this dissertation is the fact that classical DL ontologies are not suited to represent contextual knowledge inherent to many real world applications. Our goal is to investigate context-based reasoning techniques to close this gap. In a nutshell, we view each context as a subset of the given ontology. Given the possibility to distinguish a piece of knowledge w.r.t. the context it is entailed from leads to different non-standard reasoning problems in DL ontologies, which constitutes the basis in this thesis.

We employ context-based reasoning to facilitate probabilistic reasoning over DL ontologies by defining a probability distribution over the context space with the help of a Bayesian Network[1]. The resulting formalism, Bayesian DLs, is a family of probabilistic DLs where every piece of knowledge is associated with a (conditional) probability: Every consequence of the ontology is a probabilistic consequence, determined w.r.t. the probabilities of the contexts it is entailed from. Several reasoning problems have been studied in this setting, leading to tight complexity bounds for some Bayesian DLs[2]. Recent work on Bayesian DLs focused on (probabilistic) conjunctive query answering[3] and on time-evolving probabilities[4].

Context-based abstraction of ontologies forms a flexible framework and can also be used for other means of reasoning. Besides representing uncertainty, we use this technique to encode preferences over different axioms. In this setting, we describe preferences over the context space and perform preference-based reasoning tasks such as finding the most preferred answers to a query[5].

[1] İ. İ. Ceylan and R. Peñaloza, "The bayesian description logic $\mathcal{BEL}$," in *Proceedings of the 7th international joint conference of automated reasoning (IJCAR 2014)*, 2014, pp. 480–494.

[2] İ. İ. Ceylan and R. Peñaloza, "Tight complexity bounds for reasoning in the description logic $\mathcal{BEL}$," in *Proceedings of the 14th european conference of logics in artificial intelligence (JELIA2014)*, 2014, pp. 77–91.

[3] İsmail İlkan Ceylan, "Query answering in bayesian description logics," in *Proceedings of the 28th international workshop on description logics (DL'15)*, 2015, vol. 1350.

[4] İsmail İlkan Ceylan and R. Peñaloza, "Dynamic bayesian description logics," in *Proceedings of the 28th international workshop on description logics (DL'15)*, 2015, vol. 1350.

[5] İsmail İlkan Ceylan, T. Lukasiewicz, and R. Peñaloza, "Answering EL queries in the presence of preferences," in *Proceedings of the 28th international workshop on description logics (DL'15)*, 2015, vol. 1350.

11.3 Formal Quantitative Analysis of Role-based Systems

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

Role-based modeling is a promising approach to cope with the context-dependence 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 the thesis is to develop operational models for role-based software infrastructures 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.

11.4 Database Versioning

Kai Herrmann (kai.herrmann@tu-dresden.de)
Supervisor/s: Prof. Dr.-Ing. Wolfgang Lehner

Changes in modern software systems are no longer an exception but have become daily business. Following the mantra "Evolution instead of Revolution", the software technology community developed agile project management. The idea is to launch a first version of a product early and continue the development in short release cycles. This provides direct feedback, hence, a dynamic and effective software development. A major obstacle in this process is the rather inflexible database, since existing data needs to be maintained according to schema changes, which is usually realized by manual SQL scripts. This is expensive and error-prone. To keep pace with agile software developers, we need sophisticated support for *database evolution*.

However, this is not enough. The continuous evolution of a single application does not cover the whole complexity of modern software development. Often, old schema versions need to stay available to support legacy applications. This issue becomes even more challenging, as multiple applications share a database as the single point of truth. Hence, there are many different applications in many different versions, each having an individual view on the same data. This heterogeneity prohibits a joint upgrade to a new schema version and requires *database versioning*.

Current research results provide extended support for database evolution by specifying the evolution descriptively using schema modification operators[1]. They define the evolution of both the schema and the data in compact and consistent steps. Building upon such an existing database evolution language, we develop *CoDEL*[2], a database evolution language with important characteristics like completeness and a precisely defined syntax and semantics. By making the operations of CoDEL fully invertible, we realize database versioning. To the best of our knowledge, we are the first to develop a holistic tool for database versioning.

In the RoSI RTG, we aim at realizing a *role-based* database schema. Obviously, also such role-based models are subject to the continuous evolution. Hence, we extend the concepts for evolution and versioning of relational databases to role-based databases. This is an inevitable requirement to make the role-based software development practically applicable.

[1] C. Curino, H. J. Moon, A. Deutsch, and C. Zaniolo, "Automating the database schema evolution process," *VLDB Journal*, vol. 22, no. 1, pp. 73–98, Dec. 2013.

[2] K. Herrmann, H. Voigt, A. Behrend, and W. Lehner, "CoDEL - A relationally complete language for database evolution," in *Advances in databases and information systems - 19th east european conference, ADBIS 2015, Poitiers, France, September 8-11, 2015, proceedings*, 2015, vol. 9282, pp. 63–76.

11.5 Role-based Declarative Modeling of Processes in the Internet of Things

Steffen Huber (steffen.huber@tu-dresden.de)
Supervisor/s: Prof. Dr.-Ing. Thomas Schlegel

Recently, the Internet of Things (IoT) has been gaining increased attention from the Business Process Management (BPM) community. Integrating sensors and actuators into Process Aware Information Systems (PAIS) allows for annotating Business Process Intelligence related data with real-time context information and moreover for the direct manipulation of real-world objects. In a broader sense, IoT-enabled processes provide means for context-aware process execution involving virtual and physical entities.

Internet of Things-aware process execution imposes new requirements on process modeling, that are outside the scope of current modeling languages. IoT devices may vanish, appear or stay unknown during process execution. Therefore, design time process resource allocation is not feasible. From the process resource perspective, IoT devices may be able to play varying roles depending on the device capabilities and real world context at runtime. However, context-sensitive IoT service interfaces are not considered by current process modeling approaches. Additionally, context information changes and process related events may occur at any time during process execution, rendering most imperative process modeling approaches infeasible. In order to meet the required flexibility of ad-hoc ubiquitous systems in IoT, we aim at developing a role-based declarative modeling language using Linear Temporal Logic (LTL) semantics. From the process control-flow perspective, roles can be used to describe the context-sensitive interoperability capabilites of imperatively modeled subprocesses. Therefore, LTL constraint patterns are used for the role-based declarative modeling of imperatively modeled subprocess constraints. These subprocesses are annotated with playable roles describing the context-sensitive interoperability capabilities. To facilitate this flexiblity on the subprocess level, we use a novel concept for integrating semantic queries into process activities to support runtime discovery and dynamic invocation of IoT-services[1] as an extension to an existing imperative process metamodel[2].

We propose a hybrid modeling approach consisting of imperatively modeled subprocesses and declaratively modeled constraints, enabling a flexible composition of executable processes at runtime. Role concepts are applied both for context-sensitive capability specification of subprocesses and for allocating their enacting resources.

[1] S. Huber, R. Seiger, and T. Schlegel, "Using semantic queries to enable dynamic service invocation for processes in the internet of things," in *Semantic computing (ICSC), 2016 IEEE international conference on*, 2016, pp. 214–221.

[2] R. Seiger, S. Huber, and T. Schlegel, "PROtEUS: An integrated system for process execution in cyber-physical systems," in *Enterprise, business-process and information systems modeling*, vol. 214, 2015, pp. 265–280.

11.6 Role-based Database Model and Architecture

Tobias Jäkel (tobias.jaekel@tu-dresden.de)
Supervisor/s: Prof. Dr.-Ing. Wolfgang Lehner

Currently, there is a mismatch between the conceptual model of an information system and its implementation in a Database Management System (DBMS). Most of the conceptual modeling languages relate their conceptual entities with relationships, but relational database management systems solely rely on the notion of relations to model both, entities and relationships. To make things worse, real world objects are not static as assumed in such modeling languages, but change over time. Thus, modeling languages were enriched to model those scenarios, as well. However, mapping these models onto relational databases requires the use of object-relational mapping engines, which in turn hide the semantics of the conceptual model from the DBMS. Consequently, traditional relational database systems cannot directly ensure specific consistency constraints and thus lose their meaning as single point of truth for highly distributed information systems.

To overcome these issues, we propose a novel data model and query language introducing role-based data structures in DBMSs[1]. The data model defines Dynamic Data Types on the schema level and Dynamic Tuples on the instance level, which ensures role-based integrity and consistency constraints in a DBMS. Additionally, Relationship Types and Relationships are introduced as first class citizen to connect those types[2]. To access and address this kind of data, we propose RSQL, a query language for role-based data structures. It extends the Data Definition Language, the Data Manipulation Language as well as the Data Query language by Dynamic Data Types and Dynamic Tuples. Additionally, the DBMS gains more knowledge on the stored semantics which opens a wide range of possible performance optimizations, for instance a more sophisticated query optimizer, smarter access paths, or specialized page layouts.

In sum, a DBMS equipped with RSQL improves the interoperability between several role-based applications by storing their complex and dynamic objects directly without hiding the semantics of roles and relationships in relations. Additionally, object-relational mapping engines become obsolete in scenarios where the applications as well as the DBMS implement roles.

[1] T. Jäkel, T. Kühn, H. Voigt, and W. Lehner, "RSQL - A Query Language for Dynamic Data Types," in *Proceedings of the 18th International Database Engineering & Applications Symposium*, 2014, pp. 185–194.

[2] T. Jäkel, T. Kühn, S. Hinkel, H. Voigt, and W. Lehner, "Relationships for Dynamic Data Types in RSQL," in *Datenbanksysteme für Business, Technologie und Web (BTW)*, 2015.

11.7 A Family of Role Modeling Languages

Thomas Kühn (thomas.kuehn3@tu-dresden.de)
Supervisor/s: Prof. Dr. rer. nat. habil. Uwe Aßmann

Role-based modeling has been proposed in 1977 by Charles W. Bachman[1], as a means to model complex and dynamic domains, because roles are able to capture both context-dependent and collaborative behavior of objects. Consequently, they were introduced in various fields of research ranging from data modeling via conceptual modeling through to programming languages[2]. More importantly, because current software systems are characterized by increased complexity and context-dependence[3], there is a strong demand for new concepts beyond object-oriented design. Although mainstream modeling languages, i.e., Entity-Relationship Model, Unified Modeling Language, are good at capturing a system's structure, they lack ways to model the system's behavior, as it dynamically emerges through collaborating objects[4]. In turn, roles are a natural concept capturing the behavior of participants in a collaboration. Moreover, roles permit the specification of interactions independent from the interacting objects. Similarly, more recent approaches use roles to capture context-dependent properties of objects. The notion of roles can help to tame the increased complexity and context-dependence. Despite all that, these years of research had almost no influence on current software development practice.

To make things worse, until now there is no common understanding of roles in the research community and no approach fully incorporates both the context-dependent and the relational nature of roles[5]. In my thesis, I will devise a formal model for a *family of role-based modeling languages* to capture the various notions of roles[6]. Together with a software product line of *Role Modeling Editors*, this will enable the generation of a *language family* for Role-based Software Infrastructures (RoSI).

[1] C. W. Bachman, M. Daya, C. W. Bachman, and M. Daya, "The role concept in data models," in *Proceedings of the third international conference on very large data bases*, 1977, vol. 3, pp. 464–476.

[2] F. Steimann, "On the representation of roles in object-oriented and conceptual modelling," *Data & Knowledge Engineering*, vol. 35, no. 1, pp. 83–106, 2000.

[3] S. Murer, C. Worms, and F. J. Furrer, "Managed evolution," *Informatik-Spektrum*, vol. 31, no. 6, pp. 537–547, 2008.

[4] T. Reenskaug and J. O. Coplien, "The DCI architecture: A new vision of object-oriented programming," *Artima Developer*, p. 14pp, 2009.

[5] 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.

[6] T. Kühn, S. Böhme, S. Götz, and U. Aßmann, "A combined formal model for relational context-dependent roles," in *Proceedings of the 2015 ACM SIGPLAN international conference on software language engineering*, 2015, pp. 113–124.

11.8 Towards Role Dispatch - Exploring Configurable 4-dimensional Role Dispatch

Max Leuthäuser (max.leuthaeuser@tu-dresden.de)
Supervisor/s: Prof. Dr. rer. nat. habil. Uwe Aßmann

Todays software systems always need to anticipate changing context. New business rules and functions should be implemented and adapted. The concept of role modeling and programming has been discussed frequently for decades across many scientific areas. It allows the modeling and implementation of context dependent information w.r.t. dynamically changing context. Hence future software infrastructures have the intrinsic need to introduce such a role concept.

Having objects playing roles immediately raises the important question of the identity of the resulting compound object. Do they share the same identity? If so, who is responsible for answering the call and invocation of methods? And if not, how could the developer be enabled to explicitly define the desired target w.r.t. a specific context? The scope of this work is the development of an adequate solution. It is based on the fact that polymorphism is one of the key aspects of object-oriented programming languages. Methods may or may not be executed depending on the type of parameters provided during the method call. This declarative mechanism called dispatch is responsible for selecting the appropriate method. In common languages a dispatcher analyzes the type of object on which the call will be executed.

Until now the implementation with existing object oriented languages always requires the generation of a specific runtime environment and management code. The expressiveness of these languages is not able to cope with essential role-specific features, such as true delegation or binding roles dynamically. Hence, this work developed an adequate environment for roles at runtime. Its very lightweight implementation as library with Scala based on its Dynamic trait allows to augment an object's type at runtime implementing dynamic (compound-) role types. It enables role-based implementations that lead to more reuse and better separation of concerns and allows the specification of dynamic role dispatch.

11.9 Role Adaptation Through Intention Recognition

Jan Reubold (jan.reubold@tu-dresden.de)
Supervisor/s: Prof. Dr. Thorsten Strufe

Our research focuses on role information during runtime and how it can enhance privacy in social media. Given sequential behavioral data, the question is how to infer user intentions and how to apply this information then to the users' benefits. In the course of this process suitable algorithms for intention recognition will be surveyed and developed. A challenge in this context are the dynamics of the data. During runtime new data could occur, so suitable algorithms have to be able to adapt to this situation. The diversity of the underlying behavioral patterns represents another major challenge, e.g. given a dataset, how many different intentions underlie this data.

Many existing approaches in the field of intention recognition lack the ability to cope with these sequential datasets. So called finite mixture models assume that the data consists of subpopulations and explain it by fitting a specific distribution to each of them, e.g. Mixtures of Gaussians fit a Gaussian to each subpopulation. These models are capable of adapting to diverse datasets, but require a computationally expensive learning process. Furthermore, the resulting models are incapable of adapting to new unseen data.

Recent research endeavors in this area introduced nonparametric mixture models. The benefits of these models are the reduced computational costs for learning and the ability to adapt to new data. While finite mixture models use a fixed number of subpopulations, nonparametric mixture models adjust the number of mixtures to the data.

Our first contribution is developing a nonparametric equivalent to finite mixtures of Markov chains. This type of mixture model represents each subpopulation as a first-order Markov model. Due to the simple interpretability of the subpopulations, it is a preferred choice for user understanding tasks. Nonetheless, these models have a specific weakness when applied to these tasks. The number of subpopulations has to be fixed before learning the model, which is counter intuitive and a hindrance in such setups.

Our contribution solves this problem by developing an equivalent nonparametric mixture of Markov chains model called Infinite Mixture of Markov Chains (IMMC). A model which keeps the benefits of first-order Markov models while allowing the algorithm to learn the number of underlying mixtures from data.

As a next step we will evaluate if and to what extent IMMC is capable of learning intentions from data.

11.10 A Dynamic Instance Binding Mechanism for Run-time Variability of Role-based Software Systems

Nguonly Taing (nguonly.taing@tu-dresden.de)
Supervisor/s: Prof. Dr. rer. nat. habil. Dr. h. c. Alexander Schill

Variability is one of the major requirements for software systems executed in highly dynamic environments. The degree of variability of a system is determined by the number of contexts it can differentiate, its ability to perform foreseen or unforeseen changes, the granularity of change operations, the point in time these changes can be performed and the roll back mechanism in case of incident after applying adaptation.

Existing approaches for dynamic bindings working on the language level offer run-time variability only to a certain extent. Aspect-oriented Programming (AOP) weaves cross-cutting concerns into an object's code, uniformly adapting all instances of a given type, limiting the flexibility for rebinding variations, and not supporting unforeseen changes. Context-oriented Programming (COP) addresses the support of behavioral adaptation at the instance level based on layer activation. However, bringing both the anticipated and the unanticipated adaptation at the instance level is not directly supported[1]. Role-oriented Programming (ROP) also provides a solution to support variability by encapsulating dynamic behavior, modeled as role, to be bound to and unbound from the player containing static behaviors dynamically. Existing ROP solutions bind roles at compile or load time, though they can be (de)activated at run time to achieve adaptation. Therefore, this imposes a challenge to bind other unforeseen roles at run time, resulting only in foreseen adaptation that is supported[2].

Based on the concept of ROP, we address the problem of run-time variability at the instance level, allowing both anticipated and unanticipated adaptation to coexist in a single solution. We introduce a mechanism called *dynamic instance binding* that maintains a data structure representing the binding information between player and role instances in a look-up table. That table is used to dynamically invoke the behavior of the role to which a player is currently bound. The mechanism is implemented as part of the run-time, called *LyRT*, supporting the execution of role-based software systems. Based on that implementation, we demonstrate that dynamic instance binding can support flexible (re-)binding of roles and object instances as well as the introduction of new roles without having to restart the system. Furthermore, binding relation stored in the look-up table can be enhanced to support versioning of the adaptable configuration which can be triggered to roll back and forward ensuring the consistency of the adaptation.

[1] G. Salvaneschi, C. Ghezzi, and M. Pradella, "Context-oriented programming: A software engineering perspective," *Journal of Systems and Software*, vol. 85, no. 8, pp. 1801–1817, 2012.

[2] N. Taing, T. Springer, N. Cardozo, and A. Schill, "A dynamic instance binding mechanism supporting run-time variability of role-based software systems," in *Proceedings of modularity'16 workshop on live adaptation of software systems*, 2016, to appear.

11.11 Run-time Adaptation of Distributed Software Systems

Martin Weißbach (martin.weissbach1@tu-dresden.de)
Supervisor/s: Prof. Dr. rer. nat. habil. Dr. h. c. Alexander Schill

Software applications increasingly run in highly dynamic and heterogeneous execution environments that require behavioral and functional adaptation depending the user's and system's current situation and are furthermore distributed over multiple interconnected devices, cooperating to achieve a common goal. A coordinated adaptation is required in order to ensure a consistent system behavior in response to changes in the system's execution environment.

