Proceedings of the 9th Joint Workshop of the German Research Training Groups in Computer Science

**Dagstuhl 2015,
May 31st- June 3rd**

A. Babari, C. Carapelle (editors)

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 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 the meeting is organized in cooperation by RTG 1763: *Quantitative Logics and Automata* and RTG 1773: *Heterogeneous Image Systems*, and takes place at the Research Center of Schloss Dagstuhl from May 31st until June 3rd.

Since the participating RTGs present their work in different scientific areas, ranging from mechanical engineering and robotics to very theoretical fields of computer science as machine learning, formal languages and logic, the focus of the workshop remains interdisciplinary. The workshop at Schloss Dagstuhl, in fact, intends to encourage new collaborations among the participants from different RTGs, and to create and and strengthen new and existing networks.

This year's workshop includes the following activities: Fast forward sessions, where the speakers of the RTGs introduce the main topics and focus of their group and the students give a fast introduction to their research projects. Open discussion groups, poster presentation sessions as well as a programming challenge, to encourage discussion and exchange of ideas. Three invited talks, which present several important achievements in various fields of computer science.

The presentations made by the workshop participants, as well as the research projects from all students members of the involved RTGs, are summarized in short abstracts and made available in these electronic proceedings.

We would like to thank everybody who contributed to the organization of this joint meeting and in particular the authors of the abstracts and the RTGs' administrations for their cooperation. Special thanks go to our invited speakers: Prof. Dr. rer. nat. Dr. techn. hc. Dr.-Ing. E.h. Thomas Ertl - "The Joy of Visualziation", Prof. Dr. rer. nat. habil. Wolfgang Reisig - "Informatics as a scientific discipline and as a University Degree program: How it started", and Dr. Christian Rossow - "Analyzing and Detecting Malicious Software". Finally, we would like to thank the DFG for funding this meeting and the staff of Schloss Dagstuhl for the organization and for hosting our workshop.

<div align="right">

Parvaneh Babari and Claudia Carapelle
for QuantLA
Sergiu Dotenco, Arne Hendricks and Anna Yupatova
for Heterogeneous Image Systems

</div>

Contents

Contents

Contents

Contents

Contents

Contents

<div align="center">

Contents

</div>

Contents

Contents

Contents

Contents

Contents

1 GRK 1298: AlgoSyn - Algorithmic Synthesis of Reactive and Discrete-Continuous Systems

Prof. Dr. Dr. h.c. Wolfgang Thomas
Email: thomas@informatik.rwth-aachen.de
Rheinisch Westfälische Technische Hochschule Aachen
Internet: http://www.algosyn.rwth-aachen.de/

While methods of software validation and verification are by now well established, based on adequate formal models and tested in practical applications, the approach of automatic syn-thesis of software (and hardware) is as yet only developed in quite rudimentary form. On the other hand, in theoretical computer science as well as in engineering disciplines a rapidly increasing stock of techniques for algorithmic synthesis is emerging, triggered by the demand to decrease development costs by invoking algorithmic methods. However, the approach of program synthesis is only applicable in restricted scenarios, in particular in reactive (multi-agent) systems with low data complexity, such as control systems, and in the transformation and optimization of existing models. Central issues in the area are the establishment of system models which allow for an algorithmic solution of the synthesis problem, the combination of discrete and continuous parameters in hybrid systems (as this is also familiar from verification), and the exploration of the potential of applications. The aim of the Research Training Group is to unify the expertise from computer science, mathematics, and engineering disciplines (embedded systems, automatic control, process control engineering, train traffic systems) and to push forward the desired integration of methods. The research projects are organized on three levels: Theoretical foundations (algorithmics and formal models), model transformations and software engineering, and applications.

1.1 Verification of Code for Programmable Logic Controllers

Sebastian Biallas (`biallas@embedded.rwth-aachen.de`)
Supervisor: Stefan Kowalewski

Programmable Logic Controllers (PLCs) are control devices used in industry for monitoring and controlling of plants, robots and safety critical infrastructure. Since they are often used in safety critical environments where a failure might have serious effects on human health or the environment, formal verification of their programs is advised. This strive for functional correctness combined with having small, well-structured programs, makes PLCs a very interesting platform for the application of formal methods.

For their operation, PLCs have inputs, which are usually connected to sensors, and outputs, which are connected to actuators. The operation is controlled by a program, which is periodically called at a high frequency to set new output values depeding on the current inputs. The program can access non-temporary variables that retain their value for the next cycle. This allows to select, e. g, different modes of operation. The programs are usually composed of function blocks which can be written in various programming languages.

To analyse and verify PLC programs, this project automatically creates a model reflecting their operation. This model comprises states, which are tuples combing the values of the input, output and non-temporary variables after one execution of the program. A transition between states is assumed if they are reachable within one cycle. This model can then be analyzed using formal methods: We allow for model checking using CTL and past time LTL logic and offer a static analysis to determine ranges of variable values.

Such a model can naïvely be generated by simulating the program for all possible input values and iterating this process for the new states. In general this process is not feasible, since even the state space of small programs comprises too many states. Hence, we use symbolic states which abstract a set of concrete states using, e. g., intervals. To select a suitable abstraction, we start by a very coarse abstraction of the program and then use a counterexample guided abstraction refinement. That is, we analyze counterexamples returned by the model checker for feasibility in the concrete state space. If they are not feasible, we use them as a hint to refine the current abstraction. For this, we can currently use either an own constraint solver or the Z3 SMT solver. To generate the transition relation on the corresponding abstract state space we use an abstract simulator.

The results of this work are implemented in the ARCADE.PLC framework, which offers a graphical user interface, the necessary program file parsers and abstract simulators to analyse PLC programs using these techniques.

1.2 Synthesis of Succinct Reactive Systems

Benedikt Brütsch (`bruetsch@automata.rwth-aachen.de`)
Supervisor: Prof. Dr. Dr. h.c. Wolfgang Thomas

In the game-theoretic approach to controller synthesis for reactive systems, the goal is to find a winning strategy for the controller in an infinite game. Such strategies are typically represented as transition systems. However, these transition systems can be very large and hence, more compact representations are desirable. We consider the problem of directly synthesizing succinct representations of winning strategies in infinite games (without first synthesizing a transition system in an intermediate step).

1.3 Synthesized Supervisory Control for PLC programs

Florian Göbe (goebe(at)embedded.rwth-aachen.de)
Supervisor: Univ.-Prof. Dr.-Ing. Stefan Kowalewski

The Supervisory Control Theory (SCT) has been introduced by P. J. Ramadge W. M. Wonham in 1987[1]. It provides a way to automatically synthesize *supervisors* in the context of *discrete event systems*, which look and behave similar to finite deterministic automata. The synthesis bases on a previously modeled *specification* and a *generator* model that emits events. Although there has been considerable effort spent on complexity issues that arise due to the state space explosion in modular systems there are still very few applications or tools that actually apply SCT practically. In most existing approaches the generator usually represents a plant where both *controllable* and *uncontrollable events* occur. The product of the synthesis process is in this case a model of the supervised (i. e. safe) plant model, where undesired behavior is avoided by disallowing certain controllable events. In our experience, it usually is not possible to apply that supervisor to a given physical system directly.

In contrast, we address the control of real hardware plants. To this end, a generator that produces executable PLC code is an inherent part of our approach. In contrast to other approaches the generated code is not intended to realize certain almost deterministic sequences like chemical receipts but keeps close to the actual intention of SCT, namely the supervision of a given system. Consequently, in our approach the actual controller is considered to be given, either by a conventionally written program or by manual operation. This leads to a total of three acting instances: The (physical) plant, the (manually written) controller and the (synthesized) supervisor. The task of the latter is to keep the plant in a state space that is regarded as safe, independently from what the controller does. Accordingly, there are three types of events, one for each respective actor. These are the classes of *controllable events*, which are triggered by the controller and can be blocked by the supervisor, the type of *uncontrollable events*, which are associated with certain happenings detected by sensors in the plant, and in addition to the "traditional" types the *forcible events*. Those can be released by the supervisor itself in order to avoid future uncontrollable events without cutting off a whole branch in the state space.

We develop a tool that provides a graphical, Eclipse-based automaton editor for modeling and generates a framework where existing control sequences can be embedded in order to operate a real, physical plant. A signal and event generator performs the necessary translations between supervisor, controller and the I/O ports of the PLC that are connected to the plant. The entire framework is executed on the target PLC, where it emulates the supervisor and this way ensures a safe behavior.

---

[1] P. J. G. Ramadge and W. M. Wonham: Supervisory Control of a Class of Discrete Event Processes, in *SIAM Journal on Control and Optimization*, 1987.

1.4 Invariant Generation for Probabilistic Programs

Friedrich Gretz (`fgretz@cs.rwth-aachen.de`)
Supervisor: Prof. Dr. Ir. Joost-Pieter Katoen

Probabilistic programs are sequential programs where choices can be made not only depending on some condition but also randomly. Such random behaviour is interesting in several areas of computer science. To mention a few applications: random choices can make the worst-case runtime of an algorithm unlikely, many modern cryptographic methods rely on randomisation and finally randomisation is used in distributed systems as a symmetry breaking mechanism. In the last decade, the verification of probabilistic programs has received a lot of attention, and has mainly been focused on automated verification techniques, known as model checking, that verify safety and liveness properties by systematically checking all states of the underlying operational model of such probabilistic program. These techniques are typically restricted to models in which all probabilities are explicitly given. In probabilistic programs, however, the probabilities are parameters, and one is interested in general statements about correctness, i.e., properties that contain these parameters.

In order to deal with such properties, deductive verification methods for probabilistic programs have been developed. McIver and Morgan defined annotations and transformer semantics for a probabilistic language as an analogue to Dijkstra's weakest liberal precondition semantics. The key to prove a program's correctness is the discovery of so-called invariant annotations (or invariants for short). Invariants provide very general verification results, but are difficult to find. This is true for sequential programs in Dijkstra's setting, but the fact that invariants for probabilistic programs are quantitative, makes the search for invariants for this class of programs substantially harder.

In our research project we try to synthesise invariants for probabilistic programs. Currently, our method requires a user to provide a program and additionally a so-called template. This template predefines the "shape" of the desired invariant, i.e. it is an annotation with unknown parameters. Our approach is then to find constraints over these parameters that describe invariant instances of this template. We build upon a constraint-based technique which guarantees that for a given template we will find *all* its invariant instances. A software prototype tool called PRINSYS ("PRobabilistic INvariant SYnthesiS") is developed that demonstrates the applicability of our work on several examples.