Existing approaches for distributed adaptable software systems focus on strategies and algorithms, e.g DecAp[1], to calculate change prescriptions for distributed environments as well as software architectures that allow for adaptation, e.g. Rainbow[2]. The execution of such change prescriptions, especially in an unstable environment coined by message loss or temporary partitioning of the system, has not been addressed by the proposed systems. If adaptation operations are assumed that have to be executed on multiple devices in a coordinated way to prevent the system from reaching invalid configurations, adaptation in unstable environments becomes a challenging task.

Our approach is based on the role-concept[3] and uses a distributed middleware architecture of *execution runtimes* that performs adaptation operations on the adaptable software system. We propose a set of adaptation operations that explicitly allows to change variable parts of the system on multiple devices, e.g. adding, removing or migrating system functionality from one device to another. The execution runtimes require further support that goes beyond the coordination of single adaptation operations if complex adaptations, that are comprised of multiple adaptation operations that affect several devices, are to be performed. Therefore, we also propose a protocol that describes the message exchange between the execution runtimes to coordinate not only the execution of a single operation but a set of operations performed on several devices. In addition to communication errors between execution runtimes due to unstable network conditions, adaptation operations may fail locally which would result in an invalid system configuration if not handled at run time. We investigate mechanisms and approaches to handle such error scenarios without having the entire set of adaptation operations be reverted in response, which would affect the system's performance adversely. Our findings are continuously incorporated and tested in our protocol to improve the reliability of executing complex adaptations in distributed and unstable environments.

[1] S. Malek, M. Mikic-Rakic, and N. Medvidovic, "A decentralized redeployment algorithm for improving the availability of distributed systems," Springer, 2005, pp. 99–114.
[2] D. Garlan, S.-W. Cheng, A.-C. Huang, B. Schmerl, and P. Steenkiste, "Rainbow: Architecture-based self-adaptation with reusable infrastructure," *Computer*, vol. 37, no. 10, pp. 46–54, 2004.
[3] C. W. Bachman and M. Daya, "The role concept in data models," 1977, pp. 464–476.

11.12 Decentralized Composition of Adaptive Systems

Markus Wutzler (markus.wutzler@tu-dresden.de)
Supervisor/s: Prof. Dr. rer. nat. habil. Dr. h. c. Alexander Schill

Composing distributed adaptive software systems at run time is a challenging topic in frequently changing environments like Smart Cities or Internets of Things. Such infrastructures consist of a large set of independent autonomous subsystems from different providers, but only a few subsystems might be involved in a composition. Centralized self-adaptive approaches maintain a global view on the system which is infeasible for large infrastructures. Distributed approaches still require some hierarchical infrastructure and restrict reconfiguration to changes on local or subordinate nodes. Existing self-organizing systems are independent of centralized instances but lack incorporating new functionality[1]. Our approach is based on the concept of roles[2] which clearly separates static from dynamic system parts, e.g. abstract functionality (roles) from their actual execution entities (players) which makes it an interesting concept for easing composition and reconfiguration of software systems[3]. Roles encapsulate functionalities which are utilized in collaboration with other roles. Players are restricted by specified requirements which can be anything from attributes over method interfaces to context features which can be utilized for discovery and selection. Roles are independent of concrete player types, i.e. different players providing the required interfaces can play that role.

We propose a middleware architecture for decentralized composition of adaptive software systems which provides (1) an infrastructure-independent discovery mechanism that enables (2) on-demand orchestration and (3) subsequent adaptation of distributed role-based software systems. Each autonomous subsystem equipped with our approach publishes its player and role information to an infrastructure abstraction layer which is responsible for communicating with other autonomous subsystems in the infrastructure. Role-based collaboration models are annotated with a respective triggering event and describe potential compositions. The event-consuming autonomous subsystem becomes a virtual master node in a fully decentralized infrastructure responsible for coordinating orchestration and subsequent adaptations of a single collaboration. Infrastructural knowledge is provided through role-based discovery mechanism. The focus of our work is on architectural principles, coordination mechanisms and distribution aspects. We evaluate our approach in terms of robustness against common failure scenarios, scalability and performance.

[1] G. Di Marzo Serugendo and J. Fitzgerald, "MetaSelf: an architecture and a development method for dependable self-* systems," in *SAC'10: Proceedings of the 2010 ACM Symposium on Applied Computing*, 2010.

[2] G. Boella and F. Steimann, "Roles and relationships in object-oriented programming, multiagent systems and ontologies," in *Object-Oriented Technology. ECOOP 2007 Workshop Reader*, Springer Berlin Heidelberg, 2007, pp. 108–122.

[3] A. W. Colman and J. Han, "Organizational roles and players," *Roles*, 2005.

12 RTG 1994: Adaptive Preparation of Information from Heterogeneous Sources (AIPHES)

Spokesperson: Prof. Dr. Iryna Gurevych, Presenter/PI: Prof. Dr. Chris Biemann
(gurevych@ukp.informatik.tu-darmstadt.de)
Technische Universität Darmstadt, Heidelberg University,
Heidelberg Institute for Theoretical Studies
https://www.aiphes.tu-darmstadt.de

AIPHES combines innovative computer science methods from computational linguistics, algorithmics, and machine learning in a challenging application domain. We focus on adaptive methods of genre- and domain-independent language analysis, including social media data. In contrast, current systems typically target either a single genre or a single domain and do not transfer to more complex scenarios. Most of the mainstream research is done on the English language; in contrast, we develop techniques to cope with German language. The research in intelligent writing assistance is conducted in close cooperation with users of the technology, initially in the areas of online journalism and online monitoring of heterogeneous information sources. Our text corpus is built from heterogeneous genres, domains, language styles, target audiences, and levels of quality, drawn from large-scale text sources from the web. Preparation of information means extracting, condensing, aggregating, and structuring the inherent information in a large text corpus in order to generate new texts from this information. This should enable the semi-automatic generation of a particular type of texts: multi-document summaries. Adaptive means concepts and methods are to be developed that are adaptable to new, unforeseen genres, domains, etc.

Both in academia and industry, there is a high demand for scientists with a comprehensive expertise in the intersection of computer science, computational linguistics, and information management. Our mission is to assist bright, promising academics in an early career step into this vibrant field, where they conduct and accomplish their first own major research project. We want all of our PhD students grow to mature personalities, who have learned to pursue their research interests autonomously, but also collaboratively. Currently AIPHES comprises 8 Principal Investigators, 7 Associated Researchers and 11 PhD students. AIPHES cooperates with leading international researchers in all relevant research areas.

12.1 Enhanced Motif Analysis of Text-Based Graphs

Thomas Arnold (arnold@aiphes.tu-darmstadt.de)
Supervisor/s: Dr. Karsten Weihe

Graph- or network-based approaches have been successfully applied in many different computer science disciplines. Prominent examples are text mining algorithms[1] or image segmentation approaches[2]. Recently, the application of graph-based methods to analyze text based data has been discovered to be very promising. In particular, the analysis of recurrent sub-structures, or motifs, in these graphs has led to very interesting insights about textual data[3]. As part of the AIPHES research group, I want to show the possibilities of motif analysis on text induced graphs and explore more complex motif structures. The following research questions form the core of my doctoral research:

1. Can text-based motifs predict the quality labels of Wikipedia articles?
2. How can we expand motif analysis to more complex motif and graph structures?
3. Can we use the extended motif analysis, in cooperation with other AIPHES guiding themes, on different data sets that are focused on the core topics of this research group?

Wikipedia is a large source of free, textual data. The Wikipedia community can assign the quality labels "featured" or "good" to articles that fulfil specific quality criteria. As a first step of using motif based approaches on textual data, I apply motif analysis to graphs created from German Wikipedia articles and try to predict these quality labels based on motif signatures. Further, I will adapt my approach to another application, like the identification of hoax articles.

Current motif analysis concentrates on very specific types of motifs, like connected subgraphs with a certain number of nodes. I want to extend the concept of graph motifs by exploring more complex graph structures. This provides access to completely new types of motifs, including hierarchical structured or temporal motifs. These new approaches form a central part of my methodical research.

To tackle the main topics of the AIPHES research group, the newly developed methods should be combined with the progress of other doctoral researchers. This way, I hope to improve the state of the art in a core question of AIPHES.

[1] T. Washio and H. Motoda, "State of the art of graph-based data mining," *SIGKDD Explor. Newsl.*, vol. 5, no. 1, pp. 59–68, Jul. 2003.
[2] P. F. Felzenszwalb and D. P. Huttenlocher, "Efficient graph-based image segmentation," *International Journal of Computer Vision*, vol. 59, no. 2, pp. 167–181, 2004.
[3] C. Biemann, S. Roos, and K. Weihe, "Quantifying semantics using complex network analysis," in *Proceedings of COLING*, 2012, pp. 263–278.

12.2 Structured Summaries of Complex Contents

Tobias Falke (falke@aiphes.tu-darmstadt.de)
Supervisor/s: Prof. Dr. Iryna Gurevych, Dr. Christian M. Meyer

The amount of electronically available texts is growing constantly, making information overload a common challenge. One example is the work of an investigative journalist who has a large collection of documents, e.g. from WikiLeaks, but cannot read them all manually to find something worth an article. The challenge faced in this situations is known as exploratory search. In these scenarios, people are not looking for specific facts but rather want to explore a whole document collection[1].

A common tool for this task is a navigation structure, which is a graph with nodes representing specific information units from the collection and edges indicating the relationships among them. Using it, one can easily get an overview of a document collection and navigate to topics of interest. In this way, a navigation structure can be used to explore a large document collection and thereby serves both as a navigation tool and as a special type of summary.

A review of existing requirement studies indicated that users are interested in a variety of different information units in a text, such as relevant persons, topics, facts and events, and the connections between them[2]. State-of-the-art approaches to generate navigation structures create static structures that only contain either generic information units such as frequent nouns or concentrate on named entities or abstract topics. The requirements gathered in the user studies are not fully met.

We believe that navigation structures that are interactive, tailored to the user and covering a broader range of different information units from a text can bridge the gap between existing approaches and actual user requirements and thus better support exploratory search in document collections. Hence, this doctoral project aims at improving the state of the art in several ways:

First, the type and range of information covered in an automatically constructed navigation structure should be extended using semantic representations derived by parsers as an input[3]. Second, feedback gathered from the user should be integrated into the creation of the structure with the goal to adapt the structure to best support the user's information needs. Machine learning techniques such as incremental and reinforcement learning will be investigated for this purpose. The enhancements will be implemented in a prototype and evaluated in user studies.

[1] G. Marchionini, "Exploratory Search," *Communications of the ACM*, vol. 49, no. 4, pp. 41–46, 2006.
[2] G. Chin, O. A. Kuchar, and K. E. Wolf, "Exploring the analytical processes of intelligence analysts," in *CHI 2009 - digital life, new world*, 2009, pp. 11–20.
[3] L. Schubert, "Semantic Representation," in *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence*, 2015, pp. 4132–4138.

12.3 Computational Fact checking - Detection and Verification of Facts from Online Articles

Chinnappa Guggilla (guggilla@aiphes.tu-darmstadt.de)
Supervisor/s: Prof. Dr. Iryna Gurevych, Prof. Dr. Manfred Stede

Online fact-checking has become a recent trend in journalism community. Public figures such as politicians, actors, organizations make claims about facts all the time. These claims could be often false, misleading and exaggerated. Due to these reasons, information which is published in online or offline articles may not be fully correct and is unreliable. As technology and social-media disseminating information to mass audiences through all types of channels, there is a burden posed on the readers to assess the truthfulness of statements from large collection of articles which they consume.

Currently, in news organizations, before publishing articles, journalists and fact-checkers perform manual fact verification by hand-picking most popular claims related to certain situational events. Fact checkers identify reliable sources manually from online and then analyse, consolidate information from multiple sources. More importantly providing reasonable interpretations from multiple evidence sources for a given claim is not a trivial task for the journalists. This traditional way of fact checking is time consuming and laborious process and cannot keep up with the enormous volume of information that is generated online.

Recently, automated fact verification task is attempted by various Artificial Intelligence researchers[1] using external structured knowledge sources like Wikipedia, knowledge graphs but these approaches deal with only simple statements and do not provide meaningful explanations. Some approaches[2] solve fact-checking by identifying check-worthy statements and do not exploit heterogeneous textual evidences for drawing conclusions. We propose a novel, generalized and scalable NLP, IR and ML based fact checking approach which can effectively leverages online information sources and knowledge bases. The proposed approach firstly, identifies various types of check-worthy factuality statements from the given articles. Then for these check-worthy statements, retrieves relevant evidential sources through web search engines and Question Answering systems, and matches potential statements with retrieved evidences and knowledge bases and then finally provides factuality verdict and conclusions in the form of summarized evidence using textual reasoning. The proposed fact-checking approach can be adapted to multiple online discourses such as political debates, social media, news and medical.

[1] G. L. Ciampaglia, P. Shiralkar, L. M. Rocha, J. Bollen, F. Menczer, and A. Flammini, "Computational fact checking from knowledge networks," *PloS one*, vol. 10, no. 6, p. e0128193, 2015.

[2] N. Hassan, C. Li, and M. Tremayne, "Detecting check-worthy factual claims in presidential debates," pp. 1835–1838, 2015.

12.4 Entity Linking

Benjamin Heinzerling (benjamin.heinzerling@h-its.org)
Supervisor/s: Michael Strube

When given a text, computers do not have any conception of the things mentioned in it. This leads to confusion when different things are referred to in the same way. For example, *Obama* can, among others, refer to the current U.S. president or a town in Japan. Furthermore, a given entity can be referred to in various ways. For example, *the current U.S. president*, *Barack Hussein Obama*, and *the 44th U.S. president* all refer to the same person. Entity linking tackles this problem by automatically identifying mentions of **entities**, such as persons, organizations, or locations, and **linking** those mentions to their corresponding entries in a knowledge base. The knowledge base provides rich, computer-readable information about these entities, which can then be used in downstream NLP applications such as search, question answering, or automatic summarization.

Entity linking comprises the subtasks of discovering mentions of entities and the actual linking to a knowledge base. Additionally, systems also need to recognize if an entity mentioned in a text is not contained in the knowledge base, and cluster all mentions of that entity across documents in the test corpus.

Commonly, these substask are either performed using a pipeline of components that are applied in a fixed order, or by modelling multiple subtasks jointly. Pipelines are simple and fast, but suffer from error propagation and the fact that information learned at a later stage cannot be used by earlier stages. Joint approaches are more complex and slower, but allow for sharing of information between subtasks[1].

Aiming to get the best of both worlds, I created a hybrid system[2] that first takes easy decisions in a pipeline-like fashion, but allows for interaction between earlier and later stages by repeatedly running some of the components. The harder problems still left are then solved by an existing global, joint inference system[3], which now can benefit from additional information and a much smaller search space, since the easier problems have already been solved by the pipeline-like components.

In the remainder of my PhD, I will explore information- and game-theoretic approaches to find optimal decision sequences that maximally exploit information gained from earlier decisions while maximizing expected information gain for future decisions.

[1] T. Marciniak and M. Strube, "Beyond the pipeline: Discrete optimization in NLP," in *Proceedings of the ninth conference on computational natural language learning (CoNLL-2005)*, 2005, pp. 136–143.

[2] B. Heinzerling, A. Judea, and M. Strube, "HITS at TAC KBP 2015: Entity discovery and linking, and event nugget detection." in *Proceedings of the text analysis conference*, 2015, to appear.

[3] A. Judea, B. Heinzerling, A. Fahrni, and M. Strube, "HITS' monolingual and cross-lingual entity linking system at TAC 2014," in *Proceedings of the text analysis conference*, 2014.

12.5 Data-driven paraphrasing and stylistic harmonization

Gerold Hintz (hintz@aiphes.tu-darmstadt.de)
Supervisor/s: Prof. Dr. Chris Biemann

Paraphrasing methods recognize, generate, or extract units of natural language text that are semantically equivalent. In the scope of my PhD thesis, we investigate unsupervised, data-driven methods for each of these subtasks. In the context of AIPHES, a primary use-case will be their application to multi-document summarization (MDS). Determining if two text units are paraphrases of each other, as well as generating a paraphrase for a given phrase, are essential for downstream tasks; i.e. by providing a similarity measure between sentences, summarization can be performed by minimizing redundancy between extracted sentences. To approach this goal, we investigate the following research questions: How can lexical substitution, a simplified single-word paraphrasing task, be solved without linguistic knowledge? What is the remaining gap from single-word substitution to a full paraphrasing system? How can paraphrasing be leveraged to improve semantic textual similarity? We further propose the notion of stylistic harmonization, which utilizes paraphrasing to the sentences with different linguistic style, and investigate how harmonization can be used to improve MDS. One of the key challenges is bridging the lexical gap; i.e. in absence of lexical overlap between a pair of text segments, judging their semantic content with respect to semantic similarity, entailment, or equivalence. To scale to the requirements of multi-domain content, and being language-independent, we are interested in knowledge-free, unsupervised methods for these tasks. As a preliminary stage to full paraphrasing, we address lexical substitution, the prediction of substitutes for a target word instance within a sentence context. A large variety of supervised[1] and unsupervised[2] approaches have been proposed. In a first work, it was shown that an existing supervised approach for English lexical substitution[3] could be extended with state-of-the-art embedding features[4] and adopted to German[5]. Ongoing work includes leveraging data-driven methods to move towards unsupervised lexical substitution, as well as methods for paraphrase extraction from structured corpora.

[1] C. Biemann, "Creating a system for lexical substitutions from scratch using crowdsourcing," *Language Resources and Evaluation*, vol. 47, no. 1, pp. 97–122, 2013.

[2] O. Melamud, I. Dagan, and J. Goldberger, "Modeling word meaning in context with substitute vectors," in *Proceedings of the 2015 conference of the north american chapter of the association for computational linguistics*, 2015.

[3] G. Szarvas, C. Biemann, I. Gurevych, and others, "Supervised all-words lexical substitution using delexicalized features." in *Proceedings of the 2013 conference of the north american chapter of the association for computational linguistics: Human language technologies*, 2013, pp. 1131–1141.

[4] O. Melamud, O. Levy, I. Dagan, and I. Ramat-Gan, "A simple word embedding model for lexical substitution," *VSM Workshop*, Denver, USA, 2015.

[5] G. Hintz and C. Biemann, "Delexicalized supervised German lexical substitution," in *Proceedings of GermEval 2015: LexSub*, 2015, pp. 11–16.

12.6 Contextual meaning and semantic compositionality for opinion summarization

Ana Marasovic (marasovic@cl.uni-heidelberg.de)
Supervisor/s: Prof. Dr. Anette Frank

Opinion summarisation is the task of producing the summary of a single document or multiple documents, which highlights different perspectives and opinions about specific contents, or the pros and cons of a situation. It is thus a trade-off between summarization and sentiment analysis. To generate a good opinionated summary from multiple documents from different domains it is necessary to improve current sentiment analysis systems.

Sentiment analysis found application in various domains, so it is not surprising how broad research around it is. However, there are are still several challenges in automatic detection and categorisation of attitudes in text that we think are crucial for generating a good opinionated summary. Some of them that we are especially interested to are:

- *Modifiers of sentiment:* Well known modifiers of sentiment are negation and modals, e.g. *may be good* and *was not good*. We want to investigate other modifiers and compare the differences in English and German.
- *Scope:* Sentiment often changes depending on what the target, e.g. in following example author has positive attitude towards pictures during the daytime and negative at night: "Very poor picture quality at night".
- *Implicit sentiment:* Attitudes are often not explicitly stated. For example in following sentence it is implicitly said that the software is good. "The camera is actually quite good for outdoors because of the software."

Since much of the research and resource development in sentiment analysis has been on English texts, additional challenge is moving from English to German texts.

Besides restricting sentiment, modality plays other significant roles in detection and categorisation of attitudes. For example, in following sentence *should* has deontic sense and consequently we can deduce that it is author's personal wish that president insure that the sums are recovered and that it is not a fact: "President should insure that we recover the sums involved."

To summarise, in my thesis I aim to extract relevant aspects of meaning for the opinion summarisation that relate to modality, factivity and sentiment. To improve on prior approaches, I will model semantic compositionality at the level of propositions and discourse, using tensor factorisation and deep learning methods

12.7 Deep Learning embeddings for adaptive language processing

Teresa Martin (martin@aiphes.tu-darmstadt.de)
Supervisor/s: Prof. Dr. Iryna Gurevych

My PhD-project is approaching the task of semantic role labelling (SRL) by using methods of Deep Learning (DL) to learn embeddings jointly from unstructured text and from knowledge bases (KBs). SRL is a challenging task in Natural Language Processing (NLP): the aim is to annotate entities and actions connecting them; SRL answers the question of 'Who does what to whom?'. For the German language state-of-art models for SRL need to be improved, especially regarding domain- and genre-adaptation. DL provides the community with methods based on multi-layer neural networks that are able to learn complex prediction and classification tasks. Crucially, expensive hand-crafting of features is avoided by learning features within the process. For the domain of NLP, an example of such automatically learned features are embeddings. These are low-dimensional vector representations that capture both semantic and syntactic structure of words in a common embedding space. Such embeddings can be learned either from unlabelled text data (e.g., Wikipedia) or from KBs (e.g., WordNet). Work on learning embeddings from text data in an unsupervised way is presented in[1]. These embeddings can in turn be used for NLP-tasks as e.g., part-of-speech-tagging or named entity recognition. Regarding these tasks, we performed experiments with the SENNA-architecture[2], verifying that not only for English but also for German data this unified approach is able to reach nearly state-of-art results. Work on learning embeddings jointly from unstructured text and from KBs is presented in[3] for a task closer to but still simpler than SRL: relation extraction (RE). To this end, a different way of looking at embeddings, namely not embeddings for words which are single entities but embeddings for entity-pairs, is presented in[4]. Following this line, KBs could be enriched when texts are aligned with it[5]. Currently, we work on extending these models and plan to integrate the German language into them and to use them for SRL.

[1] T. Mikolov, K. Chen, G. Corrado, and J. Dean, "Efficient estimation of word representations in vector space," *arXiv preprint arXiv:1301.3781*, 2013.

[2] R. Collobert, J. Weston, L. Bottou, M. Karlen, K. Kavukcuoglu, and P. Kuksa, "Natural language processing (almost) from scratch," *The Journal of Machine Learning Research*, vol. 12, pp. 2493–2537, 2011.

[3] J. Weston, A. Bordes, O. Yakhnenko, and N. Usunier, "Connecting language and knowledge bases with embedding models for relation extraction," *arXiv preprint arXiv:1307.7973*, 2013.

[4] S. Riedel, L. Yao, B. M. Marlin, and A. McCallum, "Relation extraction with matrix factorization and universal schemas," in *Joint human language technology conference/Annual meeting of the north american chapter of the association for computational linguistics (HLT-NAACL'13)*, 2013.

[5] P. Verga, D. Belanger, E. Strubell, B. Roth, and A. McCallum, "Multilingual relation extraction using compositional universal schema," *arXiv preprint arXiv:1511.06396*, 2015.

12.8 Representation Learning for Heterogeneous Multi-Document Summarization

Maxime Peyrard (peyrard@aiphes.tu-darmstadt.de)
Supervisor/s: Dr. Judith Eckle-Kohler, Prof. Dr. Iryna Gurevych

Multi-Document Summarization (MDS) has been studied in great depth for the particular variant of extractive and generic MDS in the news domain. Real life applications of summarization would benefit from the ability to summarize content from various type of sources accross various domains. However there is a lack of works that study summarization in this set-up. In this thesis we aim to propose a general framework for adapting extractive summarization to the heterogeneous MDS. We will organise the thesis in three work packages (WP):

We first observe that recent works in MDS have achieved major improvements by relying on budgeted subset selection techniques[1]. In the first WP, we will motivate a general framework for summarization that splits the task into sentence scoring and sentence selection. By proposing a mathematically principled sentence selection procedure, the problem of extractive summarization simplifies to the problem of sentence scoring. Assumptions about dataset and other domain-specific features are moved into the Machine Learning component that scores sentences.

In order to address the lack of datasets for heterogeneous summarization, two new datasets will be collected and analysed in the second WP. One will be crawled from online news live-blogs (a news summarization task from heterogeneous source). The other dataset will be constructed based on Wikipedia. It will consist of both heterogeneous sources and heterogeneous domains. In this WP, we hope to gain insights on the heterogeneous set-up and understand its specificities.

The final WP will use the previous framework to tackle the problem of hetergoeneous MDS by investigating how to score sentences in the new set-up. We plan to build upon recent progress in representation learning[2] and domain adaptation[3] in order to develop Machine Learning methods that can adapt across domains and text types

[1] R. McDonald, "A study of global inference algorithms in multi-document summarization," in *Proceedings of the 29th european conference on IR research*, 2007, pp. 557–564.

[2] Y. Bengio, A. Courville, and P. Vincent, "Unsupervised feature learning and deep learning: A review and new perspectives," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 35, no. 8, pp. 1798–1828, 2013.

[3] A. Søgaard, *Semi-supervised learning and domain adaptation in natural language processing*. Morgan & Claypool Publishers, 2013.

12.9 Computer Assisted Multi-document Summarization and Evaluation

Avinesh PVS (avinesh@aiphes.tu-darmstadt.de)
Supervisor/s: Dr. Christian M. Meyer, Prof. Dr. Iryna Gurevych

For the past couple of decades there has been intensive work in the area of automatic summarization, but unfortunately the quality of the resulting summaries is still of low quality[1]. In view of this problem, we propose a computer-assisted summarization (CAS) framework incorporating user feedback as an alternative to existing fully automatic summarization systems. CAS systems have the potential to produce high-quality human-like summaries, as they allow the user to post-edit an automatic summary draft according to their requirements.

The concept of CAS is inspired by computer-assisted translation initially proposed by Martin Kay[2], where an amalgamation of human and system has been found to give better results compared to a fully automatic system. In CAS, the previous approaches[3] relied on document exploration and relevance assessment and presented important elements of the source document(s) to a user. Such approaches use post editing just as an assistance to the user during the final stage of summary creation. As they do not capture the user interactions, they, however, cannot learn how humans process the source document(s) and work out the corresponding summary.

We propose a novel methodology by capitalizing on the recent advances in machine learning, particularly in the area of online learning and deep reinforcement learning. The resulting approach will enable the exploitation of the user feedback in a novel summarization framework. The proposed method can also be used in multiple other scenarios namely (a) as an intelligent annotation tool, which highlights important sentences for the human annotators based on their interaction with the system; (b) as a journalistic writing aid, which presents important content from multiple source feeds (e.g., live blogs); (c) as an essay writing system for language learners learning to write comprehensive essays on a topic from multiple sources (e.g., as a training for the TOEFL integrated test). The mentioned scenarios have a common phenomenon of constant user interaction, which has not been used for learning in a CAS environment before. Our proposed approach will exploit this phenomenon and learn through constant user interaction.

[1] P. Over, H. Dang, and D. Harman, "DUC in context," *Inf. Process. Manage.*, vol. 43, no. 6, pp. 1506–1520, Nov. 2007.

[2] M. Kay, "The proper place of men and machines in language translation." *Machine Translation*, vol. 12, no. 1-2, pp. 3–23, Jan. 2007.

[3] C. Orasan and L. Hasler, "Computer-aided summarisation: What the user really wants," *Proceedings of the 5th International Conference on Language Resources and Evaluation (LREC2006)*, pp. 1548–1551, 2006.

12.10 Methods for contextual and constraint-based ranking

Markus Zopf (zopf@aiphes.tu-darmstadt.de)
Supervisor/s: Prof. Dr. Johannes Fürnkranz

Ranking approaches try to order objects according to some quality criteria. We encounter ranking approaches in everyday life by using web search engines, collaborative filtering, or news recommendations where millions of web sites, shopping items or news articles are ranked and presented to end-users to satisfy their information needs. Ranking approaches are also a key element in various applications in natural language processing like machine translation and document summarization[1].

Our first focus in AIPHES is to develop new ranking approaches for extractive document summarization of heterogeneous multi-document collections. Automatic document summarization aims to summarize a collection of documents by creating a short text, provides the most important information in a condensed form[2]. The user, for example an online journalist, can then get an overview about large text collections very efficiently. Ranking approaches are used in automatic summarization to find the most relevant information in texts by ranking sentences according to their relevance. However, finding the most relevant information is not enough: since the source documents may contain the same information multiple times it is important to consider already ranked sentences in subsequent ranking decisions. We will focus in our research on contextual ranking algorithms which are aware of a context in which they create rankings.

Heterogeneous documents cover different domains, genres, languages, and target audiences. Since the vast majority of research in automatic document summarization has been done on well-written English news articles there is great demand to investigate which challenges come along with heterogeneity in the source documents. Therefore, we intent to develop contextual ranking approaches, which will be able to handle these difficult conditions.

A second target of our research is to develop ranking techniques that are able to combine multiple local rankings to an overall ranking. We aim to develop rank aggregation methods, which are able to combine rankings at different levels of a language processing chain, like named entity recognition or at a semantic level where different possible meanings of a word have to be ranked, and combine the expertise of these separated ranking approaches to a superior joint solution.

In conclusion, our research focus is to develop new contextual ranking approaches for rank creation and rank aggregation, which will be useful in many tasks in natural language processing and information retrieval tasks.

[1] H. Li, "Learning to rank for information retrieval and natural language processing," *Synthesis Lectures on Human Language Technologies*, vol. 7, no. 3, pp. 1–121, 2014.

[2] A. Nenkova and K. McKeown, "Automatic summarization," *Foundations and Trends in Information Retrieval*, vol. 5, no. 2-3, pp. 103–233, 2011.

13 RTG 2050: Privacy and Trust for Mobile Users

Prof. Dr. Max Mühlhäuser (max@informatik.tu-darmstadt.de)
Technische Universität Darmstadt
https://www.privacy-trust.tu-darmstadt.de

Mobile information and communication technology has become virtually ubiquitous due to the proliferation of smartphones and tablet computers; large sections of the society use it to their advantage. In reference to the relationship *users-network*, public debates highlight the increasing transparency of users - in the sense of a surveilled society - while the network is deemed to be increasingly nontransparent, i.e. inscrutable. The Research Training Group (RTG) 2050 implements major contributions in reversing this trend: it will enable better privacy protection for users and better transparency, i.e. assessability of the network. *Privacy protection* shall be customizable to personal interests yet manageable by the lay person; privacy-opposing economic or societal interests shall be better reconciled. With regard to *network transparency*, the RTG will investigate *trustworthiness assessment*: the empowerment of users to sufficiently understand the networked entities surrounding them; most importantly, they shall be able to assess, by sound measures, the expected outcome and quality of a service or system they consider using - including potential risks. Coordinated research into the pair *privacy protection* - *trustworthiness assessment* suggests itself for two reasons: firstly, it corresponds to the ubiquitous pairing *user-network*; secondly, the expected research results will have transparency-reducing and transparency-increasing effects, respectively. A conflict of objectives arises, at the latest, when users double as service providers in the net.

For centuries, privacy and trust have been relevant subjects for society. Hence, an *interdisciplinary approach* is compelling. Consequently, researchers from computer science collaborate in interdisciplinary projects with those from the fields of law, economics, sociology, and usability research.

As an important *technological vision*, the RTG will conduct research into novel mobile devices that enable maximum control for the user. They represent their user to the digital network, govern privacy protection and trust assessment, negotiate between user and service provider, and command ad hoc networking. Novel approaches for such personal devices, for networked IT services, for social networks, and for sensor-based environments will be investigated.

13.1 A.1 Quantifying Indistinguishability in Databases

Spyros Boukoros (boukoros@seceng.informatik.tu-darmstadt.de)
Supervisor/s: Stefan Katzenbeisser

Privacy has many definitions and quantifying it is challenging. Even though privacy in statistical databases is a well studied field, recent attacks[1] have shown that it is still of grave importance. In my research, in A1 area which recently started, we investigate how privacy is defined in the context of genomic datasets, recommender systems, and social networks and we attempt to quantify and measure how private someone is. We base our definition of privacy on the one given by C. Dwork[2] which, we restate as: *one's risk of privacy breach should not substantial increase as a result of participating in a database.* We propose a mechanism that estimates how the privacy of a database is affected by the existence of an individual entry. Input to our mechanism will be a query and a database or a distribution of a variable with specified parameters. The distribution can either be given by the user or calculated on a provided dataset. We assume that we have a user, Alice, whose data are stored in a database. We want to estimate how easily one can identify Alice given that he has either access to a sanitized version of the database or to some released statistics of that database. We compare the results of a query or an algorithm applied on that user, with the results applied on a randomly selected one. By repeating this procedure many times, we are able to create a distribution of results for the randomly selected user, which we argue converges to the *average user*, for that dataset. As a last step, we compare the results with those for the specific user, using various metrics and we decide on the level of privacy offered. We expect the privacy preserving entries in our database to be similar to the average entry. By 'being hidden in the crowd', an adversary cannot infer something with high confidence, hence one remains private. The domains in which we are interested vary, and so do their definitions of privacy. For example, at the recommender systems the whole output of the recommendation engine gives us information about an individual while on the genomic databases, some, very specific, biomarkers. By giving privacy metrics for each one of the aforementioned domains and then abstracting them, we will be able to create a generic tool that gives results on any kind of database. Privacy on databases remains a challenging topic even though is well studied. There are no metrics for the privacy of individuals entries or for the whole dataset mainly because of the data semantics and in this work we aim to tackle this problem.

[1] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *Security and privacy, 2008. SP 2008. IEEE symposium on*, 2008, pp. 111–125.

[2] C. Dwork, "Differential privacy," in *Encyclopedia of cryptography and security*, Springer, 2011, pp. 338–340.

13.2 A.2 Uncertain risk representations and the disclosure of private information: A Bayesian approach towards understanding user behavior

Tim Schürmann (schuermann@privacy-trust.tu-darmstadt.de)
Supervisor/s: Joachim Vogt

Using either social networks or consumer-oriented service networks, there are risks involved at the side of the user. Where social networks analyze user likes and dislikes to specify news output and friend suggestions, service networks analyze consumer shopping history and preferences to identify product demand or individualize marketing practices. Depending on the nature of information gathered, the user runs the risk of their privacy being violated to a degree they are not comfortable with. Yet, while many users claim that their private information and its security is important to them, in the recent years research claims to have identified a gap between users' stated privacy concerns and their disclosure behavior: the privacy paradox[1]. Estimations of complex user decision processes in the area of privacy-related interactions regularly employ an approach named privacy calculus, which uses structural equation modeling or other forms of the Generalized Linear Model to replicate user information integration. Despite its focus on beliefs about the occurrence of uncertain events and the updating of said beliefs in light of new evidence, the cyber security literature has not yet employed a paradigm gathering attention in psychology and cognitive science that seems fairly suited for the task: Bayesian cognitive modeling.

By probabilistically combining prior knowledge about hypotheses and the likelihood of available data under the assumption that a given hypothesis is true through Baye's rule[2], literature suggests that subject decisions and beliefs should correlate well with posterior estimations of such models. Applying both naive and well-informed versions of such a cognitive model, I aim to evaluate how and to which degree user sensitization interventions sharpen users' views on privacy-related risks and benefits. The correlation between the model output of disclosure intention and actual subject behavior before and after an intervention will indicate whether or not Bayesian cognitive models provide a better statistical fit than the current privacy calculus models. Additionally, it will show if the interventions designed here prove effective to sharpen users' decision making.

[1] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of Consumer Affairs*, vol. 41, no. 1, pp. 100–126, 2007.

[2] A. Perfors, J. B. Tenenbaum, T. L. Griffiths, and F. Xu, "A tutorial introduction to bayesian models of cognitive development," *Cognition*, vol. 120, no. 3, pp. 302–321, Probabilistic models of cognitive development, 2011.

13.3 A.3 An economic perspective on privacy and trust

Nora Wessels (Wessels@is.tu-darmstadt.de)
Supervisor/s: Peter Buxmann

Since the NSA surveillance scandal and the recent unmasking of the PRISM program the protection of privacy has become an area of interest in public. More and more internet users develop concerns about the usage of web services which leads to a decline of trust in the service providers. This decrease of trust is a problem for the companies because within their current business models they have to deal with a tension between the necessity of collecting personal information about their users on the one side and on the other side the companies have to foster trust enhancement among their customers in order to gain a high number of users. Therefore companies have to be creative in finding new ways to strengthen the customers' trust in their company again and stay profitable. In order to do so and to face this trade-off a modification of the existing internet business models can be useful. Especially because the current research in the area of trust and privacy mainly focuses on the perspective of the users. Only little research has yet be done on the economic perspective. For example, Bélanger and Crossler (2011)[1] as well as Smith et al. (2011)[2] identified this research gap within their literature review.