Currently, our methods are tailored to specific subclasses of programs and invariants. In the future we would like to overcome some of these restrictions.

1.5 Model Synthesis through Transformations

Katrin Hölldobler (`hoelldobler@se-rwth.de`)
Supervisor: Prof. Dr. Bernhard Rumpe

In model driven development it is common to use models in several modeling languages to describe the different parts of a system being developed. While developing, maintaining and evolving a system these models need to be transformed in various ways. Model transformations can be seen as the automatic generation of target models from source models according to transformation definitions[1]. A transformation definition consists of a set of transformation rules describing how a target model is derived from a source model. These transformations can be, e.g., complex edit operations, structural refactorings or refinements. Furthermore, model synthesis within code generation[2] or reverse engineering could be done by model transformations.

Common model transformation approaches define transformations using the abstract syntax of the modeling language whereas only some approaches also reuse the concrete syntax to allow modeling transformations in a more intuitive way. We call such a transformation language domain specific.

We are interested in the automatic generation of domain specific transformation languages (DSTL) based on modeling languages. This approach combines the advantages of generating a transformation language and using a domain specific language. A modeler using a DSTL is able to define model transformations in an intuitive way as he is already familiar with the concrete syntax of the modeling language. Furthermore, this language should be generated to prevent the modeler from implementing a transformation language for every modeling language used.

A transformation engine to generate a DSTL using the grammar of the modeling language was developed by our group[3]. It supports transforming one source model to exactly one target model within the same language.

For model synthesis, this approach needs to be extended such that multiple input or output models can be used, e.g., to combine class diagrams to generate code. This research focuses on the generation of DSTLs for different modeling languages as well as on the development of concrete DSTLs for structural languages such as class diagrams and architecture diagrams. These DSTLs will be generated and extended to address even more domains-specific needs and thus allow an intuitive way of modeling (model) synthesis.

---

[1] A. G. Kleppe, J. Warmer, and W. Bast. MDA Explained: The Model Driven Architecture: Practice and Promise. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2003.

[2] B. Rumpe. Agile Modellierung mit UML. Xpert.press. Springer Berlin, 2nd edition, March 2012

[3] I. Weisemöller. Generierung domänenspezifischer Transformationssprachen. Aachener Informatik-Berichte, Software-Engineering. Shaker, 2012.

1.6 Graph-based Abstraction of Pointer Programs

Christina Jansen (`Christina.Jansen@cs.rwth-aachen.de`)
Supervisor: Joost-Pieter Katoen, Thomas Noll

Dynamic data structures such as lists and trees, implemented using pointers, are heavily used in e.g. all kinds of application software, but also device drivers, operating systems, and so forth. While pointers offer a flexible concept allowing for very complex program behaviour, pointer programming is error-prone, even being one of the most common sources of bugs in software[1]. Typical problems are dereferencing of null pointers, creation of memory leaks, unsought aliasing effects and the accidental invalidation of data structures through destructive updates , i.e., errors which are usually difficult to trace. However, with the flexibility of pointer programs comes the complexity of analysing them, as they generally induce unbounded state spaces. A common approach to tackle this problem is to apply *abstraction techniques* to obtain a finite representation.

We utilise hyperedge replacement grammars (HRGs) as an intuitive concept for defining and implementing such abstractions[2]. The key idea is to represent heaps as hypergraphs that contain placeholders indicating abstracted fragments of a data structure. Thus they combine concrete and abstract heap parts. Placeholders are realised by deploying *hyperedges*, i.e., edges that connect an arbitrary number of nodes, labelled with nonterminals. The semantics of the nonterminals, i.e. the kind of data structure they represent, is specified by HRGs. Abstraction and its reverse operation, concretisation, are implemented by applying grammar rules in forward and backward direction, respectively.

In this PhD research we develop sound HRG-based abstractions for intra-[3] and interprocedural[4] as well as concurrent programs. Moreover the relationship to Separation Logic[5], a well-established technique for analysing pointer programs, and the integrativeness of both approaches[6] is investigated.

---

[1] P. Fradet and R. Gaugne and D. Le Metayer, Static Detection of Pointer Errors: an Axiomatisation and a Checking Algorithm (ESOP 1996)

[2] J. Heinen and T. Noll and S. Rieger, Juggrnaut: Graph Grammar Abstraction for Unbounded Heap Structures, Proc. 3rd Int. Workshop on Harnessing Theories for Tool Support in Software (TTSS 2009)

[3] J. Heinen and C. Jansen, Juggrnaut - An Abstract JVM, 2nd Int. Conf. on Formal Verification of Object-Oriented Software (FoVeOOS 2011)

[4] C. Jansen and T. Noll, Generating Abstract Graph-Based Procedure Summaries for Pointer Programs, Graph Transformations (ICGT 2014)

[5] J. C. Reynolds, Separation Logic: A Logic for Shared Mutable Data Structures, IEEE Symposium on Logic in Computer Science (LICS 2002)

[6] C. Jansen and F. Göbe and T. Noll, Generating Inductive Predicates for Symbolic Execution of Pointer-Manipulating Programs, Graph Transformation (ICGT 2014)

1.7 Information Management in Systems of Systems

David Kampert (`kampert@plt.rwth-aachen.de`)
Supervisor: Ulrich Epple

The term "system of systems" (SoS) is attributed to systems in which each constituent system is an autonomous and operational unit of its own, but all these units work in a coordinated fashion. Examples are production plants, electrical power grids, logistics networks etc. The operation of an SoS can potentially be vastly improved on the coordination level.

Several definitions of "system of systems" have been proposed. The definitions agree to the extent that the following characteristics are met by an SoS:
1. The constituent systems have operational and managerial independence.
2. The definition and the configuration of the global system are evolutionary in nature.
3. There may be emergent behavior in the global system.
4. The constituent systems are geographically distributed.
The European Union's project DYMASOS (DYnamic Management of physically coupled Systems Of Systems) specifically addresses SoS that are coupled by flows of matter or energy. The goal is the development and validation of new methods for optimized coordination of physically coupled SoS (with respect to operational costs). Two major challenges exist: The first challenge is the development of suitable coordination methods. Different methods are investigated for this purpose: population control, marked-based coordination and coalitional control. The second challenge concerns the validation and the integration of the coordination methods into real-world systems. Both validation and information management are crucial for the long-term application of coordination methods. In particular, SoS undergo continuous modifications which have to be taken into account in the coordination system in an automated fashion. Otherwise, the effort for updates may soon become prohibitive since a vast number of mutually dependent aspects of the technical environment require consideration.

A corresponding software tool for management of information in an SoS was developed as part of the project. The tool collects information from the running SoS, e.g. by retrieving data from automation systems. The information affects the physical system structure, hierarchical control dependencies and value-based data. This set of information serves as an input to a co-simulation framework where the SoS is simulated as a whole and the coordination strategies can be tested. The co-simlation simulation framework is a second tool that is also developed in the project. Ultimately, the tools will be evaluated in a real-world case study at a chemical production site.

1.8 Solving Nonlinear Integer Arithmetic in Satisfiability Modulo Theories Using Cylindrical Algebraic Decomposition

Gereon Kremer (gereon.kremer@cs.rwth-aachen.de)
Supervisor: Erika Ábrahám

Satisfiability Modulo Theory (SMT) solving is a technique to decide the satisfiability of a propositional formula that is enriched with some theory. SMT solvers usually uses a satisfiability (SAT) solver to check the boolean structure and a theory solver to check the resulting conjunctions of theory atoms. There are several flavors of arithmetic theories that include arithmetic variables and operations, namely linear real (LRA), linear integer (LIA), *nonlinear real* (NRA) and *nonlinear integer arithmetic* (NIA). They allow to model applications at a comparatively high level of abstraction.

While the linear logics are well studied and can be solved efficiently, nonlinear arithmetic remains a challenge in practice, especially as NIA is undecidable in general. Our tool SMT-RAT[1] aims to solve these logics. With the *cylindrical algebraic decomposition*[2] (CAD), a complete decision procedure for NRA exists that has proven to be fast enough to be practically useful.

Although most industrial solvers tackle NRA and NIA using linearization, we developed several techniques to use the CAD method for NIA solving. The CAD tries to find a solution by selecting sample points that are constructed dimension by dimension. We make sure that we select integral samples, if there exists an integer sample for the current dimension. This already suffices to produce integer solution for a fair amount of benchmarks.

If there are multiple integer samples for a dimension, some may lead to a fully integral solution, while others yield a rational solution. One possibility is to use *multiple of these samples* for lifting, another is to add a *backtracking* mechanism within the sample point construction. Note that both approaches become infeasible if the number of possible samples grows.

Another possibility is to adapt *branch and bound*, commonly known to solve LIA using the simplex algorithm. Branch and bound uses another method to calculate a real solution. If this solution happens to be integral, the solution is returned. If some assignment is rational, branch and bound introduces a *split that can be lifted to the SAT solver*. We apply this idea to NIA and use the CAD method to calculate real solutions.

---

[1] Florian Corzilius, Ulrich Loup, Sebastian Junges and Erika Ábrahám. "SMT-RAT: An SMT-Compliant Nonlinear Real Arithmetic Toolbox" in *Theory and Applications of Satisfiability Testing – SAT 2012*.

[2] George E. Collins. "Quantifier elimination for real closed fields by cylindrical algebraic decompostion" in *Automata Theory and Formal Languages 2nd GI Conference, LNCS Volume 33, 1975, pages 80–90*.

1.9 Optimization of capacitive load for railway networks

Christian Meirich (`meirich@via.rwth-aachen.de`)
Supervisor: Univ.-Prof. Dr.-Ing. Nils Nießen

The German state is giving about 3.9 Billon.-Euro each year to the DB group to preserve the railway tracks in a defined condition (LuFV II). In order to control whether the money is used reasonably the German Railway Authority (Eisenbahnbundesamt) has to check the conditions.

This background is a motivation to optimize the capacitive load in the field of railway operation research. Especially there are approaches of the strategic network planning in the field of the (German) Federal Transport Infrastructure Plan. A plan like this is a comprehensive compilation of the German government for investments in the infrastructure for several carriers of traffic. Main topics are generation and restraint of traffic or a detection of bottlenecks.

Till this day there are two main methods to detect an infrastructural default or a bottleneck. On the one hand it can be detected by longer (theoretical) travel times for a train run. On the other hand, it can be counted by an existing list with the number of infrastructure defects. If the number of defects increase, the state of the infrastructure will deteriorate. In addition to the existing procedures the state of the infrastructure should be validated by a new parameter. In this consideration the new parameter is the capacity of the railway network.

Reducing the number of train runs on a railway section could be a valuable way to deal with an existing bottleneck, as leading trains on other paths reduces the number of trains on a specific railway line or a node. However, fixed and necessary stops of passenger trains increase the complexity of changing a whole path. Otherwise, in the field of freight trains it can be useful to change a path to alternative ways with lower workloads. In this case capacity reserves could be used to unload a bottleneck area.

Today the capacity of railway lines as well as the capacity of railway nodes can be calculated by means of analytic algorithms. Currently there is no generally accepted method to allocate the key figures of lines and nodes. Due to this, a single parameter to describe a railway networks capacity cannot be calculated so far.

The scope of the work will be to investigate whether it is possible to define one single parameter "capacity" for the whole railway network. The goal is, to find an adequate algorism to maximize the capacity in respect of the number of train runs and their relations for a whole railway network. The comparative value should be the capacity and as a consequence it will be possible to detect bottlenecks in such networks and synergy effects of expansions could be visualized.

1.10 Online Analysis for PLC Programs

Mathias Obster (`obster(at)embedded.rwth-aachen.de`)
Supervisor: Univ.-Prof. Dr.-Ing. Stefan Kowalewski

Programmable logic controllers (PLCs) are used in process control and automation control scenarios. They control electromechanical processes in chemical, power or production plants and other private or public facilities. Programs for these devices are written in languages defined in the IEC 61131-3 standard. Since failures in processes controlled by PLCs can lead to harm and financial loss, the interest in correct programs is high. Formal methods such as static analysis can help validate these programs and are implemented into the Arcade.PLC[1] framework for this purpose.

Classical static analysis is applied on programs considered to be complete and syntactically correct with respect to the grammar. This approach is not yet suitable to caution against errors at development time or to give hints regarding program behaviour while the programmer or technician still writes the program. Supporting hints for the programmer include value set information as well as dead code, reassignment and division by zero warnings.

Static analysis at development time and continuous refinement of the analysis result for new input, which is called online analysis, divides into three subtasks: First, the code written so far has to be parsed while it is not yet syntactically correct. A common parser technique is called parser recovery, which deals with input not conform to the language's grammar. These techniques however have practical limitations, which is why another class of grammars and parsers will be evaluated for this purpose. Parsing expression grammars allow the specification of ambiguous derivation rules to declare unfinished words of the input language to be grammatically correct and thereby parsable. The second subtask is the semantical analysis while not all information like imports and definitions can be resolved. Without limiting the generality of already written parts of a program, worst-case assumptions and null-values can be a temporary replacement to reuse already existing analysis methods. As a last part, the effort for reevaluation after adding new code will be dealt with. One approach to deal with this is to store intermediate results between analysis cycles and only take account of code affected by the newest modification.

Results of this work will be integrated into the Arcade.PLC framework to benefit from and extend existing methods for static analysis of PLC programs.

---

[1] S. Biallas, S. Kowalewski and B. Schlich, "Range and Value-Set Analysis for Programmable Logic Controllers", in *Proceedings of the 11th International Workshop on Discrete Event Systems*, 2012, pp. 378–383.

1.11 Formalization of the specification framework FOCUS in the theorem prover Isabelle

Deni Raco (`raco@se-rwth.de`)
Supervisor: Prof. Dr. Bernhard Rumpe

The goal of this thesis is the creation of a framework for the verification of distributed, asynchronous communicating systems based on domain theoretical concepts. Distributed systems exist in many different forms, such as in telecommunication networks, web applications etc. They usually consist of components cooperating and exchanging information through interaction. The development of distributed systems is complex and error prone. Precise and detailed system behavior descriptions are therefore needed. For the formal specification and stepwise development of distributed systems we use the specification framework FOCUS[1]. The key concept of FOCUS is the stream, which is a sequence of messages flowing on unidirectional channels. In our approach distributed systems are formalized using the specification framework FOCUS and embedded in the theorem prover Isabelle[2]. Isabelle is an interactive, semi-automatic theorem prover tool for creating and checking mathematical proofs. Its syntax is similar to functional programming languages. Mathematical constructs are described in a formal language and their properties can be verified. The main proof method of Isabelle is a version of resolution based on higher-order unification. We validate the Isabelle theories by using them to specify examples of distributed systems such as the Alternating Bit Protocol and verifying properties about the system.

---

[1] [BS01] Broy, Manfred ; Stolen, Ketil: Specification and Development of Interactive Systems - FOCUS on Streams, Interfaces, and Refinement. Springer-Verlag, 2001 (Monographs in Computer Science)

[2] [NPW02] Nipkow, Tobias ; Paulson, Lawrence C. ; Wenzel, Markus: Lecture Notes in Computer Science. Bd. 2283: Isabelle/HOL - A Proof Assistant for Higher-Order Logic. Springer-Verlag, 2002

1.12 Mechanism Design for Combinatorial Auctions

Andreas Tönnis (`toennis@cs.rwth-aachen.de`)
Supervisor: Prof. Dr. Berthold Vöcking

Combinatorial auctions are a form of weighted set packing problems which is, in general, a hard class of problems. Bidders assert a valuation to items and there is a constraint on the maximal occurrences of the items. A solution is an assignment of the items to the bidders, so that the social welfare is maximized, while no packing constraint for an item is violated. The social welfare is defined as the total value over all bidders. Now, in mechanism design people go one step further. The valuation functions are only known to the bidders themselves and all bidders act in a selfish manner. Therefore, if a bidder assumes he can improve his personal outcome by lying about his valuation, then he will do so. In mechanism design, we construct algorithms that are truthful, meaning bidders maximize their outcome by telling the truth about their valuation. A common technique is to introduce prizes on the items in such a way that any bidder maximizing his utility (the difference between his valuation for a set of items and the prize on this set) also maximizes the social welfare incurred by the mechanism.

Currently, we work on approximating online combinatorial auctions. In this type of online problem, it is assumed that the items to be sold are known at the start of the algorithm. Then the bidders arrive at runtime and the algorithm has to allocate them one or more items before the next bidder arrives. In the most simple form, when there is only a single item, this problem is the well known secretary problems. If there are more items, but every bidder is bound to only receive a single item, then the problem corresponds to the bipartite vertex-at-a-time matching problem. Now in the general online combinatorial auction problem, we lift the bidders constraints on the size of the sets of items and introduce multiplicities on the items. We have an optimal algorithm for the online vertex-at-a-time matching problem and online combinatorial auctions [1].

Furthermore we consider generalizations towards packing linear programs, where we assume that the columns arrive online and correspond to a bidders desired bundle. We either allocate the bundle to him or we discard it in an online fashion. We achieve an optimal algorithm for packing linear programs with sufficiently large right-hand sides in the packing constraints [2]. Currently we extend these results towards online list scheduling and secretary problems with submodular objective functions.

[1] T. Kesselheim, K. Radke, A. T. and B. Vöcking, An Optimal Online Algorithm for Weighted Bipartite Matching and Extensions to Combinatorial Auctions, ESA 2013, pages 589-600

[2] T. Kesselheim, K. Radke, A. T. and B. Vöcking, Primal Beats Dual on Online Packing LPs in the Random-Order Model, STOC 2014, pages 303-312

2 GRK 1324/3: METRIK

Prof. Dr. Joachim Fischer
Email: fischer@informatik.hu-berlin.de
Humboldt-Universität zu Berlin
Internet: http://www.gk-metrik.de

In its expiring financing period the Graduate College METRIK continues the cooperation of computer scientists and geo-scientists in Berlin and Potsdam by joint exploration of a particular type of wireless communication and cooperation of computer systems. By the implementation of principles of self-organisation and by using inexpensive (but wide-spread) sensors, the Graduate College will reach for new horizons in the development of geo-specific monitoring, information and alerting systems to analyse the environmental processes in space and time. 51 PhD projects have been started since its launch in October 2006. This impressive number was possible because additional doctoral financing could be obtained from other accompanying externally funded projects of the involved metric doctoral supervisor. In the first phase of the Graduate College a number of technologies developed within METRIK have also been applied to METRIK-related projects (funded by the EU and the BMBF) of the German GeoForschungszentrum Potsdam to implement prototypical monitoring systems. One of the most compelling applications of interdisciplinary collaboration was the model-based development of a new earthquake early warning system for the highly seismic vulnerable region of Istanbul. Meanwhile, the technology is used in an adapted form for monitoring of historically valuable buildings and major infrastructure in other earthquake-prone countries in Asia. In the second phase the METRIK technologies were consolidated and expanded. Aspects of security, mobility of sensors in form of wireless communicating flying robots, dynamic adjustment of the system in terms of the current traffic flow through intelligent change of frequency bands for data transmission or type of communication and voting rules in the cooperative interaction between the service providers have been investigated. In addition, solutions for dealing with large quantities of captured sensor data were taken into account. For this reason, the Graduate College is in deep cooperation with the DFG Research Group "Stratosphere" to investigate how this complex information data management can be implemented using "Cloud Computing". In the final phase of METRIK are issues in processing, which are thematically oriented to IT requirements for Smart Cities, where on a number of promising cooperation in the transport and lighting management in Berlin-Adlershof are already under way.

2.1 Robotic Self-Exploration and Acquisition of Sensorimotor Primitives

Oswald Berthold (`bertolos@informatik.hu-berlin.de`)
Supervisor: Prof. Dr. Verena V. Hafner, Prof. Dr. Björn Scheuermann

Problem statement

The success of a robot and its behaviour, independent of any concrete task, is intimately tied to its sensorimotor capabilities. These serve to generate behaviour based on coordinated motor signals that are in turn shaped by the information taken in from the environment. Since explicitly programming these capabilities is not feasible, the robots need to be able to acquire and refine them through continued self-exploration.

The problem then can be stated as follows: Considering a robotic system with a given set of sensors, motors and inherent dynamics, find a function that maps sensor inputs onto motor outputs such that a cost function defined on the sensor inputs is minimized.

Approach

I combine methods from Developmental Robotics (DR) with those of Reinforcement Learning (RL). A prominent concept in DR is that of *internal models*. This means that an agent builds an internal model of the dependency of sensory states on previous motor actions and exploits the model for reaching self-generated or externally imposed sensory goals. Such a model, together with its context is what I refer to as a *sensorimotor primitive* in my work. My approach inherently combines online learning of relevant features based on sensory statistics with closed-loop learning of control policies. My approach is inspired both by neuroscientific principles as well as behavioural evidence regarding related processes in the development of animals.

We have successfully applied this approach to vision-guided motion control of a flying robot [1], unsupervised acquisition of a camera exposure control policy[2], feature learning for egomotion estimation from optical flow fields[3] and acquisition of behaviour on simulated [4] and real [5] robots.