According to that, research in this sector aims at finding a way to monetarize the customer's wants of privacy and trust for the companies. Therefore, the main objective is the development of new, economic successful and customer-friendly business models with respect of the users' requirements on privacy and trust. In order to reach this main goal, the fulfillment of the three following sub goals would be useful:

1. First, an exploration of the current user data and privacy management status in companies is planned, in order to investigate, if the companies already preserve privacy and foster trust enhancement. As the performance of case studies is an effective method for analyzing the current state of data, about ten cases with interviews are planned.
2. Second, an analysis of the handling of user data and its effect on business success is intended. In order to assess the success of an optimal management of privacy and business model, investigations on the effect of the service adoption and users' willingness of information disclosure because of changes in privacy politics, is important. Therefore, experimental studies will be conducted.
3. Finally, a classification of the current business models would be useful in order to derive success factors for privacy and trust preserving internet business models.

[1] F. Belanger and R. E. Crossler, "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quarterly*, vol. 35, no. 4, pp. 1017–1042, 2011.

[2] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: An interdisciplinary review," *MIS Quarterly*, vol. 35, no. 4, pp. 989–1015, 2011.

13.4 B.1 Socio-technical processes and Institutional Design of Digital Trust Infrastructures

Markus Uhlmann (markus.uhlmann@uni-kassel.de)
Supervisor/s: Jörn Lamla

Since at least the so-called "Snowden-revelations" one can assume a crisis of trust regarding the constitution of digital infrastructures. This widely discussed crisis relates to complex trust relations among various actors like states, internet organizations as well as users of digital infrastructures. Given that challenges of trust in the digital world are often discussed with regard to objections of privacy also the contested status of privacy is revealed when trust seems to disappear[1]. However, the various challenges that are related to privacy and trust have not led to digital abstinence. On the contrary, in connection with the huge popularity of Online Social Network Sites (OSNs) we have to deal with the fact that digital mediated practices have already become a relevant component of our daily lives[2]. Therefore, it becomes clear why studying privacy and trust in the context of OSNs is related to inherently ambivalent issues. On the one hand, OSNs promote possibilities for the constitution of new forms of privacy and trust in digital environments. On the other hand, with respect to inappropriate usage of user data through state organizations or service providers of OSNs, there is no doubt that OSNs generate a lot of novel challenges concerning privacy and trust[3].

From this perspective, the doctoral thesis deals with complex socio-technical dynamics of privacy and trust that take part in the context of OSNs. Understanding privacy and trust as being part of a larger socio-technical system, the thesis aims to advance sociological insights concerning the constitution of complex digital trust infrastructures. In this context, the doctoral thesis raises three main questions: Firstly, what is the role of various forms of privacy for the constitution of trust in OSNs? Secondly, what are the various implications of trust building in OSNs for privacy? Thirdly, which technological, legal, cultural and political trust elements can be mobilized with regard to build appropriate trust infrastructures that address the various challenges of privacy and trust? Furthermore, by developing a holistic approach of privacy and trust and contrasting OSNs with other domains and socio-technical infrastructures, the research project aims to advance the interdisciplinary dialog on building digital trust infrastructures.

[1] A. E. Waldman, "Privacy as trust: Sharing personal information in a networked world," *University of Miami Law Review*, vol. 69, no. 3, pp. 559–630, 2015.
[2] A. E. Marwick and D. Boyd, "Networked privacy: How teenagers negotiate context in social media," *New Media & Society*, vol. 16, no. 7, pp. 1051–1067, 2014.
[3] S. Gürses and C. Diaz, "Two tales of privacy in online social networks," *IEEE Security Privacy*, vol. 11, no. 3, pp. 29–37, May 2013.

13.5 B.2 Empowering Users in OSN-based Communications

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

More and more people use online social networks (OSNs) for group communication. Many OSNs, e.g., Facebook, include functionality to connect people in their services. As such, OSNs gain importance in the daily activities of everybody.

Nonetheless, as todays' OSNs are *centralised*, i.e., all servers controlled by the service provider itself, all data is in the service providers' hand. As such, the service provider has full control over the content and the meta-data of the communication.

The service provider can combine data to infer *new* data, without consent and knowledge of the user. Moreover, as the data solely resides with the service provider, the service provider is the ideal point of entry for surveillance by state agencies.

Current approaches in the field of privacy-preserving communication aim to hide the content of the communication, but lack protection of meta-data against powerful attackers like state agencies[1]. Moreover, they lack on efficiency.

Within subproject B.2 of RTG 2050, I focus on empowering the user in the relationship to the service provider, that is, I want to give the control of the users' data back to the owner of the data. Hereby, all before mentioned problems are addressed, i) service provider and user process data only in consent and ii) no single point of data access. Therefore, the three following research problems have to be addressed.

a) User controlled data access: To establish a data control shared among service provider and user, I want to provide techniques for distributed anonymous communication. These techniques are able to be interweaved with features and functionalities of current OSNs and form a hybrid OSN. Prior work for anonymous communication[2] is planned to be extended to enable its usage in such a hybrid solution. The anonymous communication has to be efficient without unnecessary message overhead, which is a problem in P2P-networks without shareable knowledge. Moreover, the anonymous communication has to cope with standard user behaviour, e.g., user churn.

b) Users' privacy awareness: To exploit the ability to communicate anonymously, the user has to know her actual privacy state. Therefore, I want to develop means to quantify users' privacy, based on their communication network.

c) Privacy-preserving data access: A service provider has to have a functional business model to provide a service; therefore, I want to develop a system to hand data to the service provider without harming the users' privacy. Exemplary solution approaches may include in-network aggregation to hide the users in a considerable crowd.

[1] A. Shikfa, M. Önen, and R. Molva, "Privacy and confidentiality in context-based and epidemic forwarding," *Computer Communications*, vol. 33, no. 13, pp. 1493–1504, 2010.

[2] J. Daubert, M. Fischer, T. Grube, S. Schiffner, P. Kikiras, and M. Mühlhäuser, "AnonPubSub: Anonymous publish-subscribe overlays," *Computer Communications*, vol. 76, pp. 42–53, 2016.

13.6 B.3 The Interplay between Social and Economic Capital - New Insights from Online Social Networks

Michael Weiler (weiler@emarkets.tu-darmstadt.de)
Supervisor/s: Oliver Hinz

The proliferation and increasing usage of online social network sites (OSNs) and the therewith-affiliated availability of vast amounts of digital data allows the examination of the emergence of social capital and the influence of social capital on dependent variables such as educational outcomes. As a result, huge amounts of data that resemble social behavior and human interaction are just a few clicks away[1]. That implies new chances to promote empirical analyses and stimulates new research opportunities for the relationship between OSNs and social capital. My PhD-research aims at contributions in two areas: (a) new insights into the operationalization and measurement of social capital, and (b) which economic benefits can be assessed through the usage of OSNs. In order to achieve this, three working packages are planned:

1. Literature review: Up to now, there is no consensus in the literature on how to measure social capital. Thus, I will conduct a review with the focus to give an overview and synthesis of all quantitative studies from top-ranked economic and sociological journals between 2005 to 2015 that propose an operationalization of social capital.
2. Proxy validation: The ready availability of observational data from OSNs raises the question: Is this data source a valid proxy for offline personal networks when explaining social behavior? To answer this question, I will compare data gathered from OSNs to offline contact networks to estimate the overlapping degree between those two distinct data sources. I will collect the offline network data by applying the contact diaries method[2]. The corresponding observational data will be crawled by asking the participants that keep the diary to provide access to their OSN data.
3. Benefit estimation and impact: Here, I will take advantage of the findings from the previous work packages and focus on whether the usage of (work-related) OSNs generate a measureable benefit in terms of economic capital. The envisaged study adds to the body of research by conducting an empirical assessment of how the usage of OSNs affect social capital and concurrently would provide a unique look at how such social capital generates an economic benefit for the individuals. Subsequently, it is intended to derive conclusions out of the research for different social groups and the society as a whole, as well as implications on the culture of trust.

[1] S. A. Golder and M. W. Macy, "Digital footprints: Opportunities and challenges for online social research," *Annual Review of Sociology*, vol. 40, no. 1, pp. 129–152, 2014.

[2] Y.-C. Fu, "Contact diaries: Building archives of actual and comprehensive personal networks," *Field Methods*, vol. 19, no. 2, pp. 194–217, 2007.

13.7 C.1 Generic Decentralized Service Primitives for Privacy Protection in Human-Centered Sensor-Augmented Environments

Lars Almon (lalmon@seemoo.tu-darmstadt.de)
Supervisor/s: Matthias Hollick

Introduction: The rapid development and increased usage of human-near sensors in everyday life has introduced many challenges in the area of privacy protection. This creates the need to research and design new solutions from a technological and legal point of view. Human-centric sensing and actuation promises to support the user in everyday life by instrumenting her vital parameters and her environment, and by reacting to it. The privacy of the user is severely endangered if this data is not protected, even if those sensors only measure the surrounding environment. To this end, sensing and actuating devices such as smartphones, smart glasses, smart watches, wearables, medical implants, or exo-skeletons produce and consume a plethora of personal data and are usually connected to the Internet.

Methods: The research goal is to investigate how decentralized techniques can protect the privacy of the user in human-centric sensing and actuation scenarios. Three of these scenarios have been defined and will be evaluated:

(i) participatory sensor networks[1] in combination with smart rooms and environments,

(ii) applications to collect vital user data in combination with audio and video recordings from a user perspective, and

(iii) the combination of future medical sensor technology and actuator engineering.

Previous works such as[2] have proposed approaches to privacy friendly People Centric Sensing. New procedures for those scenarios will be developed to ensure a decentralized and secure storage, which simultaneously enables entitled users to perform exhaustive evaluations and collecting of user data. The usage of this data has to be clear and comprehensible in terms of privacy concerns for the involved user. The proposed solution should ensure usability and simplicity. The adequacy of the current legal framework for data protection has to be analyzed and possible improvements identified[3].

Note: I started working on my thesis in October 2015, funded by the DFG within RTG 2050 "Privacy and Trust for Mobile Users" at the Technische Universität Darmstadt.

[1] D. Christin, A. Reinhardt, S. S. Kanhere, and M. Hollick, "A survey on privacy in mobile participatory sensing applications," *Journal of Systems and Software*, vol. 84, no. 11, pp. 1928–1946, 2011.

[2] D. Christin, P. S. López, A. Reinhardt, M. Hollick, and M. Kauer, "Share with strangers: Privacy bubbles as user-centered privacy control for mobile content sharing applications," *Information Security Technical Report*, vol. 17, no. 3, pp. 105–116, 2013.

[3] A. Roßnagel, S. Jandt, H. Skistims, and J. Zirfas, *Datenschutz bei wearable computing.* Springer Vieweg, 2012.

13.8 D.1 AlterEgo as Assistant for Trust Assessments

Michael El Hanafi (lalmon@seemoo.tu-darmstadt.de)
Supervisor/s: Melanie Volkamer

In the digital world, users carry out their day to day tasks via different kind of services, e.g., web services, sensor or social networks. While using those services, users have to make many decisions. One fundamental decision is whether to trust a given service or not. The assessment about the trustworthiness of the service is thereby individual to the user. While technically-adept can make decisions based on their knowledge and experience, laymen and woman are often on their own and have no other option but to trust a given service blindly. Albeit the risk exposure of technically-adept is less, the consequences of a wrong decision stay the same, both for technically-adept and laymen and woman and can linger for a long time. These consequences can include a loss of social reputation (e.g., identity theft), a financial loss (e.g., phishing) and can even cause direct or indirect physical harm (e.g., critical infrastructure).

In this research area a digital representation of users' preferences regarding their privacy attitudes shall be developed. This representation, called AlterEgo, will act as an "Assistant for Trustworthiness Assessments". The Assistant shall support informed decision making of laymen and woman and experts alike, depending on their given knowlegde and skills. During the setup phase, AlterEgo and users have to get to know each other. While users become familiar with the given possible settings, especially regarding their privacy, AlterEgo has to broadly find out the key interests and the mental model of an individual user. This should allow AlterEgo to properly take actions and communicate with the user. Especially for the latter point, risk messages that inform about potential harms have to communicate in a manner that is, for each individual user, understandable[1]. Therefore communications have to respect the mental models of individuals, to support privacy-aware decision making. A challenging task hereby is to find the right balance between the necessarity of communication and the possible overload and mental stress that could arise through interruptions in users' workflows.

If users' preferences are known, special actions taken by AlterEgo should proceed automatically without extra user interaction. A resulting task is to find out if the communication of completed processes is helpful or even disturbing.

Another Topic is how to deal with user effects like the privacy paradox[2], that leads to an opposite user behaviour regarding his own preferences and therefore weakens the role of AlterEgo itself. Approaches of Gamification could be promising to counter this effect and to strengthen the relationship between the user and his or her AlterEgo.

[1] M. Volkamer and K. Renaud, "Number theory and cryptography: Papers in honor of Johannes Buchmann on the occasion of his 60th birthday," Springer Berlin Heidelberg, 2013, pp. 255–280.

[2] S. B. Barnes, "A privacy paradox: Social networking in the United States," *First Monday*, vol. 11, no. 9, 2006.

13.9 D.2 Enhancing the German Electronic ID Card to Serve as a Trust Anchor on Mobile Devices

Jacqueline Brendel (jacqueline.brendel@crisp-da.de)
Supervisor/s: Marc Fischlin

The goal of the Research Area D is to develop a digital system - in the following referred to as AlterEgo - which acts as an interface between the mobile user and the internet (and vice versa). As such, its main purpose is to enforce the user's desired requirements with respect to trust assessment and privacy protection in the network. At the same time, other counterparts in the network must be able to assess and verify the trustworthiness of an AlterEgo as the digital representative of a user. How to achieve this from a technical point of view is the main research objective of D.2.

Ordinarily, the establishment of trustworthiness in the internet is accomplished by digital certificates. But this approach has repeatedly proven to be unsatisfactory. For once, the usage of digital certificates expects users to have a good understanding about the design and working of the underlying system and public key infrastructure, which is generally not given. Furthermore, there exist countless many certificate authorities of which the majority is fully trusted by default (e.g. by browsers). Various incidents in the past have however shown that this trust is often misplaced. Therefore, the currently most prominent used approach is not sufficient to provide the demonstration of trustworthiness of an AlterEgo as a participant in the network.

We investigate the possibility to let the German electronic identity card (nPA) serve as a trust anchor on mobile devices (especially in combination with an AlterEgo) building on previous work by Fischlin et al.[1,2]. This approach assumes only a single central trustworthy certificate authority as opposed to many. Furthermore, the nPA supports pseudonyms for the holder of the ID card, as well as control over the transmitted personal data in a case-by-case fashion. We wish to develop enhancements to the German ID card according to specifications of the AlterEgo such that the privacy of the user is protected while still enabling trust assessment by other parties in the network.

The research progress in this project is still at the very beginning, because I have just started in February 2016.

[1] J. Bender, Ö. Dagdelen, M. Fischlin, and D. Kügler, "Information security: 15th international conference, ISC 2012, Passau, Germany, September 19-21, 2012. proceedings," Springer Berlin Heidelberg, 2012, pp. 104–119.

[2] J. Bender, M. Fischlin, and D. Kügler, "The PACE, CA protocol for machine readable travel documents," in *Proceedings of the 5th international conference on trusted systems - volume 8292*, 2013, pp. 17–35.

14 RTG 2167: User-Centred Social Media

Norbert Fuhr (norbert.fuhr@uni-due.de)
University of Duisburg-Essen
https://www.ucsm.info

The emergence of Social Media marks a significant step in the application of information and communication technology with a profound impact on people, businesses, and society. Social Media constitute complex sociotechnical systems, encompassing potentially very large user groups, both in public and organizational contexts, and exhibiting features such as user-generated content, social interaction and awareness, and emergent functionality. While Social Media use is widespread and increasing, significant research gaps exist with respect to analyzing and *understanding* the characteristics and determinants of user behaviour, both at the individual and the collective level, as well as regarding the user-centered design of Social Media systems, aiming at *empowering* users to better appropriate, control and adapt systems for their individual goals. There is a growing demand in academia and in industry for scientifically trained experts that are knowledgeable both in the human-oriented and the technical aspects of Social Media.

The Research Training Group "User-Centred Social Media" addresses this need by providing an outstanding interdisciplinary research and qualification environment, located in a University department that fully integrates researchers from computer science and psychology. Our research and qualification program provides students with the knowledge and methods from both areas required to perform high-quality research and development in Social Media. Besides following their individual research project, the PhD students also form inter-disciplinary working groups focusing on aspects such as credibility, information awareness and control, social network analytics, and hatespeech detection.

Our research program covers the three major sub-areas of Social Media:

- *Users*, aiming at modeling and understanding user behavior, where we investigate Social Media-related topics such as e.g. models of seeking and searching, decision support, information diffusion, or raising users' awareness of privacy issues.
- *Systems*, dealing with social media engineering, like e.g. transparency of subjective information, detection of deceptive messages, privacy and security.
- *Crowd*, addressing social media analytics, like e.g. detecting behavior patterns, tracing the evolution of ideas, social navigation and guidance for collaborative writing.

14.1 Social Media Retrieval

Huda Barakat (hbarakat@is.inf.uni-due.de)
Supervisor/s: Prof. Dr.-Ing Norbert Fuhr

Social media has become an essential source of information that increases every day as the number of tools, platforms and users in social media increases. People today depend on information from social media in many tasks like finding a solution for a problem or an answer to a question, knowing someone's opinion on a specific topic or evaluating a product based on others reviews. In fact, these tasks are particularly related to information retrieval but there are some issues that differ them from the traditional retrieval tasks.

The retrieval process in its basic form concerns with finding the most relevant information to the user query. However in social media, relevance is not the only criteria that conditioned the process, but there are also other aspects that need to be considered for more accurate retrieval results. One main aspect is the different properties (i.e. credibility, contradictory) that information objects (posts, reviews, answers,etc.) have in social media. In fact, such properties influence the user selection and therefore need to be considered in the retrieval process.

Beside the information objects there are also other related objects(ratings, tags, users, items, etc.) in social media that can appear in the retrieval process and participate in formulating its results. These objects participate in the process not just by their descriptions or their properties but also by the different relations that may exist and connect one object to another (i.e., a user may prefer the book that her friend or her relative selected before).

This thesis aims at developing alogic-based framework though which a social media retrieval model will be developed. As logical basis, we will consider two candidates: probabilistic 4-valued logic[1] and the subjective logic. The proposed model will be able to model the issues of contradictory and credibility and also different types of objects in social media and relationships among them. We will be also formulating rules for the retrieval strategies developed within our framework. The expected output of our retrieval strategies within the logic-based framework will enable our proposed model to provide a two-dimensional ranking for the retrieval results(i.e., ranking by relevance/credibility).

[1] N. Fuhr and T. Rölleke, "HySpirit - a probabilistic inference engine for hypermedia retrieval in large databases," in *Proceedings of the 6th international conference on extending database technology (EDBT)*, 1998, pp. 24–38.

14.2 User-controllable Methods for Generating Trustworthy Recommendations from Social Media Sources

Catalin-Mihai Barbu (catalin.barbu@uni-due.de)
Supervisor/s: Prof. Dr.-Ing. Jürgen Ziegler

Current recommender systems mostly do not take the wealth of information available in social media sufficiently into account, preventing the user from obtaining a broad and reliable overview of different opinions and ratings on a product. Furthermore, there is a lack of user control over the recommendation process (which is mostly fully automated and does not allow the user to influence the sources and mechanisms by which recommendations are produced) and the presentation of recommended items. Consequently, recommendations are often not transparent to the user, are considered to be less trustworthy, or do not meet the user's situational needs. Against this background, further optimizing the already quite mature recommender algorithms alone is unlikely to yield significant additional benefits for the user. Instead, more user-oriented approaches to recommending are needed[1].

The aim of this thesis is to develop a more interactive approach to recommending that combines algorithmic methods with techniques such as interactive filtering. Users should be able to control different sources of background data (in particular social media data such as ratings, tags, textual contributions, or user-user and user-item relationships) in a flexible manner. Furthermore, the visualization of the recommendations should be adapted to suit the user (e.g., by presenting personalized summaries of the recommended items). By taking these aspects into account, the trustworthiness of recommendations shall be increased. A hybrid recommender software framework developed in the Interactive Systems group[2], which allows to integrate different background data, will serve as a basis for this development. Novel techniques for making recommending more interactive (e.g., by combining algorithmic techniques based on latent factors with interactive steps for efficiently eliciting the user's current preferences[3]) will also be leveraged.

This PhD project will investigate the theoretical foundations for user-controllable, interactive methods of recommending, will develop techniques that exploit social media data in conjunction with other sources, and will validate the research empirically in the area of e-commerce product recommendations. The methods developed are intended to be applicable in a wide range of recommending and decision support scenarios.

[1] J. A. Konstan and J. Riedl, "Recommender systems: From algorithms to user experience," *User Modeling and User-Adapted Interaction*, vol. 22, pp. 101–123, 2012.

[2] T. Hussein, T. Linder, W. Gaulke, and J. Ziegler, "Hybreed: A software framework for developing context-aware hybrid recommender systems," *User Modeling and User-Adapted Interaction*, vol. 24, pp. 121–174, 2014.

[3] B. Loepp, T. Hussein, and J. Ziegler, "Choice-based preference elicitation for collaborative filtering recommender systems," in *Proceedings of the 32nd international conference on human factors in computing systems (CHI 2014)*, 2014, pp. 3085–3094.

14.3 Uncovering Graph Structures and the Evolution of Networks

Benjamin Cabrera (benjamin.cabrera@uni-due.de)
Supervisor/s: Barbara König

The analysis of networks and its abstraction in graphs has been a well studied research interest for quite some time. However, with the rise of the Internet, Social Media and Social Networks in particular the types of networks and requirements for algorithms have changed. Especially the size of interesting networks to study has increased dramatically which makes many methods that can be used for smaller graphs infeasible.

My research interests can roughly be devided into two fields. On the one hand I want to improve existing and develop new methods for uncovering structural properties of plain static graphs. On the other hand I'm interested in the dynamics of (social) networks, i.e. the evolution of networks over time. As an input I generally use labelled graphs (with node labels and optional edge labels) because in many applications on social media the networks contain more information than just the structure of nodes and edges.

For the analysis of static graphs a common problem is to compute frequent subgraphs (see Frequent Subgraph Mining). However, many of the applications for these technique focus on large graph databases (e.g. 10000 graphs) where each graph is relatively small (eg. 50 nodes, 100 edges). This is due to the complexity of the subgraph isomorphism problem (NP-complete) which makes testing if a graph contains a certain subgraph infeasible for large (dense) graphs. Nevertheless one can try to use approximative methods (maybe probabilistic algorithms) to get some meaningful results that then tell something about the structure and properties of (social) networks.

To mine the evolution of graphs in time we try to transfer the technique of process mining to graphs. Process mining usually gets log files that contain sequences of steps in some complicated process and then tries to identify the underlying process. This approach can be transfered to graphs where the log files are replaced with representations of network at different times and where the output consists of rules for the evolution of the input network.

14.4 Addressing Privacy Threats in Social Media

Nicolas E. Diaz Ferreyra (nicolas.diaz-ferreyra@uni-due.de)
Supervisor/s: Prof. Dr. Maritta Heisel

Social Media has set new standards for our interpersonal relations, and has accelerated the dynamics of our lives. Users of Social Network Sites (SNSs) spend considerable amounts of time exchanging (consuming or sharing) information, and using the services provided by these platforms. However, none of this comes for free since SNSs survive (in part) at the expense of the information that users place in their profiles, and the behavior they exhibit online.

Discovering hidden knowledge in social networks is a centerpiece in many personalized on-line services and targeted advertisement techniques, and is basically what makes a SNS profitable. Moreover, without the users' contributions, SNSs would lack of diversity and fail in being interesting enough for the users to engage with. However, many of the content that is uploaded to social platforms (text, image, video, location) contain a high level of private and sensitive information which -if disclosed- can bring harmful consequences to the users.

Among the different privacy breaches in Social Media there are the ones of identity disclosure, attribute disclosure, social link disclosure, and affiliation disclosure. All of these breaches can lead to harmful situations as a consequence of revealing the user's real identity to an adversary. However, not only scammers, stalkers, and identity thieves take advantage of the richness and diversity of personal information stored across the different SNSs. Nowadays is common to explore online profiles in order to get insights about people's personal aptitudes, political affiliation or sexual orientation. Nevertheless, this practice can easily derive into several discrimination and segregation scenarios.

Although existing privacy-protection mechanisms in Social Media have been improved over the years, they still do not provide a user-oriented assessment. Furthermore, current approaches are far from empowering the users with the necessary means for a better control of their personal information. We believe that in order to address information disclosure, and consequently reduce the likelihood of privacy threats, it is necessary to raise the levels of awareness among the users of SNSs.

This thesis projects aims to address the different Social Media privacy breaches from an interdisciplinary and user-oriented perspective. Since disclosing sensitive information is a common denominator of all these breaches, one of the goals of this project is to develop an approach based on self-adaptation which can assist users in identifying sensitive content among their contributions. In line with this, patterns of information diffusion will be analyzed and adapted in order to determinate the scope (reached audience) of the content being shared, and thereby reveal possible disclosure scenarios. Finally, an analysis of the different privacy harms and vulnerabilities in SNSs

14.5 User Models of Information Search in Social Media

Sebastian Dungs (dungs@is.inf.uni-due.de)
Supervisor/s: Prof. Dr.-Ing. Norbert Fuhr

Compared to traditional information retrieval—where information is provided by an authority—user generated content in social media is expected to be unreliable. Contradicting and low quality information as well as personal opinions pose new challenges for users of information systems.

Research in (interactive) information retrieval has focused on building an understanding of how users engage in the search process by creating models like Bates' Berrypicking Model, Belkin's Anomalous State of Knowledge hypotheses and his Episodic Interaction Model or Ellis' Model of Information Seeking Behaviour. While all of these papers had great impact on the information retrieval community, they were based on the concept of relevance given an information need and a set of documents providing objective and trustful information.

With the dominance of social media in peoples' every day media usage comes a shift in information origin. It is no longer created by authorities but by users themselves. While the aspect of document relevance to an information need is certainly still a major factor in search behaviour, content mainly created by users introduces new dimensions to information search which are not accounted for by above mentioned models and theories.

During this thesis, necessary extensions or constraints to well established qualitative models will be uncovered by taking the subjectivity of information, the existence of contradicting statements and the potentially overall poor quality of information into account. After models have been validated or extended a better understanding of the overall search process in social media IR can be of benefit to system designers and researchers.

Additionally, search in social media will be described quantitatively using Hidden Markov Models (HMM) and data gathered by user centred experiments. HMM are capable of modelling unknown processes or states based on observations that can be measured—i.e. modelling the user's cognitive processes during search by considering only the directly observable system logs. The challenge will be to find a good trade-off between model's complexity and expressiveness as well as to make sense out of the unlabelled hidden states returned by the model generation algorithm.

Given that these challenges can be dealt with, Hidden Markov Models can be used to make predictions about user's future actions in social media search. If these predictions are of sufficient quality, they can be used to guide the user in the search process. One potential outcome may be a reduced time to task completion or higher task completion rates and user satisfaction.

14.6 Human models of credibility judgement: An interdisciplinary approach

Matthias Lippold (matthias.lippold@uni-due.de)
Supervisor/s: Prof. Dr. Nicole Krämer and Prof. Dr. Norbert Fuhr

While using social media, users have to constantly evaluate onscreen-information based on their credibility. A lot of domain specific cues, which influence credibility judgement, are recognized (see. Choi et al. 2015 for an overview), but the human process of credibility judgement seems to be still under investigation. Some scholars claim, that people use heuristics to make their judgement (Metzger & Flanagin, 2013; Hilligoss & Rieh, 2008), however the evidence for a heuristically process is only based on surveys (Bellur & Sundar, 2014). Also, these proposed heuristic seemed to be under specified and it remains unclear, whether these heuristic strategies are an intuitive or deliberated processes. There is a big debate in the field of Psychology, whether people really use heuristically strategies automatically and a lot of consensus, that people might not use heuristics in their intuitive decisions (see. Hammond et al., 1987; Hogarth, 2001; Slovic et al., 2002; Kahneman & Frederick, 2002; Glöckner & Betsch, 2008). Even data from consumer choices shows evidence against heuristic processing but focuses more on a cue weighting model (Hilbig, 2014). Consequently, the first part of my thesis will transfer this knowledge to the current credibility research. I will formalize some of these proposed heuristic models and test them empirically. Following that, I plan on developing a new interdisciplinary model for credibility judgement on the basis of the lens model from Brunswick (1956). The lens model is usually used in judgment task, where the unobservable criteria is estimated by observable cues. The unobservable criterion is in the case of credibility the ground truths and which is estimated by using the observable credibility proxies. With machine learning techniques I will try to predict the cue validity of the given cues. The cue utilization, or the cue use of the individual user, will also be determine. These approach will combine computer science and psychology and might help to lead to more cooperation between these two disciplines

14.7 Social Media in and for Crisis Communication

Milad Mirbabaie (milad.mirbabaie@uni-due.de)
Supervisor/s: Professor Dr. Stefan Stieglitz

Social Media is used in many different domains, e.g. in an organisational context for marketing purposes, in a political context or in crisis situations e.g. for warning purposes. Social Media can be used as well for spreading information into the crowd (push factor), as receiving Information from the crowd (pull factor). Therefore, it is necessary to consider and examine both perspectives. The main object of this work is the crisis communication in Social Media. Consequences of crisis situation can be disastrous and have negative impacts on humans or on organisations. After a crisis occurs, a lot of information is produced in Social Media, as, people seek to gain a quick insight of the crisis and its possible impact. It is also necessary for Emergency Management Agencies (EMA), such as the police or fire brigade, to oversee the crisis's extent and to manage it in a short period of time. However, the mass of Social Media Data and the different nature of the platforms make it very difficult for volunteers, but also for EMAs to understand the crisis, examine detailed information quickly and act helpfully. Many ways and techniques exist in order to collect Social Media Data which depend on the structure of the platform and whether it offers an API or not. By collecting the data, new opportunities for the different stakeholder become apparent. Companies could collect Social Media Data for detecting raising Shitstorms and so preventing crisis situations. Public Organisations could make use out of social media for crisis communication for detecting rumours or false information. EMA's could analyse the data of crisis situations in order to predict disasters. Volunteers or bystanders in an affected area could use social media during a crisis, in order to inform other people. However, these aspects are barely researched and little mechanisms and scientific methodologies exist for analysing patterns of crisis communications. The overall question of this work is: "How can Social Media be used in order to support crisis management?" Within this more general question two Research questions are addressed:

RQ1: What types of Social Media data and information can be used during a crisis?

RQ2: What patterns of information diffusion exist in Social Media crisis communication?

For answering the first RQ, interviews with different EMA's will be conducted to identify requirements. Also several systematic literature reviews will be performed for gaining the status quo on the types of data and information. For the second RQ, a mixed method approach will be applied for detecting patterns in the information diffusion. For identifying the participating roles and the influence of the roles, several Social Network Analyses will be performed. Also emotions are influencing factors of a crisis situation and will be therefore identified in several crisis situations through sentiment analyses.

14.8 Transparency and personalization of subjective information

Michael Rist (rist@is.inf.uni-due.de)
Supervisor/s: Prof. Dr. Norbert Fuhr, Prof. Dr. Torsten Zesch

The internet, and especially social media content, contains a relatively large amount of subjective information. This of course lies in the very nature of social media as the content is user generated without any control instance, as existent in the traditional media. This work tries to create methods in order to help users find relevant informations within social media. In particular the focus lies in user generated product reviews as found on many online shopping sites. The reviews which will be used are gathered from the English Amazon page. From those reviews the mostly discussed aspects of each product should be extracted and the user, in search for information about a certain product, can filter and search for those, assumably most interesting, aspects.

To really help the decision making of a user, not only the most relevant aspects of a product will be extracted, but also the corresponding statements. Finding relevant aspects may only help to a certain degree, because the aspects reflect only interesting parts of a product but doesn't give any sentiment. This means a user would only know what's interesting about a product but not if this aspect is a problem or an especially positive feature of the product. Further this may be bothersome if this aspect is a rather ambiguous one and the opinions are varying. A user has to read many reviews to be able to make reasonable buying decision. So the sentiment towards an aspect is as an important part for presenting information to a user and improving the decision making.

A relevant statement of a product should not contain a arbitrary proposition of a user. This means that those reviews containing only the information whether the product is liked or not should be ignored. Such an arbitrary proposition is already given by the star-rating from Amazon or other, similar ratings. The relevant statements are rather the opinion of a user about a certain feature of the product. So only those statement will be considered that actually give more detailed information about the performance or aspects of a product.

Unlike many other approaches the focus does not lie in rating the sentiment. There exist several sentiment analysis methods for social media but finding reliable methods is still a problem as they are not completely accurate[1]. This may hinder a user in making a proper decision about a product. The focus of this work is to find the relevant aspect and retrieve the corresponding statements. These will be aggregated so that a user can see which statements were given and therefore the user can make a decision based on a summarization of the statements without possibly wrong-tagged sentiment.

[1] J. Serrano-Guerrero, J. A. Olivas, F. P. Romero, and E. Herrera-Viedma, "Sentiment analysis: A review and comparative analysis of web services," *Information Sciences*, vol. 311, pp. 18–38, 2015.

14.9 Raising users' awareness of privacy issues

Johanna Schäwel (johanna.schaewel@uni-due.de)
Supervisor/s: Prof. Dr. Nicole Krämer and Prof. Dr. Maritta Heisel

Users of Social Network Sites (SNSs) disclose a large amount of information to their online network. Research on the privacy paradox (Barnes, 2006) has shown that even though users (sometimes) know about the risks of (extensive) online sharing-behavior, they continue disclosing personal data. But in some cases, users simply are not aware of their audience, of what information could be sensitive, and of the consequences of their sharing behavior. Consequently, there is the need of privacy protection systems that raise users' awareness of these privacy issues. Although there have been developed some privacy protection mechanisms in the past, there is no extensive, user-friendly, adaptive and efficient solution for supporting the user in his / her online behavior. With my theses I aim at identifying the boundary conditions of the privacy paradox (since its validity has been discussed recently), and at identifying efficient and accepted privacy protection mechanisms or functions that raise users' awareness. In order to protect the user and to develop an efficient privacy protection system, it is necessary to understand in detail why (online) self-disclosure is beneficial and what the users' requirements are. But most importantly it has to be figured out which technical features to secure privacy will be accepted and employed by the users. Self-disclosure has been defined as the "act of revealing personal information to others" (Archer, 1980) and as the "process of making the self known to other persons" (Jourard and Lasakow, 1958). The extent of self-disclosing varies between users, depending on the personality characteristics, knowledge and awareness. Reasons for and benefits of self-disclosure are for instance gratifications such as social support, self-clarification, relationship development and self-representation in a very cautiously way. Self-disclosure, especially in online contexts, is associated with fundamental individually different needs like the need for diversion and entertainment, the need for social relationships and the need for identity construction (Debatin, 2009). Additional variables that influence the privacy behavior on the one hand, and the self-disclosing behavior on the other hand, are the need for popularity, the self-esteem value and the levels of trust in the social network (Christofides, Muise, & Desmarais, 2009). As a consequence, all these values have to be considered when developing a privacy protection system. Since self-disclosing personal information is rewarding for the users, I aim at identifying a more valuable reward for secure online behavior. One access point could be the use of gamified elements instead of providing merely a warning text-unit. In addition to that, such a privacy protection system should consider the individual online-behavior (quantity of sharing, content of posts, sensitivity of information) in order to adapt on the users' online-practices. All these values and characteristics can help to provide an adequate degree of support. For examining these suggestions there is the need of controlled experiments and the testing of the gamified incentives.

14.10 Recommending Scientific Literature based on Content and Network Analytic Approaches

Laura Steinert (steinert@collide.info)
Supervisor/s: Prof. Dr. H. Ulrich Hoppe

Literature search for scientists new to a field poses many challenges, among them the lack of knowledge of the correct keywords to use in a query. Although several paper recommender systems exist, a system that specifically provides papers to gain an overview of a specific scientific topic for researchers has – to the best of my knowledge – not been explored yet.

Therefore, in my dissertation I intend to develop a system that recommends papers that provide an overview of a scientific field. Potential beneficiaries of such a system are PhD and master students that just started working on their thesis or scientists that switched to a new field. How exactly such recommendations can be characterized is my first research question.

An expert study will focus on the characterization of such recommendations. In this study experts are asked to handpick papers that together provide an overview of the expert's area of expertise to a starting PhD student. Furthermore, the experts are asked to rate the importance of specific criteria – e.g. diversity – for their paper selection. Afterward, the sets of papers will be evaluated with respect to the rated criteria with objective measures. Furthermore, shared characteristics of the sets of papers will be analyzed – e.g. their connections in the citation network or their topical similarity.

It is expected that each of the selected sets of papers has a high diversity while each paper is prototypical. Furthermore, the expectation is that the recommended papers together cover most of the key aspects and subtopics of the targeted scientific topic. Thus, the breadth of covered subtopics in the set of recommendations is high, whereas the depth to which the subtopics are explored is moderate.