---

[1] Berthold, Hafner, (2013), Increased Spatial Dwell-Time for a Hovering Platform Using Optical Flow, Technical Report

[2] Berthold, Hafner, (2013), Unsupervised learning of camera exposure control using randomly connected neural networks, 2nd RED-UAS Workshop, Compiegne, France

[3] Berthold, Hafner, (2014), Unsupervised learning of sensory primitives from optical flow fields, Proceedings of the Simulation of Adaptive Behaviour Conference, Springer 2014

[4] Berthold, Hafner, (2013), Neural sensorimotor primitives for vision-controlled flying robots, IROS'13 Workshop on Vision-based Closed-Loop Control and Navigation of Micro Helicopters [...], Tokyo, Japan, `http://rpg.ifi.uzh.ch/docs/IROS13workshop/Berthold.pdf`

[5] Berthold, Hafner, (2015), Closed-loop acquisition of behaviour on the Sphero robot, Accepted for European Conference on Artifical Life (ECAL) 2015 Conference, York, UK

2.2 Self-Organization in Networks of Mobile Sensor Nodes

Christian Blum (`blum@informatik.hu-berlin.de`)
Supervisor: Prof. Dr. Verena V. Hafner, Prof. Dr. Joachim Fischer

Self-organized wireless multihop (ad hoc) networks can form an easily deployable, robust and reconfigurable communication infrastructure, which can be employed for example in a disaster scenario, when static communication infrastructure has been destroyed. Furthermore, the paradigm of the Internet of things will add network capabilities to many objects, often via wireless interfaces enabling machine-to-machine communication creating a wireless network. As such wireless networks use the air as a shared physical medium, the parameters of these networks often show very space- and time-varying noisy characteristics. Intelligent robotic network nodes can overcome these problems posed by these dynamics and measurement noise by exploiting sensorimotor interaction. By actively shaping the sensory information by moving the robot in the wireless environment, complexity can be reduced.[1]

Several algorithms for single robots for network exploration in wireless networks[2] as well as gradient-based navigation[3] for different robot platforms have been successfully designed, simulated, implemented and evaluated for indoor as well as outdoor use. Additionally, an internal model-based meta-algorithm to solve tasks like finding a node or bridging two nodes has been developed and implemented experimentally in an indoor scenario.

For the case of multiple robots, i.e., a swarm of wirelessly connected robots, a lot of interesting algorithms for example for optimal placement of mobile network nodes have been developed. However, none of them are being used in real world scenarios. One of the reasons for that is insufficient safety and fault tolerance of naive algorithms. To overcome this problem the use of an internal model-based architecture using an internal simulation has been investigated in multi-robot scenarios to enhance the safety of these systems, making them more suitable for real world use.

Two test scenarios have been investigated using this architecture: In the first experiment a robot had to prevent other robots from coming to harm while ensuring its own safety and fulfilling a task [4]. In a second experiment, a robot had to navigate through a narrow corridor without colliding with other robots. The proposed architecture has been shown to be very effective.

---

[1] C. Blum and V. V. Hafner, *An Autonomous Flying Robot for Network Robotics*, Proceedings of the 7th German Conference on Robotics (ROBOTIK 2012), pp. 36-40, Munich (2012)

[2] C. Blum and V. V. Hafner, *Robust Exploration Strategies for a Robot exploring a Wireless Network*, Workshop SACS/SoCoDiS – NetSys – KiVS 2013, Stuttgart (2013)

[3] C. Blum and V. V. Hafner, *Gradient-based Taxis Algorithms for Network Robotics*, arXiv:1409.7580 [cs.RO], (2014)

[4] A. F. T. Winfield, C. Blum, and W. Liu, *Towards an Ethical Robot: Internal Models, Consequences and Ethical Action Selection*, Advances in Autonomous Robotics Systems. Springer International Publishing, pp. 85-96, (2014)

2.3 Event Pattern Matching

Dr. Bruno Cadonna (`cadonna@informatik.hu-berlin.de`)

The goal of my research is to design, develop and evaluate new methods for event pattern matching. Event pattern matching is a query technique where a stream of events is matched against a pattern. The output is a set of matches. An event is a data item with a timestamp that represents its occurrence time. Examples of events are the administration of a medication to a patient, the trade of shares in stock markets, or the measurement of a sensor. Events in a stream are chronologically ordered by occurrence time. A pattern specifies constraints on chronological order, temporal extent, attribute values, and quantification of matching events. Matches contain events from the stream that satisfy the constraints specified in the pattern. Event pattern matching is widely applicable in different domains such as RFID-based tracking and monitoring, RSS feed monitoring, health services, sensor networks and workflow monitoring.

Besides the pattern, event pattern matching algorithms use a selection strategy to adapt the result to application-specific needs. The selection strategies that have been proposed restrict the set of matches based on the positions of the matching events to each other. For example, a selection strategy may specify to find only matches whose events are contiguous in the stream or matches with events that occur earliest after the start of the match. We investigate a selection strategy that detects the top k matches that maximize a scoring function over the matching events rather than considering the positions of matching events. Such a selection strategy allows to find matches depending on the contents and the number of matching events. For example, to find the most probable matches in a stream with uncertain events the product of the likelinesses of matching events is maximized. In another example that uses a pattern that specifies a variable number of matching events (e.g. Kleene plus), the sum of the events in a match is maximized to find the matches with the most events.

In some scenarios, even domain experts do not know how to specify a pattern that precisely describes a situation from the real world one wants to detect in a stream. We investigate methods to automatically learn patterns by analyzing historical event traces. The input to this problem is a set of historical event traces labeled where the situation of interest occurred. The output is a pattern, that can be used to detect situations of interest in streams. Our approach uses supervised learning techniques to infer the constraints specified in the pattern such as the events involved, their order, and the constraints on the attribute values.

2.4 Information Extraction for Disaster Management

Lars Döhling (`doehling@informatik.hu-berlin.de`)
Supervisor: Prof. Dr. Ulf Leser, Prof. Dr. Doris Dransch

Year after year natural disasters like floods or earthquakes are striking our planet. After such events, decision makers require precise and timely information to assess damages and to coordinate relief operations. Understanding "the big picture" in emergency situations, a construct referred to as situational awareness (SA), is presumably a prerequisite for effective responses. More and more, SA-supporting information can be found in textual form on the Internet, both in conventional sources like newspapers[1], as well as in social networks like Twitter. These sources offer among the most detail information available, but searching them manually is a time-consuming and therefore costly task.

Information Retrieval (IR) deals with the problem of finding documents relevant for a given request within a set of documents. Web search engines are a prominent example of IR-applications today, used to search efficiently the overwhelming number of documents on the Web. While IR searches relevant documents, Information Extraction (IE) studies the problem of automatically extracting structured information from given unstructured text. Methods in IE build on a multitude of different techniques, including pattern matching, natural language processing (NLP) and machine learning.

We suggest treating the problem of finding relevant pieces of information within documents as a combined IR / IE problem. Such information snippets, forming n-ary relationships, may include temporal and spatial attributes. Clearly, this requires specific solutions because those relations typically contain incomplete tuples or ones spanning multiple sentences. Dealing with automatically extracted information also leads to the problem of inconsistent results, due to different sources, points in time or granularities. Furthermore, addressing web content carries the danger of ungrammatical texts, which might break NLP methods.

Considering crisis events like earthquakes, the question arises: How may modern IR and IE techniques contribute to situational awareness? This can be refined as: (I) What methods are best for finding event-relevant documents, especially for Web data sources which are solely accessible by HTML-based search interfaces? (II) Which IE methods are the most appropriate ones to analyze textual messages in the context of natural disasters?

Even though there are established methods for IR / IE, they need to be adapted for the target domain.

---

[1] Döhling, L. and Leser, U. (2011). EquatorNLP: Pattern-based Information Extraction for Disaster Response. In Proceedings of Terra Cognita 2011 Workshop, Bonn, Germany.

2.5 Efficient Multi-Domain Similarity Search on Big Data

Fabian Fier (`fabian.fier@informatik.hu-berlin.de`)
Supervisor: Prof. Johann-Christoph Freytag, Ph.D.

Web data becomes increasingly structured. Semantic markup like schema.org allows websites to enrich their contents with standardized metadata describing them semantically. Semantic information allows to dramatically improve web search, which is currently only a textual search. The search process is cumbersome for two reasons: First, users have to anticipate which keywords might appear on websites that are interesting for them. Second, users cannot easily navigate between websites that are intuitively "similar". Consider a novel kind of web search that allows users, starting from one current website, to find other (potentially similar) websites. For the currently opened website, the user can see its attributes and their values, which originate from the structured data on the site. The user chooses query attributes that are relevant for him. He can keep or modify their values in order to issue a new web query that finds results that are similar to the values of the chosen attributes. From a database perspective, such a novel kind of web search requires to efficiently process similarity search queries with attributes of multiple domains on large datasets. Considering the two domains time and location, there are numerous approaches to process queries with either time or location separately. There exist further approaches on how to efficiently process queries that involve time and location together. What happens if another attribute from a different domain is added to the query, like text? To our knowledge, there is no systematic way to efficiently deal with similarity search queries involving attributes from an arbitrary number of differing domains. We plan to create a generic framework to perform similarity searches with multiple attributes of different domains on large datasets efficiently.

2.6 Automated Pattern Learning for Event Pattern Matching

Lars George (`lars.george@informatik.hu-berlin.de`)
Supervisor: Prof. Dr. Joachim Fischer

Everyday we are faced with various events. For example, it starts raining, smoke is detected, or the temperature increases. The occurrence of such real life events can be represented as programming entities in computing systems. These event entities have attributes like precipitation rate, oxygen content, temperature, and occurrence time. Combinations of primitive events can describe situations of interest, also known as complex events. For example, a complex event *fire* consists of a smoke event, multiple temperature events with increasing values above 40 degrees, and the absence of rain events. To detect complex events we can use event pattern matching. Event pattern matching is a query technique where patterns specify constraints on extent, order, values, and quantification of events. Example applications for event pattern matching are monitoring in sensor networks, health monitoring applications in a hospital, and RFID-based tracking applications. Patterns are usually described with pattern matching languages such as Esper, SES and SASE+. The description of a situation of interest with pattern matching languages is not always trivial and often involves a combination of several events and attributes with constraints that even domain experts may not know.