After successfully identifying characteristics that define good recommendations, various algorithms will be analyzed with regard to their suitability for this task. Among these algorithms will be a hybrid algorithm developed earlier by me that uses both content information of the papers as well as the information how the different papers are connected via their citations (cf.[1]). Another of the analyzed algorithms will be the Main Path Analysis[2] that is able to identify the main scientific papers that shaped the development of a scientific field. If none of the existing systems proves sufficiently suited for the task one of the algorithms will be improved or a new algorithm developed.

[1] L. Steinert, I. Chounta, and H. U. Hoppe, "Where to begin? Using network analytics for the recommendation of scientific papers," in *Collaboration and technology - 21st international conference, CRIWG 2015, Yerevan, Armenia, September 22-25, 2015, proceedings*, 2015, pp. 124–139.

[2] N. P. Hummon and P. Doreian, "Connectivity in a citation network: The development of DNA theory," *Social Networks*, vol. 11, no. 1, pp. 39–63, 1989.

14.11 Stance-based Argument Mining in Social Media

Michael Wojatzki (michael.wojatzki@uni-due.de)
Supervisor/s: Prof. Dr.-Ing. Torsten Zesch

Argumentation is a constellation of propositions that is used to convince someone of a standpoint. Especially in social media, argumentation is frequently observable and can be considered as an essential element of social media interaction such as online debates. Since this phenomenon occurs at a massive scale, many groups of information seekers (e.g. researchers, journalists, companies, etc.) could benefit from an automated analysis of social media argumentation. This automated identification of argumentative structures within written communication is called argument mining[1].

However, current approaches in argument mining face serious difficulties if applied on social media data. After analysing the state-of-the-art, we identified two fundamental problems of current approaches. First, most approaches rely on strict formalisms such as the Claim-Premise-Scheme which requires that an argument is composed of exactly one claim and an arbitrarily large number of premises, justifications and other forms of support[2].

These schemes are developed to model argumentation highly elaborated, well-formed text (e.g. scientific writing or legal text) and less suited to deal with the noise and lower argument density of social media. Second, in contrast to elaborated text, social media contains a high proportion of implicit argumentation (e.g. up to 50% of the claims are implicit in an online debate).

In order to tackle the described problems, we propose stance-based argument mining as the topic for the dissertation. A stance is the attitude (being in favor or against) of an author towards a given target like a politician or a controversial topic[3]. By transforming propositions into a constellation of stances towards targets, one should obtain a more abstract representation of arguments that should be more robust against implicitness and noise. Therefore, the first milestone for the dissertation is to develop the ability detect the stance towards a defined target. Hence, we have already participated in the *SemEval 2016 Task 6: Detecting Stance in Tweets* with considerable success. As a next step, this ability should be applied to targets which are determined at runtime. Further, experiments will be conducted which will help to model the combination of several targets into a comprehensive schema.

[1] N. Green, K. Ashley, D. Litman, C. Reed, and V. Walker, Eds., *Proceedings of the first workshop on argumentation mining*. Association for Computational Linguistics, 2014.

[2] I. Habernal, J. Eckle-Kohler, and I. Gurevych, "Argumentation mining on the web from information seeking perspective," in *Proceedings of the workshop on frontiers and connections between argumentation theory and natural language processing*, 2014, pp. 26–39.

[3] S. M. Mohammad, S. Kiritchenko, P. Sobhani, X. Zhu, and C. Cherry, "Semeval-2016 task 6: Detecting stance in tweets," in *Proceedings of the international workshop on semantic evaluation*, 2016.

15 RTG HPI: HPI Research School on Service-oriented Systems Engineering

Prof. Dr. Andreas Polze (andreas.polze@hpi.uni-potsdam.de)
Hasso Plattner Institute at the University of Potsdam
http://hpi.de/en/research/research-school.html

Design and implementation of service-oriented architectures impose numerous research questions from the fields of software engineering, system analysis and modeling, adaptability, and application integration.

"Service-oriented Systems Engineering" represents a symbiosis of best practices in object orientation, component-based development, distributed computing, and business process management. It provides integration of business and IT concerns.

Our research school devotes to current topics in the field of IT systems engineering with high potential in academic research as well as in industrial application. Supported by an internationally renowned grant, PhD students at our school participate in joint activities such as lectures, seminars, winter schools, and workshops. The professors of the HPI, each one having an own research group, are the supporting pillars for our research school. With its interdisciplinary structure, our school interconnects the HPI research groups and fosters close and fruitful collaborations.

In context of the research school, the different groups at HPI work on the following topics: Human Computer Interaction (Prof. Dr. Patrick Baudisch), Computer Graphics Systems (Prof. Dr. Jürgen Döllner), System Analysis and Modeling (Prof. Dr. Holger Giese), Software Architecture (Prof. Dr. Robert Hirschfeld), Internet Technologies and Systems (Prof. Dr. Christoph Meinel), Information Systems (Prof. Dr. Felix Naumann), Enterprise Platforms and Integration Concepts (Prof. Dr. h.c. Hasso Plattner), Operating Systems and Middleware (Prof. Dr. Andreas Polze), Business Process Technology (Prof. Dr. Mathias Weske), Algorithm Engineering (Prof. Dr. Tobias Friedrich), Knowledge Discovery and Data Mining (Prof. Dr. Emmanuel Müller).

15.1 Visualization and Analysis of Public Social Geotagged Data to Provide Situational and Public Safety Awareness

Aragats Amirkhanyan (aragats.amirkhanyan@hpi.de)
Supervisor/s: Prof. Dr. Christoph Meinel

Nowadays, social networks are an essential part of modern life. People post everything what happens with them and what happens around them. The amount of data, produced by social networks, increases dramatically every year. And, also, there is a trend, that users more often post geotagged messages. For researchers, it is important, because it gives us more possibilities for visualization and analysis of social data, since we can be interested not only in the content of messages but also in the location, from where these messages were posted. And now, there are many tools that visualize and analyze social data and social geotagged data. Most of them are focused on visualization, analysis and provision of different statistics to support marketing and business.

Our research is based on increasing the popularity of location-based social networks (LBSN) and increasing the amount of geotagged messages produced by social networks. Also, it is based on the statement that social networks are very reflective to real-word events. Therefore, we suppose that if something happens in the real-world then it will be almost immediately reflected in social networks in the form of geotagged messages. Such events (happenings) could be different, but we are mostly interested in local real-world threats, such as bomb threats, traffic accidents, house fires, thefts and others. Therefore, from our perspective, we are aimed to use publicly available social geotagged data from LBSN to provide situational awareness and public safety awareness.

In the scope of our research, we develop the approach from the sketch and we try to find the best ways of visualization and analysis of public social geotagged data to provide mentioned situational and public safety awareness. And for that, we need to find and provide only valuable statistics that can help to analyze in real-time public safety awareness. Also, we address the challenge of filtering data from invaluable data in the perspective of describing the situation around, because not all geotagged messages from social networks describe the situation around, even if they have geo location information. Another challenge is to cluster geotagged messages around some area, during some period of time and describing the same topic. And then identify whether the cluster describes local spatial event, what type of the event and whether the event is a local threat. Within all mentioned challenges and future plans, with our research, we are aimed to improve public safety awareness, in order to help law enforcements make cities safer.

15.2 Improving Decision Making in Business Processes

Ekaterina Bazhenova (ekaterina.bazhenova@hpi.de)
Supervisor/s: Prof. Dr. Mathias Weske

Business process management is widely used by many companies to run their businesses efficiently. To ensure optimal process executions, decision management should incorporate decision logic documentation and implementation. An interest from academia and industry in the development of decision management has lead to the recently emerged DMN standard[1] aimed to be complementary to the BPMN standard[2].

To assist companies with successful automated decision management, knowledge about ''as-is" decision making needs to be retrieved. This can be done by analysing process event logs and discovering decision rules from this information. Existing approaches for decision mining concentrate on the retrieval of control flow decisions but neglect data decisions and dependencies that are contained within the logged data. To overcome this gap, we extended an existing approach to derive control flow decisions from event logs[3] with additional identification of data decisions and dependencies between them. Furthermore, we proposed an algorithm for detecting dependencies between discovered control flow and data decisions. In order to improve business process executions, we propose a method of prioritizing of input data in decision tasks with the help of dynamic restructuring of underlying decision structures.

Our approach is demonstrated on example of credit assessment in banks. Thus, we firstly demonstrate how an automation rate of a decision process in credit assessment can be increased by semi-automatic extraction of the decision rules from a simulated event log. Secondly, we detect possibility of minimizing the number of questions the bank asks the customers in order to give the credit and suggest.

[1] OMG–DMN, "Decision Model and Notation (DMN), v. 1.0 - Beta 2." 2015.
[2] OMG–BPMN, "Business Process Model and Notation (BPMN), v. 2.0.2." 2013.
[3] A. Rozinat and W. van der Aalst, "Decision mining in business processes," BPM Center Report BPM-06-10, 2006.

15.3 Runtime data-driven software evolution in enterprise software ecosystems

Thomas Brand (thomas.brand@hpi.de)
Supervisor/s: Prof. Dr. Holger Giese

Often new ideas for optimization and additional functional requirements emerge shortly after a software system is put into service. To which extend the software system and its underlying software products can maintain or extend their relevance depends significantly on how they evolve and get adapted to changing conditions and feedback.

Thus for manufacturers of software products the following tasks are crucial:

- Understand the customers' change requests and requirements.
- Generalize customer requests, prioritize and integrate them into existing software products. Additionally foster the maintainability and adaptability of the products.
- Offer and provide the resulting changes to the customers.

With our research project we want to investigate, how feedback from running software systems can help to adapt and enhance the underlying products incrementally over time. The whole feedback cycle shall be considered: How to gain and utilize feedback from running software systems and how to rollout resulting software product changes to the customers' systems?

Currently I am focusing on adaptive monitoring to utilize it for usage measurement. For this purpose I am working on a mechanism to simulate the runtime data generation in multiple differently configured systems, which are based on the same software product. This shall later help to test approaches to control runtime data gathering, processing and preserving in a self-adaptive manner.

15.4 Equivalence between Deterministic and Random Graph models for Real-World Networks

Ankit Chauhan (ankit.chauhan@hpi.de)
Supervisor/s: Prof. Dr. Tobias Friedrich

In recent years, there has been extensive research to understand real-world networks such as social networks, the WWW, or protein-protein interaction networks. It has been observed experimentally that almost all real-world networks follow a power law degree distribution, exhibit ultra-small shortest paths, and have a large clustering coefficient.

There are many random models that try to mimic these behaviors, e.g., the Preferential Attachment model, the Chung-Lu model, and the Geometric Inhomogeneous Random Graph model[1,2]. All these models have the most important property of real-world graphs: they follow a power law distribution. Recently, Brach et. al.[3] developed the first deterministic graph model known as Power Law Bounded (PLB) model, which captures the scale-free property of real-world networks. Further, Brach et.al. defined the PLB-neighborhood property for PLB networks, leading to faster algorithms for problems like counting the number of triangles, or perfect matching. They also proved that finding a maximum clique is in polynomial time for the class of PLB-neighborhood graphs.

In this regard, we are analyzing the relation between the PLB model and the random graph models for real networks. If random graph models also produce graphs with the PLB-neighborhood property, we can directly translate this into faster algorithms on these models for counting triangles or the perfect matching problem. Also, we can say that there exists a polynomial time algorithm for finding maximum cliques in these random graph models.

Further, we will work on the PLB graph model to characterize parameterized problems[4] such as k-Clique or k-DominatingSet. Of particular interest is whether a k-clique or a k-dominating set in PLB graphs can be found in FPT time. It has been observed that, in some real-world networks, hard problems can be solved fast with simple preprocessing. We want to analyze the impact of these preprocessing steps on the formal PLB model.

[1] F. Chung and L. Lu, "The average distance in a random graph with given expected degrees," *Internet Math.*, vol. 1, no. 1, pp. 91–113, 2003.

[2] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[3] P. Brach, M. Cygan, J. Lacki, and P. Sankowski, "Algorithmic complexity of power law networks," *CoRR*, vol. abs/1507.02426, 2015.

[4] J. Flum and M. Grohe, *Parameterized complexity theory (texts in theoretical computer science. an EATCS series)*. Springer-Verlag New York, Inc., 2006.

15.5 Scalable Visualization of Massive, Semantically Rich 3D Point Clouds

Sören Discher (soeren.discher@hpi.de)
Supervisor/s: Prof. Dr. Jürgen Döllner

Applications for environmental monitoring, urban planning and development, as well as disaster and risk management require precise and up-to-date information about objects and structures of a given landscape, city, or surface area. Such information can be acquired by using in-situ or remote sensing technology such as LiDAR and image matching algorithms. Processing and visualizing the resulting 3D point clouds –i.e., discrete, digital representations of real-world surfaces– poses challenges for hardware and software systems due to the massive amount of data that needs to be handled. Even worse, if additional data layers such as thematic and temporal information or analysis results have to be combined with the raw point data, the management becomes more critical with respect to performance and storage requirements. Traditional geoinformation systems tend to address this challenge by reducing the point cloud's precision and density, and, therefore, they typically fail to make use of the full resolution and potential of the data.

To visualize arbitrary large 3D point clouds even if the data exceeds a system's GPU or main memory capacities, external memory algorithms have to be applied, that render only the most relevant points for a given view. Thus, an efficient access to subsets of the data based on different data layers –especially a point's spatial position– is required. This can achieved by combining spatial data structures and level-of-detail concepts. Traditionally, external memory algorithms focus on high-end desktop computers featuring direct data access. To visualize massive 3D point clouds even on low-end mobile devices, such algorithms have to be combined with client-server-based approaches that limit workload and data traffic on client-side by using a central server infrastructure to maintain and distribute the data.

My work is focussed on the interactive exploration, inspection, and analysis of massive, heterogeneous, time variant, and semantically rich 3D point clouds. Towards that goal, visualization techniques are designed and evaluated to enhance the recognition of objects, semantics, and temporal changes within 3D point cloud depictions as well as filtering and highlighting techniques to dissolve occlusion and to give context-specific insights. As an example, such techniques can be used to identify differences and structural changes within a captured site (e.g., constructed, demolished, or modified buildings) by dynamically highlighting points that indicate such changes. Building upon these visualization techniques, the work focusses on efficient and intuitive navigation and interaction concepts to further facilitate the exploration of 3D point clouds (e.g., by allowing to select visually identified objects within the data set) as future work.

15.6 Experimental dependability evaluation of complex software systems

Lena Feinbube (lena.feinbube@hpi.uni-potsdam.de)
Supervisor/s: Prof. Dr. Andreas Polze

This research focusses on evaluating software dependability both from a theoretical, and a practical perspective.

Fault injection is a useful tool testing the fault tolerance features by artificially inserting faulty behaviour and error states into a running system. Thus, fault injection represents the notion that the faultload needs to be incorporated into the software testing process.

To increase representativeness and coverage of fault injection, the questions of when and where to inject faults need to be answered.

Therefore, the theoretical focus of this research is to better understand the details of fault activation and error propagation in software. Fault models for software are currently limited, either to purely code-based aspects, or to high level failure behaviour. The state conditions which trigger the activation of dormant software faults, and thus lead to error states still form an elusive aspect.

A dependable software system must be fault tolerant at all layers of the software stack.

Our practical research focus lies upon fault injection at the operating system and distributed middleware layers. At the operating system level, we show how different classes of software faults in libraries can be simulated using link-time API hooking. The fault classes are chosen as representatives from the community-maintained CWE database of real world software problems. At the distributed level, modern cloud services have to fulfill needs such as scalability, availability and security simultaneously. Therefore, experimental dependability assessment using distributed fault injection is steadily gaining relevance. Ongoing research on fault injection in OpenStack is discussed.

15.7 The Design and Implementation of the Babelsberg-Family of Object-Constraint Programming Languages

Tim Felgentreff (tim.felgentreff@hpi.de)
Supervisor/s: Prof. Dr. Robert Hirschfeld

Constraints allow developers to specify properties of systems and have those properties be maintained automatically. This results in compact, declarations to describe interactive applications, avoiding scattered code to check and imperatively re-satisfy invariants in response to user input that perturbs the system. Constraints thus provide flexibility and expressiveness for solving complex problems and maintaining a desired system state. Despite these advantages, constraint programming is not yet widespread, with imperative programming still being the norm.

There is a long history of research on constraint programming as well as its integration with general purpose programming languages, especially from the imperative paradigm. However, this integration typically does not unify the constructs for encapsulation and abstraction from both paradigms and often leads to a parallel world of constraint code fragments intermingled with the general purpose code. This impedes re-use of modules, as client code written in one paradigm can only use modules written to support that paradigm — thus, modules require redundant definitions if they are to be used in both paradigms. Furthermore, clear distinction between the paradigms requires developers to learn about and fully understand both paradigms to make use of them.

In our work, we have developed a design for a family of object-constraint languages called Babelsberg. Our design unifies the constructs for encapsulation and abstraction by using only object-oriented method definitions for both declarative and imperative code. Just like assertions, our constraints are expressed using ordinary imperative expressions, including full objects and message sends. Unlike assertions, however, the system attempts to satisfy them if they are not currently true, and keeps them satisfied throughout the remaining execution. We provide a semantics that guides implementers of our design to combine Babelsberg with existing object-oriented host languages both semantically and syntactically and to demonstrate its feasibility with an executable semantics and three concrete implementations of Babelsberg. To allow developers to use the power of constraints without having to understand the specifics of different constraint solving strategies, we integrate an architecture for using multiple cooperating solvers. Finally, based on our experience with the concrete implementations, we propose performant implementation strategies of key features for object-constraint programming.

We argue that our approach provides a useful step toward making constraint solving a useful tool for object-oriented programmers. We also provide example code, written in our implementations, which uses constraints in a variety of application domains, including interactive graphics, physical simulations, data streaming with both hard and soft constraints on performance, and interactive puzzles.

15.8 Detecting and Monitoring Changes in Urban Areas Based on Multi-Temporal 3D Point Clouds

Dietmar Funck (dietmar.funck@hpi.de)
Supervisor/s: Prof. Dr. Jürgen Döllner

Recent developments in remote sensing technologies such as laser scanning and image matching have lead to widespread capturing of landscapes, urban regions, and cities. The resulting 3D point clouds are digital snapshots of the captured environments and used for a growing number of applications such as deriving 3D building models, terrain models, and vegetation models. A regular data acquisition (e.g., once a year) of an area results in so-called multi-temporal 3D point clouds. Such multi-temporal 3D point clouds can be used to detect and monitor changes over time as well as accumulating 3D point clouds captured at different points in time.