The goal of my dissertation is to develop techniques to automatically learn a pattern that precisely describes a situation of interest from historical event traces. The input is a set of historical event traces labeled where the situation of interest occurred. The output is a pattern in a generic format, that can be transformed into a given pattern matching language to detect future situations of interest. My approach is to use supervised learning techniques to infer the constraints of the pattern such as the events involved, their order, and constraints on the attribute values of the involved events. I distinguish between properties and relationships of a constraint. Property constraints of attribute values are against constants and relationships describe relations between two attributes of events. Relationships can be used to describe trends in data such as an increase of temperature as described in the example above.

Automatic generated patterns can aid domain experts in finding the hidden causality between incoming events and a situation of interest. I apply my solution to different domains. I label the data by using a given pattern and an existing event pattern matching language. The evaluation of the quality of the learned pattern is done by comparing the found situations of interest after using the given pattern and the learned one. This approach is used to evaluate the precision of the learning process on real world data.

2.7 Model-based Testing of Variant-Rich Software Systems

Hartmut Lackner (`lackner@projektbetreuung.de`)
Supervisor: Prof. Dr. Holger Schlingloff

A trend of our time is that consumers tend to favor customizable products, because they want to gain the highest benefit for the costs. Thus, systems become more complex and have more features in different variants while at the same time a high level of quality has to be maintained. One prominent example for this is the German automotive industry where for current car models, on average, each car configuration is produced only once. Similar, earthquake warning system share commonalities, but at the same time, each of them is tailored towards its target environment. As a result, system engineering processes face challenges mainly focused at requirements engineering for multi-variant systems and quality assurance, e.g. by testing.

The interaction between both phases, requirements engineering for multi-variant systems and testing, is a key concern for engineering software product lines of high quality. Two significant complexity drivers located in these phases are the growing number of product variants that have to be integrated into the requirements engineering and the ever growing effort for manual test design. There are modeling techniques to deal with both complexity drivers separately like, e.g., variability modeling and automated test design. Their combination, however, has been seldom the focus of investigation.

We introduce a process for efficient and effective design of product line tests. Our approach for integrating variability modeling and automated test design relies on preserving variability throughout the test design phase until test execution is imminent. This enables us to select the products for testing *after* tests have been designed. On this basis, we define new coverage criteria for selecting products from test cases, e.g. a minimal/maximal set of products for executing each test case once. For interoperability reasons, we employ standard modeling techniques in all the stages for software product line engineering and automated test design, which enable reuse with many commercially and freely available tools.

Our approach enables us to select products for testing with new intentions, e.g., the fewest or most products for executing all tests once. The recently developed SPL mutation system enables qualitative test assessment. Furthermore, it prepared the ground for new research on fault propagation in SPL Engineering.

2.8 Spatial Active World Modeling for Autonomous Mobile Robots

Heinrich Mellmann (`mellmann@informatik.hu-berlin.de`)
Supervisor: Prof. Dr. Verena Hafner

In the near future we will see more and more robots entering our lives, for instance as members of the smart cities or helpers in disaster situations. Imagine a group of autonomous heterogeneous robots is exploring a disaster area, where the robots coordinate themselves to efficiently cover the area depending on the local situation and the capabilities of the particular units. This task requires for each robot to be able to create and maintain an adequate representation of the spatial structure of the surrounding environment enabling the robot to make predictions concerning the results of its possible actions and to explain the results of the past actions. To achieve this the robot needs to actively *collect* and *integrate* the information about its environment as well as to *infer* not directly observable information necessary to solve its task.

The incomplete and noisy sensor information leads to the uncertainty in the robots' belief of the world. Generally, we can differ between two qualitatively different sources of uncertainty: the *noise* in the sensory input, in particular false perceptions; and *ambiguity* in the interpretation of the sensor readings, i.e., there is not enough information to determine a complete model. Noisy or false perceptions may lead to *inconsistencies* in the perception while *redundant* data from different sensors may be used to reduce uncertainty caused by noise. The robot might *actively* gather information to improve its spatial model. For that, it needs to know which parts of the model require an improvement and which actions have to be taken to achieve that. While those aspects are well studied in the related classical fields, e.g. signal processing, the requirement for a machine to act autonomously in a unconstrained dynamic environment defines a wholly new level of complexity.

This project aims to explore the fundamental principles of building and maintaining a situation model based on heterogeneous sensory data. For the investigations, the scenario of humanoid robot soccer is being used as the experimental environment. Here, teams of humanoid robots equipped with a number of sensors like directed camera, gyro, accelerometer etc. play soccer autonomously on a simplified soccer field. Thus, it provides an excellent experimentation framework for this project.

In the given scenario, the situation model needs to integrate partial information, allowing for local navigation and interaction with objects; deduce a global view if possible; forget unimportant or wrong parts, i.e., reinterpret information; store inconsistent information for later interpretation; decide which action should be taken to improve the model.

2.9 Parallel Analysis of High Dimensional Data Sets

Tobias Rawald (`trawald@gfz-potsdam.de`)
Supervisor: Prof. Doris Dransch

Recurrence Quantification Analysis (RQA) is a statistical method to quantify recurrent behaviour of dynamic systems, e.g., the Earth's climate system, captured in one or more time series. It is based on reconstructing a set of multidimensional vectors and comparing them regarding their mutual similarity. By employing a similarity measure and a neighbourhood condition, a binary similarity matrix (*recurrence matrix*) is created. If two vectors are considered to be similar, the corresponding matrix element is assigned with the value 1 (*recurrence point*) whereas dissimilar vectors are assigned with the value 0. The RQA comprises several scalar measures, quantifying small scale structures formed by recurrence points, such as diagonal and vertical lines.

Considering existing RQA computing approaches, each reconstructed vector is compared to every other vector in the set, resulting in a time complexity of $O(N^2)$. Furthermore, existing RQA tools are limited concerning the size of the matrices that can be be processed, e.g., 10,000 by 10,000 matrix elements. Our goal is to provide a computing approach that allows to process even very long time series ($> 1,000,000$ data points) in a reasonable amount of time.

In a first step, we developed an approach that divides the recurrence matrix into multiple sub matrices. The RQA measures rely on frequency distributions of diagonal and vertical lines. Hence, for each sub matrix individual histograms are created, which are further recombined into two global frequency distributions. Recognising the condition that a single diagonal or vertical line may spread over multiple sub matrices, we introduce additional data structures. The so-called diagonal and vertical *carryover buffer* store the length of lines at the horizontal and vertical borders of the sub matrices.

We provide several implementations of our *divide and recombine* approach using the *OpenCL* framework. They differ regarding the representation of input data, the materialisation of the similarity matrix, the representation of similarity values and the recycling of intermediate results. We discover that depending on the hardware platform selected for execution as well as the assignments of the parameters steering the properties of the recurrence matrix, the performance characteristics of each implementation varies drastically. Hence, we derive guidelines for selecting an appropriate implementation for a given computing environment.

An essential part of conducting RQA is the computation of mutual similarities of vectors in high dimensional space. This problem is of high relevance regarding other methods such as *k-nearest neighbour search*. We plan to adapt our computing approach to this method and to validate, whether it can compete with other optimisation strategies, e.g., the application of *index structures*.

2.10 Coupled Evolution in Model-based Domain-specific Language Development

Martin Schmidt (`schmidma@informatik.hu-berlin.de`)
Supervisor: Prof. Dr. Joachim Fischer

In the life cycle of software systems, evolution is a critical process. For prevalent software development scenarios an increasingly number of evolution tools and mechanisms are available and integrated into development environments for support changes. But most of the tools refer to only one formalism, e.g. refactorings in Java. Software systems nowadays are build up using different formalism that cover domain-specific challenges. Even if every formalism is used for solving a specific problem, these artifacts are related to each other in some cases. So there is a need for tools that support the *coupled evolution* of different parts of a software.

Domain-specific languages (DSLs), seen as software systems, are highly specialized computer languages. Like all computer languages, DSLs evolve. But in contrast to general-purpose languages this process is much faster. Since the introduction of model-driven engineering (MDE), it is possible to develop DSLs model-based. In this scenario different artifacts (e.g. metamodel, grammar, code-generator) describe the different aspects of the language (e.g. abstract syntax, notation, semantics). These artifacts form a system, where changes within one artifact demand the coupled evolution of other artifacts in consequence of changing user or technical requirements.

The goal of this work is to provide different methods for supporting coupled evolution in the field of model-based DSL development. Referring to existing taxonomies of software evolution different challenges exist, that need to be overcome. These challenges are not only about *how* to execute a change, but also about *when, where* and *what*.

How. In our previous work we developed a method to change the heterogeneous parts of a DSL. To solve this problem we use asymmetric bidirectional transformations on models - called *lenses*. Lenses are designed for ensuring consistency between one abstraction (view) and the corresponding model (source). For this purpose we adapt the lenses approach for multiple targets, which accord to the corresponding aspects of a DSL.

When. Our work focuses the support during the development process, where sequential changes have to be performed. In addition the changes concerns the source code of the DSL, so that it needs to be recompiled for the changes to become available.

Where, What. For changing the relevant parts it is necessary to identify the elements that need to be changed. For this purpose we add an abstraction layer to the different aspects of a DSL. On this layer we will execute queries for targeting the elements that will be changed.

2.11 Remote sensing-based approaches for modeling 3D vegetation information in urban areas

Johannes Schreyer (`johannes.schreyer@geo.hu-berlin.de`)
Supervisor: Prof. Dr. Tobia Lakes

While 3D information on cities has been frequently assessed in recent years, this is mainly limited to the built-up area. Such information for assessing the benefits and associated disservices like carbon sequestration or allergies caused by pollens are missing for most cities. New data and methods for calculating vegetation characteristics including remote sensing techniques offer large benefits for addressing this lack of information, comprising private and public space and being comparable in time and space. There are several approaches using very high resolution (VHR) data mostly coming from active airborne systems, however, their spatial coverage and temporal resolution is limited due to financial and time costs.

The aim of the ongoing project is to test state-of-the-art remote-sensing data for 3D vegetation assessment in urban areas that are tackling mentioned data problems and which are currently unexploited for this purpose. More specifically, two different techniques for assessing vegetation parameters on two spatial scales were chosen: 1) a low-cost unmanned airborne vehicle (UAV) generating 3D point cloud data for small scale assessments and 2) TanDEM-X data with a global coverage for assessing vegetation on a city scale. 1) In cooperation with the group of cognitive robotics, HU Berlin we currently test the assessment of information with two quadrocopters. We have iteratively modified and improved the settings according to results of several flight campaigns. Automatically selected and matched images were used to generate point clouds with delivering accurate information on sub- and above canopy vegetation. 2) On the level of a city or a metropolitan area there are only few systems that obtain high resolution 3D data with global coverage. The Satellite-based synthetic aperture radar (SAR) of the most recent Tandem-X mission derives a digital elevation model (DEM) with a resolution including components such as single or bundled trees for the entire earth surface in the upcoming years. The current work process aims to derive a normalized digital vegetation model (nDVM) using an intermediate TanDEM-X DEM and a vegetation/building layer from airborne UltraCam data within a morphological workflow for Berlin, Germany. For this purpose, several morphological filters are compared to detect vegetation in typical urban surroundings such as backyards or streets. Great forest-like vegetation, mostly in parks and allotments are assessed comparing results of an interpolation and a weighted morphological approach. Vertical and horizontal accuracy are validated using the UltraCam data and an official DTM for Berlin. At the same time, results of UAV field campaigns during 2014/15 are processed to assess small scale parameters of (sub)canopy vegetation. Results of the TanDEM-X approach will be improved in collaboration with the German Aerospace Center.

3 GRK 1408: MDS - Methods for Discrete Structures

Prof. Dr. Martin Skutella
Email: martin.skutella@tu-berlin.de
TU Berlin, FU Berlin, HU Berlin
Internet: http://www.math.tu-berlin.de/MDS/

The scientific program of the GRK *Methods for Discrete Structures* is targeted towards the flexible use and combination of modern tools as applied to discrete problems at the interface between mathematics and computer science — with an emphasis on methods. In the framework of the lectures, colloquia, block courses etc. of the graduate college, tools and methods are treated in a broad sense. In particular, the scientific program treats the following areas.

- Geometric methods

- Approximation and online methods

- Graph methods

- Topological and algebraic methods

- Enumeration methods

- Probabilistic methods and extremal combinatorics.

The GRK's mission is to equip its students with a panoramic view of these methods and to introduce them to the basic ideas of each class of methods. The students learn to experiment, combine, and sharpen the tools which are relevant to their individual research topics and thesis projects, which are of course more specific and focused. These projects come from various aspects of discrete mathematics, including graph theory, theoretical computer science and algorithms, combinatorial and network optimization, mathematical operations research, and discrete geometry.

3.1 Flag-Vectors of Polytopes, Spheres and Eulerian Lattices

Philip Brinkmann (`philip.brinkmann@fu-berlin.de`)
Supervisor: Günter M. Ziegler

In my PhD-project I work on the sets of flag-vectors of convex polytopes and more general objects. In particular I will develop a theory of strongly connected Eulerian lattices, which contain the face lattices of convex polytopes, but also that of (triangulations of) connected odd-dimensional manifolds. I will compare the set of flag-vectors of these lattices to that of convex polytopes and strongly regular spheres.

In 1906 Steinitz[1] gave a complete description of the set of all f-vectors of 3-polytopes. He also figured out the simple respectively simplicial polytopes as the extremal cases and it follows from his result on the graph of 3-polytopes[2] that strongly regular CW 2-spheres and Eulerian lattices of length 4 have the same sets of f-vectors (this actually holds for flag vectors).

Compared to this our knowledge about the four dimensional case is relatively sparse[3][4]. It is not even clear whether strongly regular CW 3-spheres or Eulerian lattices of length 5 have the same sets of f- resp. flag-vectors as 4-polytopes, nor is there a complete description of the set of all flag-vectors of 4-polytopes.

Therefore, in my work I will focus on the four dimensional case and the question whether or not the sets of flag vectors of 4-polytopes, 3-spheres and Eulerian lattices of rank 5 are the same.

---

[1] Steinitz, Ernst. Über die Eulersche Polyederrelation. *Archiv der Mathematik und Physik, Series 3*, 11:86–88, 1906.

[2] Steinitz, Ernst. Polyeder und Raumeinteilungen. In W. Fr. Meyer and H. Mohrmann, editors, *Encyklopädie der mathematischen Wissenschaften mit Einschluss ihrer Anwendungen, Band III.1.2*, 9:1–139, Teubner, Leipzig, 1922.

[3] Bayer, Margaret M. The Extended f-Vectors of 4-Polytopes. *Journal of Combinatorial Theory, Series A*, 44:141–151, 1987.

[4] Ziegler, Günter M. Face Numbers of 4-Polytopes and 3-Spheres. *Proceedings of the ICM, Beijing 2002*, 3:625–636, 2003.

3.2 Optimization methods in Discrete Geometry

Moritz Firsching (`firsching@math.fu-berlin.de`)
Supervisor: Prof. Günter M. Ziegler

Abstract of thesis.

In this thesis we use methods from nonlinear optimization in order to obtain results in various problems in Discrete Geometry. These include questions about packing, realization and inscription of matroids and simplicial manifolds, graph drawings among others. One focus lies in techniques, which enable us to go from numerical results to exact algebraic answers.

Kepler (1619) and Croft (1980) considered the problem of finding the largest homothetic copies of one regular polyhedron contained in another regular polyhedron. For arbitrary pairs of polyhedra, we propose to model this as a quadratically constrained optimization problem. These problems can then be solved numerically; in case the optimal solutions are algebraic, exact optima can be recovered by solving systems of equations to very high precision and then using integer relation algorithms. Croft solved the special cases concerning maximal inclusions of Platonic solids for 14 out of 20 pairs. For the six remaining cases, we give numerical solutions and conjecture exact algebraic solutions. These results have been published[1].

Given a simplicial sphere or an oriented matroid we can ask if those objects are polytopal and if this is the case are they inscribable? This question can be rephrased as "is a certain semialgebraic set empty?". In many cases we can answer this question numerically with the help of nonlinear optimization and then obtain exact solutions from the numerical solutions. As application of this method we present a description of all 3-spheres with small valence, and an attempt to enumerate all simplicial 4-polytopes with 10 vertices.

---

[1]Moritz Firsching. Computing Maximal Copies of Polyhedra Contained in a Polyhedron. *Experimental Mathematics*, 24(1):98–105, 2015.

3.3 Theta-rank of point configurations

Francesco Grande (`fgrande@zedat.fu-berlin.de`)
Supervisor: Raman Sanyal

The Theta rank of a finite point configuration V is the maximal degree necessary for a sum-of-squares representation of a non-negative linear function on V. This is an important invariant for polynomial optimization that is in general hard to determine.

A point configuration V is k-**level** if for every facet-defining hyperplane H there are k parallel hyperplanes $H = H_1, H_2, \ldots, H_k$ with

$$V \ \subseteq \ H_1 \cup H_2 \cup \cdots \cup H_k.$$

An important result [1] states that a point configuration V has Theta rank 1 if and only if V is 2-level. This motivates the interest in 2-level point configurations. In particular, we focus on 0/1-configurations coming from what we call 2-level matroids.

Our main result is the following equivalence theorem for a matroid M and its base configuration V_M:

- V_M has Theta rank 1 or, equivalently, is 2-level;

- M has no minor isomorphic to $M(K_4)$, $\mathcal{W}^3$, Q_6, or P_6;

- M can be constructed from uniform matroids by taking direct sums or 2-sums;

- The vanishing ideal of V_M is generated in degrees ≤ 2;

- The base polytope P_M has minimal psd rank.

Moreover, we provide an asymptotic enumeration of this matroid family and prove that all 2-level matroids are positroids. We further give an excluded minor characterization for k-level graphs and investigate the excluded minors for graphs of Theta rank 2.

We also have results about general k-level matroids and about non-negative rank of hypersimplices.

---

[1] João Gouveia, Pablo Parrilo, and Rekha Thomas. Theta bodies for polynomial ideals. *SIAM Journal on Optimization*, 20(4):2097–2118, 2010.

3.4 On certain problems in extremal and additive combinatorics

Codrut Grosu (`grosu.codrut@gmail.com`)
Supervisor: Prof. Tibor Szabó, PhD

The main results in my thesis are the following.

The first result[1] concerns the existence of partial isomorphisms (i.e. bijective maps that preserve only a finite number of algebraic relations) between subsets of $\mathbb{F}_p$ and subsets of $\mathbb{C}$. Vu, Wood and Wood[2] showed that any finite set S in a characteristic zero integral domain can be mapped to $\mathbb{F}_p$, for infinitely many primes p, while preserving finitely many algebraic incidences of S. I show that the converse essentially holds, namely any small subset of $\mathbb{F}_p$ can be mapped to some finite algebraic extension of $\mathbb{Q}$, while preserving bounded algebraic relations. This answers a question of Vu, Wood and Wood. The theorem has several applications, in particular it is shown that for small subsets of $\mathbb{F}_p$, the Szemerédi-Trotter theorem holds with optimal exponent $\frac{4}{3}$, and it improves the previously best-known sum-product estimate in $\mathbb{F}_p$. Furthermore some advances related to an old question of Rényi about the number of terms of the square of a polynomial are obtained.

The second result[3] in my thesis concerns Turán densities of hypergraphs. This is an old and classical field of study in graph theory, with many basic problems still unsolved. The main theorem asserts the existence of an abstract algebraic structure on the set of Turán densities. Several facts about Turán densities (which were previously proved by others) can be re-deduced in a streamlined fashion. In particular, explicit irrational densities for any $r \geq 4$ are constructed (their existence was first shown by Pikhurko[4]).

The third result[5] is joint work with Anna Adamaszek, Michał Adamaszek, Peter Allen and Jan Hladký. It is about the Graceful Tree Conjecture, a 50 year old and very beautiful problem, with important ramifications in the field of graph decompositions. The main theorem is a proof of an asymptotic version of the conjecture for trees of bounded degree. We further show that the conjecture is asymptotically true for random trees as well.

---

[1] C. Grosu. $\mathbb{F}_p$ is locally like $\mathbb{C}$. *J. London Math. Soc.*, 89(3):724–744, 2014.

[2] V, Vu, M. Wood, P. Wood. Mapping incidences. *J. London Math. Soc.* 84(2):433–445, 2011.

[3] C. Grosu. On the algebraic and topological structure of the set of Turán densities. *Submitted*, Available online at http://arxiv.org/abs/1403.4653, 2014.

[4] O. Pikhurko. On Possible Turán Densities. *Israel J. Math.*, 201:415–454, 2014.

[5] A. Adamaszek, M. Adamaszek, P. Allen, C. Grosu, J. Hladký. Almost all trees are almost graceful. *Preprint*, 2015.

3.5 Intersection Graphs and Geometric Objects in the Plane

Udo Hoffmann (uhoffman@math.tu-berlin.de)
Supervisor: Stefan Felsner

The thesis deals with several topics concerning graphs derived from geometric objects in the plane.