We develop concepts and techniques to maintain, process and analyze multi-temporal 3D point clouds. Our workflow takes as input dense 3D point clouds captured at different points in time. Classification and change detection approaches are used to categorize every point (e.g., surface category, degree of change). Redundancy and temporal changes are identified and used to solve further analysis tasks such as detecting and classifying changes in the environment, e.g., new buildings, removed vegetation, and leveled terrain. Out-of-core data structures and GPU-based processing schemes are introduced to handle massive 3D point clouds containing billions of points at reasonable processing times. As a case study, we demonstrate our approach for an urban area of a city.

The results show that the approach opens new ways to manage, process, and analyze large-scale, dense, and time-variant 3D point clouds as required by a growing number of applications and systems.

15.9 Utility-Driven Modularized MAPE-K loop architectures for Self-Adaptive Systems

Sona Ghahremani (sona.ghahremani@hpi.de)
Supervisor/s: Prof. Dr. Holger Giese

Self-adaptive software provides the capability to observe changes of itself at runtime, reason about itself, and autonomously adapt itself. However, this additional capability is always limited concerning its power to reason on itself and there is always the tradeoff which costs come with the reasoning and adapting. On the one end of the spectrum of possible approaches are rule-based approaches which are often limited concerning their reasoning power but highly efficient and on the other end are utility-driven approaches that consider often costly algorithms to achieve a good optimization of the utility.

We peruse a hybrid adaptation policy in a modularized multi-concern self-adaptive system where each module is allowed to apply the type of adaptation strategy which fits better to its concern. The goal of the hybrid adaptation is to benefit from the strong points of each methodology and let them compensate for each others? weaknesses. Regarding the challenges caused by modularization such as the order in which modules need to be executed and dependencies among modules, we intend to apply a policy in which we avoid the probable unwanted interferences. We also propose benefiting from a utility-driven policy to obtain the optimal ordering scenarios for executing modules, for that purpose we need to assign utility values to each module and define a utility function which assigns a real-valued scalar representing the desirability of system configuration identifying how good that specific state or configuration is as opposed to others. The proposed approach allows to define a utility function for architectural runtime models, to specify the possible improvements or repairs of the architecture by means of rules, and finally to achieve the incremental triggering of the rules according to their impact on the utility. We were able to show that the suggested utility-driven rule-based adaptation works incrementally and that under certain assumptions it always results in the optimal improvement of the utility over time.

15.10 Resource management in rack scale architectures

Andreas Grapentin (andreas.grapentin@hpi.uni-potsdam.de)
Supervisor/s: Prof. Dr. Andreas Polze

Currently, we can observe three parallel threads of development in the resource architecture of distributed computing and high end rack scale server systems that will force operating systems to adapt in order to efficiently distribute system resources to processes.

Firstly, with the arrival of *nonvolatile memory (NVM)* in server systems imminent, we expect to see a paradigm shift in the memory hierarchy within the next years - future generations of NVM devices are expected to be fast, powerful and affordable enough to possibly replace the traditional block layer. Secondly, there has been ongoing work on optical interconnects with color multiplexing, which have the potential to practically eliminate the *nonuniform memory architecture (NUMA)* characteristics of server systems. Thirdly, based on these developments, there is the possibility of a new type of distributed computing architecture which has been named *shared something architecture*. These shared something machines consist of a large memory pool shared between a heterogeneous set of compute nodes, each with a smaller pool of local memory.

This thesis evaluates whether the traditional resource management approaches implemented by modern operating systems and their common manifestations in user space APIs - such as `malloc` and `mmap` - are still relevant on these new architectures and what changes will be necessary to be able to efficiently manage resource allocations.

In order to answer these questions, different resource management strategies are implemented in a virtualized environment resembling a smaller shared something architecture on a heterogeneous set of compute nodes and evaluated in a set of different allocation scenarios.

15.11 Mechanisms from Metamaterial

Alexandra Ion (alexandra.ion@hpi.de)
Supervisor/s: Prof. Dr. Patrick Baudisch

Recent advances in fabrication technology, such as high-resolution 3D printers, allow fabricating objects with internal microstructure, also known as mechanical metamaterials. In this work, we create a new class of metamaterials: mechanisms, i.e., devices that transform forces and movement. These mechanisms from metamaterials require no assembly since they are made from one single material and in one piece. We arrange cells of different topologies to create the desired output force or motion, e.g. a door latch mechanism where the latch is pulled in when the user pushes the handle down.

Designing the internal microstructure–potentially consisting of billions of cells–is a complex task. As a first step, we approach this by creating an editor that helps experts to design such mechanisms from metamaterial. We argue that the key to more complex metamaterials is to allow users to manipulate individual cells and sub-cell elements interactively. We propose a system that converts metamaterials to (stacks of) bitmaps and back, enabling the use of efficient image processing tools. We read color information from pixels and construct the cells of the 3D model's microstructure. Depending on objects' size and (future) 3D printer resolution the number of cells can be arbitrarily large, leading to challenges in terms of space and time complexity. Therefore, we investigate efficient data structures and caching algorithms to reuse already processed blocks of geometry. In the future, we will computationally generate the cells and their arrangement in order to synthesize a mechanism.

15.12 Profiling the Web of Data

Anja Jentzsch (anja.jentzsch@hpi.de)
Supervisor/s: Prof. Dr. Felix Naumann

Over the past years, an increasingly large number of data sources has been published as part of the Web of Data. Metadata gives consumers of the data clarity about the content and variety of a dataset and the terms under which it can be reused, thus encouraging its reuse.

A Linked Dataset is represented in the Resource Description Framework (RDF) embodying an entity-relationship-graph. In comparison to other data models, RDF lacks explicit schema information that precisely defines the types of entities and their attributes. Therefore, many datasets provide ontologies that categorize entities and define data types and semantics of properties. However, ontologies are not always dereferenceable or may be incomplete. Algorithms and tools are needed that profile the dataset to retrieve relevant and interesting metadata analyzing the dataset.

Existing work on data profiling often can not be applied to Linked Datasets due to their different nature. To overcome this gap we introduce a comprehensive list of data profiling tasks which compute the most important statistical properties along different groupings.

Finding information about Linked Datasets is an open issue on the constantly growing Web of Data. While most of the Linked Datasets are listed in registries as for instance at the Data Hub, these registries usually are manually curated. We present approaches and challenges for cataloging Linked Datasets and retrieving relevant metadata.

Data profiling often exhibits considerable performance problems. We introduce three common techniques for improving performance, and present an approach that relies on parallelization and adapts multi-query optimization for relational data to optimize execution plans of Linked Data profiling tasks.

As Linked Datasets are usually sparsely populated, key candidates often consist of either multiple low-density properties or cannot be found at all. We present two approaches for key discovery, a traditional unique column combination adaption and an approach that tackles the sparsity on the Web of Data by combining the uniqueness and density of properties.

Graph analysis can be used to gain more insight into the data, induce schemas, or build indices. We present an approach for frequent graph pattern mining, and a set of common and re-occuring graph patterns that can be considered the core of most Linked Datasets.

All presented approaches are evaluated thoroughly on real-world datasets, and are implemented in the interactive Linked Data profiling suite ProLOD.

15.13 BottlePrint: Scaling Personal Fabrication by Embedding Ready-Made Objects

Robert Kovacs (robert.kovacs@hpi.de)
Supervisor/s: Prof. Dr. Patrick Baudisch

Personal fabrication tools, such as 3D printers have achieved a desktop form factor. As a result, they have spread to the maker community, as well as increasingly also to consumers[1]. In contrast, the fabrication of large objects has remained a privilege of industry, which has access to specialized equipment, such as concrete printers to make houses[2], as well as fabrication robots[3]. The owners of the widespread desktop devices, in contrast, cannot participate in this step in evolution, as the underlying technology does not scale. Even if we break down large models into parts that fit into a desktop-scale device[4] fabricating a large model consumes time and material proportional to the size of the model, quickly rendering 3D printing and related techniques intractable for larger-than-desktop-scale models.

BottlePrint is a fabrication system that allows users to produce large-scale objects on desktop-scale fabrication machines. The key idea behind bottlePrint is to complement 3D printing with ready-made objects, in our case empty plastic bottles. BottlePrint considers 3D models as wireframe models; it then fabricates only the hubs of this wireframe model, while it implements all edges as bottles. The resulting large-scale objects are sturdy enough to carry human users.

Our main contribution is that we enable large-scale fabrication on desktop-size fabrication devices. The key idea is to include ready-made objects, in particular empty plastic bottles as the main building element. Our software system allows users to create bottle-based 3D objects by converting an existing 3D model or by modeling from scratch.

In addition to enabling users to fabricate large-scale objects on conventional desktop-scale devices, our approach offers the following benefits: *(1) Fast:* the bulk of the objects volume is ready-made. *(2) Light:* Can be moved around even in assembled form. *(3) Modular:* modify, extend, combine, or fix objects with only local changes. *(4) Environmentally conscious:* most of the materials are upcycled. *(5) Ubiquitous:* plastic bottles can be acquired anywhere worldwide, so users setting up large installations elsewhere can travel lightly, carrying just the hubs.

[1] J. G. Tanenbaum, A. M. Williams, A. Desjardins, and K. Tanenbaum, "Democratizing technology: Pleasure, utility and expressiveness in DIY and maker practice," in *Proceedings of the SIGCHI conference on human factors in computing systems*, 2013, pp. 2603–2612.

[2] B. Khoshnevis, "Automated construction by contour crafting—related robotics and information technologies," *Automation in construction*, vol. 13, no. 1, pp. 5–19, 2004.

[3] S. Jokic, P. Novikov, S. Maggs, D. Sadan, S. Jin, and C. Nan, "Robotic positioning device for three-dimensional printing," *arXiv preprint arXiv:1406.3400*, 2014.

[4] M. Lau, A. Ohgawara, J. Mitani, and T. Igarashi, "Converting 3D furniture models to fabricatable parts and connectors," in *ACM transactions on graphics (TOG)*, 2011, vol. 30, p. 85.

15.14 Theory of Estimation of Distribution Algorithms for Discrete Optimization

Martin S. Krejca (martin.krejca@hpi.de)
Supervisor/s: Prof. Dr. Tobias Friedrich

Traditional optimization algorithms, for example for finding good solutions for the traveling salesperson problem (TSP), are designed by carefully analyzing the problem and then tailoring an algorithm that exploits the problem structure. Research on optimization has progressed sufficiently so that, for many classic optimization problems, very good problem-specific algorithms are available.

When the problem structure is not well understood and no problem-specific algorithm for the optimization task is available, generic optimization algorithms are frequently the only way to achieve decent optimization. Many of such generic optimization algorithms fall into the group of *Estimation of Distribution Algorithms* (EDAs)[1]. They are search meta-heuristics that maintain a probability distribution of the solution space and iteratively update it according to samples from this distribution.

Hauschild and Pelikan[2] give a nice survey of EDAs where they point out many successful applications of these algorithms to a wide range of problems, frequently yielding better results than any other competing algorithms. They also state advantages of EDAs that give an explanation to *why* they perform so well.

The main goal of our research is to further the understanding of EDAs in the discrete domain $\{0,1\}^n$, using *formal* arguments. We focus on, what Hauschild and Pelikan call, *univariate, incremental* EDAs since this model subsumes many EDAs that have been both analyzed theoretically and applied in practice. This model assumes independence of the individual bits in the solution space and only creates very few samples each iteration.

Up to now, there are only few theoretical results on univariate, incremental EDAs; most of them considering run times for specific algorithms. Our goal is to give structural results, not only necessarily run time results, for great classes of EDAs to gain a deeper understanding of what properties result in certain behavior and how this affects the optimization process.

[1] P. Larrañaga and J. A. Lozano, *Estimation of distribution algorithms: A new tool for evolutionary computation*. Kluwer Academic Publishers, 2002.

[2] M. Hauschild and M. Pelikan, "An introduction and survey of estimation of distribution algorithms." *Swarm and Evolutionary Computation*, vol. 1, no. 3, pp. 111–128, 2011.

15.15 Interactive Exploration of High-level Programming Concepts

Stefan Lehmann (stefan.lehmann@hpi.uni-potsdam.de)
Supervisor/s: Prof. Dr. Robert Hirschfeld

Providing abstractions to increase the expressiveness of source code has been of research interest for long time. Abstractions provide a specific, complex behavior through a simplified interface. Using a mixture of domain-specific and general purpose abstractions developers can express desired functionality near the problem domain by hiding implementation details. By bridging the gap between the problem domain and the underlying machine model abstractions increase the readability and maintainability of static source code.

However, while raising the abstraction levels of the language and runtime, the development of appropriate programming tools is often neglected. As a result, conventional debuggers present run-time information at the level of basic language concepts, thereby breaking the encapsulation introduced by the used abstractions. For example, when extending a language and runtime with means for context-specific behavioral variations the code can be more concise and expressive, but that complexity of implementation details is often exposed unnecessarily when exploring run-time behavior. Hence, the intended behavior is often lost in the implementation details of abstractions. Because those details are hidden on the source code level, the mapping of run-time behavior to source code is hard. This gap between the static and dynamic representation of the program increases the cognitive effort to comprehend the behavior of a program. Therefore, programming tools have to be made aware of the new language constructs and the characteristics of runtime concepts.

The concept of an abstraction-aware debugger is twofold. First, only information relevant to the current use case should be presented to lower the amount of information the developer has to comprehend. Depending on the current situation a developer could either be the user or the provider of an abstraction. The debugger has to be aware of the use case and filter information accordingly. Second, the information has to be presented in a way that matches the mental model of the static source code. To reify abstractions at run-time the debugger refines views on the system state to reflect the presented abstraction as perceived by the programmer in static source code.

To increase the usability and accessibility of a new programming concept, specialized tools have to co-evolve with the concept.

15.16 Proprioceptive Interaction

Pedro Lopes (pedro.lopes@hpi.de)
Supervisor/s: Prof. Dr. Patrick Baudisch

We advance our research in the exploration of interactive wearable systems that use electrical muscle stimulation (EMS). Insofar by using EMS to actuate the user's body instead of using motors, we've drafted two main benefits: (1) force-feedback devices with wearable form factor; and, (2) write to a new output channel: the user's proprioceptive sense is particularly useful in eyes-free scenarios. However the EMS-based systems, that either we created or that can be found in related work, communicate only a few bits of information to the user per interaction (e.g., turn left or right, use an object in n pre-defined ways, etc).

Currently, we explore how to create interactive systems based on EMS of high expressiveness. We propose a mobile system that assists users in cognitively demanding activities, such as writing math, by providing them with access to a computer system. Using pen-on-paper interaction, users write formulas and the system responds by drawing graphs. Unlike earlier work, however, our system uses the pen not only for input (based on Anoto tracking technology), but also for output: it uses electrical muscle stimulation to make the user's hand plot.

Our main contribution is that our system is the first interactive system that actuates users using an EMS signal to achieve a continuous output signal. This allows it to produce spatial output, which is substantially more expressive than earlier systems that produced discrete poses only. Still, the use of EMS allows our system to achieve a compact mobile form factor. We are currently investigating how our system behaves with participants in a user study setting.

15.17 Use Events to Implement BPMN Processes

Sankalita Mandal (sankalita.mandal@hpi.de)
Supervisor/s: Prof. Dr. Mathias Weske

Business process management (BPM) has gained a lot of popularity in past few decades. Organizations are striving continuously to come up with more efficient operations by improving their processes. Complex event processing (CEP) has already proven to be a very powerful mean to achieve this[1].

In recent years, more and more systems are following event-driven approach. They produce events, consume events, react on events, take decisions based on events and also predict future paths from event-logs. The OMG standard Business Process Model and Notation (BPMN 2.0)[2] defines several start events, intermediate events, and end events which can occur at the beginning, during or end of a process, respectively. Depending on the position, type and information contained, they determine the course of the process afterwards.

Current process engines support the basic events like 'Message Events' or 'Timer Events'. But there are inconsistencies between modeling these events and implementing them. Mostly, the simple events are aggregated into complex events using an event platform and the process engines act on the higher level events produced by the CEP platform. Also, the correlation between the event instances and the corresponding process instances is not visible in the model level. Therefore, the process experts miss the consistent view. Even worse, for the more complicated events like 'Parallel Multiple Events', there is no strong support from either the existing process engines or the existing event platforms.

Our research goal is to bridge these gaps in a two-folded way: by providing modeling support to ease the definitions of CEP and by focusing on the implementation concepts that can pave the way for automated implementation consistent with the model level.

[1] O. Etzion and P. Niblett, *Event processing in action*. Manning Publications, 2010.
[2] OMG, "Business Process Model and Notation (BPMN), Version 2.0." http://www.omg.org/spec/BPMN/2.0/, January-2011.

15.18 Data-Driven Process Improvement in Agile Software Development Teams

Christoph Matthies (christoph.matthies@hpi.de)
Supervisor/s: Prof. Dr. Hasso Plattner

Software Developers have access to a wide range of tools that statically analyze development artifacts, especially code, in order support them in their work. An example of this approach are linting tools, which identify suspicious source code fragments that violate a set of predefined coding rules. These checks can be run frequently, to provide up-to-date information.

Such automated feedback tools are equally desirable for "linting" the executed processes in agile development teams. However, providing timely, concrete feedback on possible process improvements in a team is a challenging task. This is mostly due to the intentional lack of formal agile process models[1] and the complexity of reviewing the interactions of team members. Currently, we give concrete feedback mostly through process experts, i.e. coaches, who observe teams during their regular work. While this approach yields high quality, custom-tailored improvement suggestions, it is also biased by the expert's own opinions and does not scale well to large amount of teams.

We propose an approach which tackles these issues by analyzing development artifacts, e.g. commits or test results, and the implicit knowledge about the executed process they contain. This allows automatic analysis and feedback without interfering with developers' regular workflows[2]. Possible problems in the executed process are identified and linked to concrete development artifacts, which can be further researched and discussed. Using this approach, development teams receive immediate feedback on their executed development practices. They can use this knowledge to improve their workflows, or can adapt the metrics to better reflect their project context.

Future work includes defining and iterating the process metrics that can be employed[3], exploring the impact of employing automated feedback tools in teams and researching the applicability of these approaches to professional software development.

[1] K. Schwaber and J. Sutherland, "The Scrum Guide," in *The Definitive Guide to Scrum: The Rules of the Game*, 2011, p. 1.

[2] P. M. Johnson, H. Kou, J. Agustin, C. Chan, C. Moore, J. Miglani, S. Zhen, and W. E. J. Doane, "Beyond the Personal Software Process: Metrics collection and analysis for the differently disciplined," in *Proceedings of the 25th international conference on software engineering*, 2003, pp. 641–646.

[3] N. Zazworka, K. Stapel, E. Knauss, F. Shull, V. R. Basili, and K. Schneider, "Are Developers Complying with the Process: An XP Study," in *Proceedings of the 2010 ACM-IEEE international symposium on empirical software engineering and measurement*, 2010, p. 14.

15.19 Exploring Predictive Models in Live Programming Environments

Toni Mattis (toni.mattis@hpi.uni-potsdam.de)
Supervisor/s: Prof. Dr. Robert Hirschfeld

For programmers, a major challenge during the evolution of complex software is building a mental model of concepts and dependencies in order to combine them to new functionality. Failure to do so may result in redundant code, applying the wrong functionality, or the utter inability to complete the task at hand.

Current tools increase discoverability of concepts and their connections by ubiquitous navigation, search and code completion. Recent research tries to advance the capabilities of these tools by mining semantic units that transcend the hierarchical decomposition, such as cross-cutting concerns and topics. However, these appproaches stick to the classical concept of compile-and-run workflows and do not make use of live data alongside the code base.

Live data is central to the programming experience in *live programming environments*, such as Squeak/Smalltalk or Lively, which facilitate the manipulation of a program while it is being executed. This way, the programmer recieves immediate feedback on whether the change manifests as intended. Moreover, experimentation with live data or example instances is well supported, e.g. for getting used to an API, testing an assumption one is unsure about, or reproducing an error condition.

In live programming environments, object manipulations and code snippets executed during experimentation also convey meaning, e.g. dissecting example strings may indicate the programmer intends to parse text. A tool capable of understanding the concepts related to a previously unseen piece of code can support the programmer, e.g. by proposing already existing parsing functionality via code completion, or providing example instances of a parser object for the programmer to experiment with. This serves as a first step towards tactically predictive live environments that present the developer with possible future versions of its program to choose from[1].

Building on previous research[2], we investigate the use of a topic model to associate code with abstract concepts and vice versa. Several conceptual challenges, such as encoding the hierarchical nature of code in the model, representing the dependencies among topics, incorporating live data, and learning from being corrected by the programmer are currently in the focus of our research. Also, evaluation metrics of such models should be reassessed in the context of live environments, where immediacy and traceability of a proposal may be more relevant than guessing the correct code snippet.

[1] S. L. Tanimoto, "A perspective on the evolution of live programming," in *Proceedings of LIVE 2013*, 2013, pp. 31–34.

[2] E. Linstead, P. Rigor, S. Bajracharya, C. Lopes, and P. Baldi, "Mining concepts from code with probabilistic topic models," in *Proceedings of ASE 2007*, 2007, pp. 461–464.

15.20 Adaptive Data Structure Optimization for Evolving Dynamic Programming Languages

Tobias Pape (tobias.pape@hpi.uni-potsdam.de)
Supervisor/s: Prof. Dr. Robert Hirschfeld

Dynamic programming languages evolve over time. New concepts of programming, paradigms, and methodologies require adaption to languages and, hence, their implementations. The typical implementation process for programming languages, however, is complex, since a large number of programming languages are written in lower-level languages such as C or C++ mainly for reasons of performance. This holds especially for dynamic languages that typically run hosted on a VM. Sophisticated memory management, Gc, multi-stage interpreters and JIT compilers are complex tasks common to typical dynamic language VMS.

Using meta-programming is hence a common way of implementing new concepts. Meta-programming may ease the implementation and maintenance of large systems by changing the language "from within". As such meta-level programs are written in the same high-level, dynamic language for which they are written, they can benefit from already present concepts from automatic memory management to extensive standard libraries, to name a few. However, these meta-level constructs can cause a performance overhead, as most execution environments are optimized for non-meta-level programs - a potential impact on the programs using it.

To alleviate this, a common approach is to adapt the execution environment, resorting to lower-level implementation means, handling special cases and optimizations for each new language element for better performance. On the other hand, programming language implementations are harder to maintain with every new special case for a certain feature.

We argue that fast generic VM optimizations, such as adaptive data structure optimizations can alleviate the performance impact of meta-level implementations of programming language elements and support the evolution of dynamic programming language in a maintainable fashion. With adaptive data structure optimizations, that take ordinary, generic data structures and optimize them in the execution environment, no special cases in the execution environment nor in the programming language are necessary to obtain acceptable performance when using meta-level facilities to implement new programming concepts.

15.21 Bio-inspired Heuristic Optimization of Noisy Functions

Francesco Quinzan (fq00@posteo.de)
Supervisor/s: Prof. Dr. Tobias Friedrich

In many practical optimization problems, the objective function has some kind of stochastic component that arises out of different factors such as measurement error, simulation nonlinearities, the finite precision of Monte Carlo sampling, or other environmental effects. In these scenarios, the direct evaluation of the objective function is not as reliable, and optimization algorithms must employ some kind of noise-handling strategy.

The idea of reducing noise by means of resampling has been approached from different perspectives over the years. Aizawa and Wah[1] proposed a detailed adaptive strategy for modeling the underlying noise in order to determine the appropriate number of samples. Stagge[2] recognized that noise can be reduced by repeated sampling, even at the cost of a higher number of fitness evaluations. Many other detailed sampling frameworks have been proposed, such as ones based on selection races from the machine learning community[3].

Ant Colony Optimization (ACO) have been observed to be particularly well-suited for solving dynamic and noisy problems[4]. ACO algorithms do not explicitly keep a population of solutions in memory, but instead construct a sequence of pheromone values that represent a probability distribution over the search space. This approach appears to make them particularly robust in a changing, noisy environment.

However, the impact of resampling and implicit distribution-building mechanisms of ACO algorithms are not clear. We look at the interplay between statistical resampling and implicit noise-handling that arises from the cooperative distribution-building mechanisms of ACO algorithms. We empirically compare the performance of the $(\mu + 1)$-EA (a mutation-only evolutionary algorithm), the $(\mu + 1)$-GA (a steady-state genetic algorithm employing crossover) and λ-MMASib (an ant colony optimization algorithm). We investigate the trade-off between resampling and implicit noise-handling ability of each of these algorithms.

[1] A. N. Aizawa and B. W. Wah, "Scheduling of genetics algorithms in a noisy environment," *Evolutionary Computation*, vol. 2(2), pp. 97–122, 1994.
[2] P. Stagge, "Averaging efficiency in the presence of noise," *In Proc. of PPSN '98*, pp. 188–200, 1998.
[3] P. Rolet and O. Teytaud, "Bandit-based estimation of distribution algorithms for noisy optimization: Rigorous runtime analysis," *In Proc. of LION '10*, pp. 97–110, 2010.
[4] M. S. K. T. Friedrich T. Kötzing and A. M. Sutton, "Robustness of ant colony optimization to noise," *In Proc. of ISAAC '15*, pp. 17–24, 2015.

15.22 Medical Image Analysis by Deep Learning

Mina Rezaei (Mina.Rezaei@hpi.de)
Supervisor/s: Prof. Dr. Christoph Meinel

During the past years deep learning has raised a huge attention by showing promising result in some state-of-the-art approaches such as speech recognition, handwritten character recognition, image classification, detection and segmentation. There are expectations that deep learning improve or create medical image analysis applications, such as computer aided diagnosis, image registration and multimodal image analysis, image segmentation and retrieval. There has been some application that using deep learning in medical application like cell tracking and organ cancer detection.Doctors use medical imaging to diagnosis diseases. Medical application and diagnosis tools make it faster and more accurate.

An advance application based on deep learning methods for diagnosis, detection and segmentation of brain magnetic resonance imaging (MRI) is my goal. I started working with 5 different categories of MR brain images. I have achieved notable result in brain abnormality detection between healthy, tumor high and low grade glioma, Alzheimer and multiple sclerosis disease by deep learning.My deep learning network for classification is based on the network proposed by Krizhevsky et al[1]. The difference is between number of convolutional neural network layers and number of pooling layers. Furthermore I tuned the model and use log loss instead of softmax. In future I would like continue on object detection and segmentation of brain lesion by convolutional neural network.Our evaluation results on UCF101 video dataset for human action recognition show our approach achieves very competitive performance compare to recent work. Our future work will focus on exploring more sophisticated fusion model. On the other hand, we will consider data augmentation techniques for further improving spatial and temporal mode accuracy.

[1] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in *Advances in neural information processing systems 25*, Curran Associates, Inc., 2012, pp. 1097–1105.

15.23 Trading Something In for an Increased Availability

Daniel Richter (daniel.richter@hpi.uni-potsdam.de)
Supervisor/s: Prof. Dr. Andreas Polze

Although there are many techniques to deal with faults and errors, one usually cannot assure that a software system is hundred percent fault free. In addition, there are types of faults such as design faults than cannot be faced with error processing based on redundancy.

The key idea of this research is to increase the availability of software systems without having highly available infrastructure is to relax other system properties: On data level, one can trade in (strong) consistency guarantees, and on algorithm level, one can trade in feature richness, accuracy and precision and even correctness to reduce the periods when a system cannot perform its primary function.

To benefit from relaxed consistency, one has to identify different roles of components or code paths and their need for a specific level of consistency. There may are components that need a global view on data and strong consistency, for other components it could sufficient to only know what they did, while some components can work with data that do not have to be up-to-date but should not be too old, and some other components may only need some value without having to know whether operations were performed in the correct order.

On algorithm level, one can use flexible computation and trade in feature richness, imprecise computation and trade in accuracy and precision, and resilient computation and trade in correctness. Flexible computation means that depending on the system state (appearance of errors, system loads) some optional components may are deactivated or replaced by alternative components (i.e. faster, smaller, more reliable). With imprecise computation depending on the runtime an algorithm is provided with, the accuracy of the result increases. Such algorithms usually are interruptible and can provide a result at any point in time. The most "radical" mean to increase the availability is to use resilient computation – the focus here is to deliver a result under all circumstances. It is guaranteed to get a result, but that may is not correct.

In the end, suitable methods to fulfil acceptability properties such as safety, integrity, and exactness for relaxed algorithms as well as the correspondence to different criteria of improvement (e.g. execute as many optional tasks as possible with flexible computing, get the most precise result with imprecise and resilient computing, or get a strong consistent view as fast as possible with relaxed consistency guarantees) according to specific error metrics (e.g. minimize total error, average error, or maximum error) have to be developed.

15.24 Propositional Satisfiability and Scale-Free Networks

Ralf Rothenberger (ralf.rothenberger@hpi.de)
Supervisor/s: Prof. Dr. Tobias Friedrich

Over the last decades it was observed that many real-world networks exhibit degree distributions that follow a power-law, including Internet topologies, the Web, social networks, power grids, and literally hundreds of other domains. Furthermore, it was shown that these networks feature a unique set of additional properties besides their power-law degree distribution. These properties include the existence of a giant component, which contains all but a linear fraction of nodes, small average distance between two nodes, normally in the range of $O(\log \log n)$, community structure, i.e. the emergence of densely connected subgraphs which are only sparsely connected to the rest of the network, and the existence of hub nodes, which are connected to a large fraction of nodes in the network[1].

One domain, where problem instances with these properties occur, is the satisfiability of propositional formulas (SAT). For *industrial instances* it was recently shown that their clause and variable distributions resemble power-laws[2] and that they exhibit community structure[3]. Industrial instances arise from problems in practice, such as hardware and software verification, automated planning and scheduling, and circuit design. Although SAT is NP-complete in theory, even *large industrial instances* with millions of variables can often be solved very efficiently by modern SAT solvers. This implies that their structural properties might be beneficial for the runtime of SAT solvers.

The goal of this thesis is to develop models which generate synthetic formulas that are similar to real ones, and to analyze these formulas. Having realistic models would provide a means of creating large-scale benchmarks for solvers. To this end, we propose using approaches known from the generation of scale-free networks to achieve this goal.

On the foundations of such models, it is possible to do rigorous analysis. The goals of this analysis are to identify phase transitions in the satisfiability of instances depending on different parameters and to design heuristics to efficiently solve instances generated in our models. Our hope is that the results of this analysis and the developed algorithms can be transferred to the original real-world problems. This might improve the efficiency of SAT solvers or at least explain the effectiveness of state-of-the-art solvers. Achieving this goal requires developing new probabilistic tools suitable for the analysis of scale-free SAT instances. As the constraint and incidence graphs of such instances are scale-free graphs, we can reuse some recent methods developed for the analysis of scale-free networks.

[1] R. van der Hofstad, "Random graphs and complex networks," 2011.
[2] C. Ansótegui, M. L. Bonet, and J. Levy, "On the structure of industrial SAT instances," in *Principles and practice of constraint programming - CP'2009*, Springer, 2009, pp. 127–141.
[3] C. Ansótegui, J. Giráldez-Cru, and J. Levy, "The community structure of SAT formulas," in *Theory and Applications of Satisfiability Testing–SAT 2012*, Springer, 2012, pp. 410–423.

15.25 Linespace: a sense-making platform for the blind

Thijs Roumen (thijs.roumen@hpi.de)
Supervisor/s: Prof. Dr. Patrick Baudisch

For visually impaired users, making sense of spatial information is difficult as they have to scan and memorize content before being able to analyze it. Even worse, any update to the displayed content invalidates their spatial memory, which can force them to manually rescan the entire display. Making display contents persist, we argue, is thus the highest priority in designing a sense-making system for the visually impaired. We present a tactile display system designed with this goal in mind. The foundation of our system is a large tactile display (140x100cm, 23x larger than Hyperbraille), which we achieve by using a 3D printer to print raised lines of filament. The system's software then uses the large space to minimize screen updates. Instead of panning and zooming, for example, our system created additional views, leaving display contents intact and thus preserving user's spatial memory.

Linespace is a platform and thus supports various different applications to run on it. In exploring this concept we aimed for complex visual applications, currently we have maps, excel, a software debugger, games and more running on the device. This is all supported through a developed programming platform. Next steps would be to make the device mobile (instead of a printer running on the table it would be driving around) and integrated as a service within the infrastructure of blind users.

As early evaluation we have had 10 blind users interact with the device so far. On top of that we had sighted experts in accessibility give feedback when they observed interacting blind users. Participants responded favorably to the system and expressed, for example, that having multiple views at the same time was helpful. They also judged the increased expressiveness of the lines over more traditional dots as useful for encoding information.

15.26 Distributed Incremental Duplicate Detection

Ahmad Samiei (ahmad.samiei@hpi.de)
Supervisor/s: Prof. Dr. Felix Naumann

Duplicate detection is a time-expensive process that is periodically executed on a database. The sheer amount of streaming data, generated as a result of wide spreading internet, sensor data, etc., added to an already clean, de-duplicated database makes it obsolete very fast, and therefore imposes extra cost to its maintenance. Incremental record de-duplication attempts to address this problem and makes databases with many transactions always up-to-date and clean. That is, duplicate detection must happen on the fly, as the data arrives and enters the database.

The prevalence of distributed platforms for data processing has made it very attractive for researchers to investigate and utilize them for efficient parallelization of such computationally intensive jobs. There are already some works focused on batch-deduplication approaches, mainly on Apache Hadoop, a Map-Reduce based platform. In this work we investigate and compare different frameworks for distributed data processing, namely Apache Flink and Apache Spark, for the task of incremental deduplication. The mentioned platforms add a new API for stream-data processing, which could be suitable for incremental duplicate detection. We attempt to utilize this new feature and devise an incremental algorithm that efficiently parallelizes the task, and finally compares the performance of the two different frameworks.

15.27 Omniscient Debugging in Database Applications

Arian Treffer (arian.treffer@hpi.de)
Supervisor/s: Prof. Dr. h.c. Hasso Plattner

Developers spend between 40 and 60 percent of their time working on defects. A lot of that time is spend in the debugger, searching for the cause of an observed problem. While debugging, the developer's attention is divided between multiple tasks, which fall into two categories: first, understanding the program at different levels of abstraction and second, operating the debugger and other related tools.

Debuggers work with very low and technical concepts, such as variables and instructions. The mapping to higher conceptual levels is left to the developer. Furthermore, debuggers are unforgiving: a step to far and the entire debug session has to be restarted. Thus, the developer is forced to step forward with utmost care, which requires a level of attention that makes it difficult to think about the actual problem simultaneously.

In our work, we combine existing concepts of omniscient debugging and object-centric debugging to create a Java debugger that allows the effortless navigation of program executions, both forwards and backwards through execution time. Additionally, we devised a new configurable algorithm for dynamic slicing that fits the interactive nature of the debugging workflow. In sum, we were able to create a debugging toolchain that helps the developer to investigate complex problems without diverting her attention to tool operation.

Large and complex applications also often use a database to handle complex operations on large amounts of data. While most modern databases allow to attach a debugger to queries or scripts, the general tool support for understanding complex programs in databases is rather poor compared to that of popular object-oriented languages.

To accommodate the demand for better debugging tools in database programs, we transferred our research findings to SQL Script. We developed a method to leverage the mix of imperative control flow and declarative SQL statements in SQL Script. This allowed us to created an omniscient debugger which is much more efficient with large amounts of data than previous solutions for object-oriented languages. Furthermore, we adapted our dynamic slicing algorithm to the increased complexity by implementing different levels of accuracy.

15.28 Video Classification with Convolutional Neural Network

Cheng Wang (cheng.wang@hpi.de)
Supervisor/s: Prof. Dr. Christoph Meinel

With the rapid development of Internet technology, tremendous amount of videos are uploaded to World Wide Web every day. Statistics[1] shows that 300 hours of video are uploaded to YouTube every minute. It is hard for a human to go through them all and find videos of interest. One possible way to narrow the choice is to look for video according to category or label information. But, most videos do not contain semantic meta data and the video platforms are left clueless about the contents. Thus, classifying video according to their content is important to video search and retrieval.

Video classification is a challenging task which attracts much attention recently. Inspired by the recent advance of deep learning, many efforts have been made to enhance the understanding of video, for example, video action recognition with convolutional neural network(CNN). One commonly used approach for video classification is based on classifying the key frames that extracted from videos. Recent work have proved that temporal clues can provide additional information for improving video classification performance. In this work, we firstly train spatial and temporal models with CNN separately with deep learning framework. Our framework comprises of three components: the *spatial*, *flow* and *fusion* nets respectively. Based on pre-train models, we extracted the features of the 6-th fully connected layer from each CNN. And then, we impose a fusion layer which consists of two fully connected layers to combine the features from different streams. Since fusing multiple feature such as text-image fusion, audio-video fusion has provided a promising results for video classification, we also focus on the exploration the fusion approach for combining spatial and temporal information.

Our evaluation results on UCF101 video dataset for human action recognition show our approach achieves very competitive performance compare to recent work. Our future work will focus on exploring more sophisticated fusion model. On the other hand, we will consider data augmentation techniques for further improving spatial and temporal mode accuracy.

[1] https://www.youtube.com/yt/press/en-GB/statistics.html