In the first part we investigate the interplay between bipartite intersection graphs of objects in the plane and the order dimension of its comparability graph. For various shapes in the plane the order dimension is bounded. First we use the dimension on subclasses of grid intersection graphs to derive simple separating examples between those classes. As a byproduct, we obtain a proof for the fact that vertex-face incidence posets of outerplanar graphs have interval dimension three (it was known that they may have dimension four).

A further result using the dimension of intersection graphs is that the order dimension of intersection graphs of segments using k slopes is bounded by $2k$. We use this as an entry point to study the number of slopes that is required to represent a graph as segment intersection graph (*slope number*). We show that minimizing the slope number of a given segment intersection graph is NP-hard. The tool used for this result is a correspondence between Hamiltonian paths in a planar graph and segment intersection representations of its full subdivision.

A similar technique also gives a new, simple proof for a result by Kratochvíl and Matoušek[1], who show that the recognition of segment intersection graphs, even with a bounded number of slopes, is NP-hard. Furthermore, it can be used to show that the slope number of a segment intersection graph can be linear in the number of vertices, but drops down to two upon the removal of a single vertex of the graph.

In the second part we discuss the complexity of the recognition problem for visibility graphs of points in the plane (PVG). Recently, Roy[2] has shown that PVG recognition is NP-hard. We improve this result by showing that the problem is hard in the *existential theory of the reals*, i.e., as hard as deciding the solvability of an inequality system with integer coefficients over the real numbers. In addition, we give examples of PVGs that require irrational coordinates in every realization.

---

[1] Jan Kratochvíl and Jiri Matoušek. NP-hardness Results for Intersection Graphs. *Comm. Math. Univ. Caro.*, 30(4):761–773, 1989.

[2] Bodhayan Roy. Point Visibility Graph Recognition is NP-hard. *arXiv preprint 1406.2428*

3.6 Congruence Testing for Point Sets in 4-Space

Heuna Kim (`heunak@zedat.fu-berlin.de`)
Supervisor: Günter Rote

We gave an $O(n \log n)$ time algorithm for the exact congruence testing problem for two sets of n points in 4-space. This problem is to decide if two point sets in the 4-dimensional Euclidean space are the same up to rotations and translations. The problem is sensitive to numerical errors, but since congruence testing with error tolerances is known to be NP-hard[1], we restrict our concern to the exact case and use the Real Random-Access Machine (Real-RAM) model.

For two and three dimensions, there are $O(n \log n)$ algorithms due to Manacher[2] (1976) and Atkinson[3] (1987). It has been conjectured that $O(n \log n)$ algorithms should exist for any fixed dimension. The best algorithm so far by Brass and Knauer[4] (2000) takes $O(n^{\lceil d/3 \rceil} \log n)$ time in d-dimensional space and therefore $O(n^2 \log n)$ in 4-space. The new algorithm makes use of properties of planes in 4-space, such as angles, distances, and packing numbers, and also properties of rotations in 4-space. In particular, we also provided an alternative construction of Hopf fibrations.

[1] Claudia Dieckmann. *Approximate Symmetries of Point Patterns*. PhD thesis, Freie Universität Berlin, 2012. Sebastian Iwanowski. Testing approximate symmetry in the plane is NP-hard. *Theoretical Computer Science*, 80(2):227–262, 1991.

[2] Glenn Manacher. An application of pattern matching to a problem in geometrical complexity. *Information Processing Letters*, 5(1):6–7, 1976.

[3] M. D. Atkinson. An optimal algorithm for geometrical congruence. *Journal of Algorithms*, 8(2):159–172, 1987.

[4] P. Braß and C. Knauer. Testing the congruence of d-dimensional point sets. *International Journal of Computational Geometry and Applications*, 12(1&2):115–124, 2002.

3.7 Distinguished Structures in Graphs (Postdoctoral Research)

Alexey Pokrovskiy (`apokrovskiy@zedat.fu-berlin.de`)
Supervisor: Tibor Szabó

Aharoni and Berger [1] conjectured that every bipartite graph which is the union of n matchings of size $n + 1$ contains a rainbow matching of size n. This conjecture is a generalization of several old conjectures of Ryser, Brualdi, and Stein about transversals in Latin squares. I proved an approximate version of this conjecture—that the conclusion holds as long as all the matching have size at least $n + o(n)$. The proof involves studying connectedness in coloured, directed graphs. The notion of connectedness that is required is new, and of independent interest.

Recently Kühn, Lapinskas, Osthus, and Patel [2] introduced a new tool for studying connectedness called "linkage structures". Informally, a linkage structure L is a small set of vertices such that for any pair of vertices x and y, there is an x to y path which is mostly contained in L. Kühn et al. showed that every highly connected tournament contains many disjoint linkage structures, and used this to solve two conjectures of Thomassen. I used a variation of linkage structures to solve two conjectures of Kühn, Lapinskas, Osthus, and Patel. One of these conjectures is that every $O(k^2)$-connected tournament has k edge-disjoint Hamiltonian cycles. The other is that every $O(k)$-connected tournament is k-linked.

Erdős, Faudree, Gyárfás, and Schelp [3] studied graphs with $2n-2$ edges which have no proper induced subgraphs with minimum degree 3. They studied cycles in such graphs and conjectured that every graph with $2n - 2$ edges which have no proper induced subgraphs with minimum degree 3 contains cycles of lengths $3, 4, 5, 6, \ldots, C(n)$, where $C(n)$ is some increasing function in n. Together with Narins and Szabó we disproved this conjecture, by producing graphs satisfying the conditions of the conjecture but with no C_{23}. Our construction relies on first reducing the problem to studying possible path lengths in binary trees. This raised the following natural problem "given a binary tree, what can be said about the possible lengths of leaf-leaf paths that it must contain".

[1] R. Aharoni and E. Berger. Rainbow matchings in r-partite r-graphs. *Electron. J. Combin.*, 16, 2009.

[2] D. Kühn, J. Lapinskas, D. Osthus, and V. Patel. Proof of a conjecture of Thomassen on Hamilton cycles in highly connected tournaments. *Proc. London Math. Soc.* 109: 733–762, 2014.

[3] P. Erdős, R. Faudree, A. Gyárfás, and R. Schelp. Cycles in graphs without proper subgraphs of minimum degree 3. *Ars Combin.*, 25:159–201, 1988.

3.8 Resource Minimization in Online Deadline Scheduling

Kevin Schewior (`schewior@math.tu-berlin.de`)
Supervisor: Martin Skutella

Our goal is to minimize different resources in the following fundamental scheduling problem. We consider jobs with deadlines arriving online at their release dates, where the instance is assumed to possess a feasible preemptive offline schedule on a m parallel machines. As proposed by Phillips et al.[1] as well as Lam and To[2], we are looking for the minimum resources, that is, speed, the number of machines, or the trade-off between both, such that we can always produce feasible schedules online. It is known[3] that we have to augment the resources, that is, the m machines used offline, to achieve that.

Regarding augmentation by speed, we give new lower bounds on the required speed for various algorithms such as the very natural one Least Laxity First (LLF). We also note that the analysis of the algorithm proposed by Anand et al.[4], which was claimed to be the best known one, is incorrect, and we are working towards fixing this issue. Furthermore, we open up the analysis of instances with a fixed number of release dates, generalize known results, and give completely new ones such as tight bounds for LLF in this setting. We are also working on a tight algorithm for two release dates, which may lead to a better algorithm in the general case.

Moreover, we give the first algorithm that only requires $f(m)$ unit-speed machines for some function f. In our case, f is even polynomial. The algorithm is based on an analysis of different complementary subclasses of the problem, which are also of their own interest. Our conjecture is that even a linear such function f exists, and the plan is to obtain such a function in the future.

We are also working on the trade-off between speed and the number of machines, which can also be posed as the question for the required number of machines if the speed on all machines is fixed to be $1 + \varepsilon$.

[1] C. A. Phillips, C. Stein, E. Torng, and J. Wein. Optimal time-critical scheduling via resource augmentation. *Algorithmica*, 32(2):163–200, 2002

[2] T. W. Lam and K.-K. To. Trade-offs between speed and processor in hard-deadline scheduling. In *Proc. of the 10th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 623–632, 1999.

[3] M. L. Dertouzos, A. K. Mok Multiprocessor on-line scheduling of hard-real-time tasks. *IEEE Transactions on Software Engineering*, 15(12):1497–1506, 1989.

[4] S. Anand, N. Garg, and N. Megow. Meeting deadlines: How much speed suffices? In *Proceedings of the 38th International Colloquium on Automata, Languages and Programming (ICALP 2011)*, volume 6755 of *LNCS*, pages 232–243. Springer, 2011.

3.9 High-Dimensional Geometric Problems: Algorithms and Complexity

Yannik Stein (`yannik.stein@fu-berlin.de`)
Supervisor: Wolfgang Mulzer

In the first part, we consider algorithmic problems related to high-dimensional convexity. Let $P_1, \ldots, P_{d+1} \subset \mathbb{R}^d$ be point sets that each contain the origin in its convex hull. We think of the points in P_i as having color i. A *colorful choice* is a set with at most one point of each color. The *colorful Carathéodory theorem* guarantees the existence of a colorful choice whose convex hull contains the origin. So far, the computational complexity of finding such a colorful choice is unknown. This is particularly interesting as there are polynomial-time reductions from Tverberg's theorem, the First-Selection-Lemma, and the colorful Kirchberger theorem.

We approach this problem from two directions. First, we consider approximation algorithms: an *m-colorful choice* is a set that contains at most m points from each color. Using a dimension reduction argument, we show that for any fixed $\varepsilon > 0$, an $\lceil \varepsilon d \rceil$-colorful choice containing the origin in its convex hull can be found in polynomial time. This notion of approximation has not been studied before, and it is motivated through the applications of the colorful Carathéodory theorem in the literature. Second, we present a natural generalization of the colorful Carathéodory problem: in the *nearest colorful polytope* problem (NCP), we are given sets $P_1, \ldots, P_n \subset \mathbb{R}^d$ that do not necessarily contain the origin in their convex hulls. The goal is to find a colorful choice whose convex hull minimizes the distance to the origin. We show that computing local optima for the NCP problem is PLS-complete, while computing a global optimum is NP-hard.

In the second part, we focus on a generalization of the well-known *approximate nearest neighbor* problem. Let $k \geq 0$ be an integer. In the *approximate k-flat nearest neighbor* (*k*-ANN) problem, we are given a set $P \subset \mathbb{R}^d$ of n points in d-dimensional space and a fixed approximation factor $c > 1$. Our goal is to preprocess P so that we can efficiently answer *approximate k-flat nearest neighbor queries*: given a *k*-flat F, find a point in P whose distance to F is within a factor c of the distance between F and the closest point in P. We present the first efficient data structure that can handle approximate nearest neighbor queries for arbitrary k. The data structure delicately interweaves sub-data structures for high and low dimensions.

3.10 Problems Related to Social Networks: Election Control and Anonymization

Nimrod Talmon (`nimrodtalmon77@gmail.com`)
Supervisor: Prof. Rolf Niedermeier

We consider several combinatorial problems related to social networks, and study their computational complexity, with an emphasis on their parameterized complexity. We begin by studying the complexity of several problems of election control, where we assume some relationships between the voters of the given elections which can be seen as dependent on an underlying social network over the voters. Then, we study issues of privacy when publishing social networks and elections-related data.

For the election control problems, we assume a given election, defined through a collection of voters, each having a linear order over a set of some alternatives, and an external agent, which can manipulate the election. We assume some combinatorial structure over the election, such that the external agent can, at some cost, influence the way several voters vote, at once. First, we consider election control by adding or deleting alternatives, for election with only a few voters[1]. Then, we consider combinatorial bribery, that is, that an external agent can shift the position of its preferred alternative in the votes of several voters, at once[2].

For the issues of privacy when publishing social networks, we concentrate on k-anonymization. The general task here is to transform an undirected input graph into a k-anonymous graph, where a graph is said to be k-anonymous if for every vertex degree d in it there are at least k vertices with degree d. First, we concentrate on making a graph k-anonymous by adding new vertices[3]. Then, we concentrate on making a graph k-anonymous by contracting edges[4]. Finally, instead of k-anonymizing graphs, we consider k-anonymizing elections, where an election is said to be k-anonymous if for every voter in it there are at least k voters with the same preference order[5].

---

[1] Jiehua Chen, Piotr Faliszewski, Rolf Niedermeier, Nimrod Talmon. Elections with Few Voters: Candidate Control Can Be Easy. AAAI 2015: 2045-2051.

[2] Robert Bredereck, Piotr Faliszewski, Rolf Niedermeier, Nimrod Talmon. Large-scale election campaigns: Combinatorial shift bribery. AAMAS 2015: 67-75.

[3] Robert Bredereck, Vincent Froese, Sepp Hartung, André Nichterlein, Rolf Niedermeier, Nimrod Talmon. The Complexity of Degree Anonymization by Vertex Addition. AAIM 2014: 44-55.

[4] Sepp Hartung, Nimrod Talmon. The Complexity of Degree Anonymization by Graph Contractions. TAMC 2015: 260-271.

[5] Nimrod Talmon. Privacy in Elections: k-Anonymizing Preference Orders. Submitted for publication. April 2015.

3.11 Order Dimension and Cover Graphs

Veit Wiechert (`wiechert@math.tu-berlin.de`)
Supervisor: Stefan Felsner

In my dissertation I study combinatorics of partially ordered sets (for short *posets*). One of the most studied parameter for the complexity of a poset is its *dimension*. A quite recent research in this area investigates the relationship between dimension and *cover graphs* of posets. Typical questions are: How does the cover graph of a large dimensional poset look like? Which structural properties of the cover graph impose small dimension on the poset? In my thesis I contribute to the solution to these problems.

A classic result of Moore and Trotter from 1977 states that posets with trees as cover graphs have dimension at most 3. More recently, it was shown that also posets whose cover graphs are outerplanar[1] or have pathwidth[2] 2 have bounded dimension. Because of these results it was conjectured that posets with cover graphs of treewidth 2 have bounded dimension. In a joint work with Joret, Micek, Trotter and Wang[3] we settled this in the affirmative.

One cannot hope for such a result if we only ask for planarity as Kelly introduced posets with planar cover graphs that have arbitrarily large dimension. However, it was noted that they contain a long chain and hence have large height. Consequently, Felsner, Li and Trotter conjectured that posets of bounded height and whose cover graphs are planar have bounded dimension. Motivated by this, in a sequence of papers it was proven that bounded height posets whose cover graphs are planar[4], have bounded treewidth[5], or exclude a fixed graphs as a (topological) minor[6] have bounded dimension. Together with Micek we reproved all these results in an elementary way without using structural decomposition theorems for graphs, and we improved existing bounds by a lot[7]. Moreover, we introduced new techniques to upper bound dimension and applied them to other interesting classes of posets. Quite recently, in a joint work with Joret and Micek we further generalize all mentioned results and give a full description of which sparse graph classes impose bounded dimension.

[1] S. Felsner, W. T. Trotter and V. Wiechert. The dimension of posets with planar cover graphs. *to appear in Graphs and Combinatorics.*

[2] C. Bíró, M. T. Keller and S. J. Young. Posets with cover graph of pathwidth two have bounded dimension. *to appear in Order.*

[3] G. Joret, P. Micek, W. T. Trotter, R. Wang and V. Wiechert. On the dimension of posets with cover graphs of treewidth 2. *submitted.*

[4] N. Streib and W. T. Trotter. Dimension and height for posets with planar cover graphs. *European J. Combin.*, 35:474–489.

[5] G. Joret, P. Micek, K. G. Milans, W. T. Trotter, B. Walczak and R. Wang. Tree–width and dimension. *to appear in Combinatorica.*

[6] B. Walczak. Minors and dimension. *SODA 2015*: 1698–1707.

[7] P. Micek, V. Wiechert. Topological minors of cover graphs and dimension. *submitted.*

4 GRK 1424: MuSAMA - Multimodal Smart Appliance Ensembles for Mobile Applications

Prof. Dr. Thomas Kirste
Email: thomas.kirste@uni-rostock.de
University of Rostock
Internet: http://www.musama.de

MuSAMA is based on the hypothesis that ubiquitous machine intelligence, envisioned for our future everyday environments, will be provided by dynamic ensembles: Local agglomerations of smart appliances, whose composition is prone to frequent, unforeseeable, and substantial changes. Members of such ensembles need to be able to cooperate spontaneously and without human guidance in order to achieve their joint goal of assisting the user. The resultant concept of autonomous cooperative assistance poses new challenges for the research on ubiquitous and ambient information technology. Work in MuSAMA concentrates on the investigation of models and algorithms that allow dynamic ad-hoc ensembles to deliver assistance independently of external or global knowledge. Coherent ensemble behaviour emerges from local interaction of individual appliances. The application scenario are instrumented rooms supporting teams in knowledge exploration based on distributed displays. The following research areas are addressed: RA1. Ubiquitous Context Sensing and Analysis. Use of distributed sensors and sensor networks to recognise the current context, specifically with respect to the spatial configuration of users and devices. RA2. Multimodal Interaction and Visualisation. Information visualisation based on distributed display infrastructures and ubiquitous displays. Adaptive interaction with an ad-hoc ensemble based on explicit task models. RA3. Intention Recognition and Strategy Generation. Recognition of user activities and intentions based on knowledge about typical behaviour and explicit interactions. Techniques for the cooperative generation and execution of strategies for assisting user objectives by the ensemble. RA4. Data Management, Resources, and Infrastructure Management: Underlying communication and data management services for cooperative strategies. Resource-adaptive communication mechanisms for dynamic ensembles.

4.1 Scenario-based Creation of Behavioural Models and their Evaluation in Smart Environments

Gregor Buchholz (`gregor.buchholz@uni-rostock.de`)
Supervisor: Prof. Dr.-Ing. habil. Peter Forbrig

Connecting the widest range of devices and sensors is part of our near future. The vision of Ubiquitous Computing is to make a dynamically composed ensemble of devices support the user in his tasks. Different approaches exist to identify the users' intentions based on, for example, previous observations and the current context as detected by sensors. This work further examines the application of structured knowledge about the users' tasks in form of task models. In particular, the process of developing such models is of central interest.

The application of models is a well-established principle of numerous engineering techniques for designing interactive systems. Task models represent activities from the users' point of view and combine a precise process description with user-friendly readability. As such, they can be used both as machine-readable process description and means of communication between all stakeholders during the system's development and usage.

Usually, the modelling of user behaviour is based on the knowledge acquired during the requirements analysis phase and aims at manually formalizing the domain-specific insights into concepts, roles, processes, and other characteristics. However, with increasing level of detail and decreasing level of abstraction the construction of models become more and more laborious and prone to error, so time and labour saving assistance would be an effective support.

With the help of process mining techniques and based on recorded scenario traces, the construction of models can be achieved as a combination of creative top-down modelling and interactive bottom-up generation.

Within this work a tool chain is to be established that supports several development steps: the expert-based recording of scenario traces in a simulated environment (Sur40), the semi-automatic completion of models based on the scenario protocols, and the simulation of ambient intelligence support in the virtual environment.

By the presence of a comprising process description the user support can be adjusted to the specific situation of the users. Beyond this, task models can be used as a direct interaction tool between users and the system during runtime.

Amongst the key challenges are the merging of the traditional top-down modelling method with the bottom-up production, the identification and reduction of the shortcomings of virtual scenario recording and simulation, and the integration of existing pattern-based modelling methods and tools.

4.2 Information presentation in multi-presenter scenarios

Christian Eichner (`christian.eichner@uni-rostock.de`)
Supervisor: Prof. Dr.-Ing. Heidrun Schumann

Electronic presentations are a powerful means to support talks and discussions. While common approaches focus on presenter-audience scenarios, we aim to support multi-presenter scenarios. In a multi-presenter scenario different presenters contribute with individual contents to dynamically create a composite presentation. We propose techniques to create and display such "multi-presentation" in multi-display environments. This requires an appropriate model to describe the structure of the presentation and a suitable strategy to integrate contents from different sources into the presentation. Furthermore an enhanced user interface is needed to support the users in creating such a multi-presentation. Finally interaction concepts need to be designed to fit the presentation scenario.

In our approach we use a layered graph to describe the structure of a presentation. Each node of the "presentation-graph" represents a single piece of content used in a presentation (e.g. a slide or a particular view) and edges show the relationships between the nodes. For temporal ordering of nodes we introduce a layered structure. Each layer represents those nodes that belong to a certain time point. Intra-layer edges provide spatial constrains for calculated layouts. Inter-layer edges are temporal links and are used to generate temporal stable layouts. Finally structural links connect nodes based on the subject matter of the respective content. These edges are used to spontaneously navigate in a presentation or adapt the visualization of the shown content set.

The graph is ad-hoc extendable and allows merging of prepared content from different presenters and on-the-fly generated content. Presenters can provide individual contents to a common content pool. Starting with a single path structure presenters are able to generate the graph by adding edges or extend layers with contents from the pool. Graphs of multiple presenters can be merged to form a composite presentation.

We provide user interfaces that visualize the presentation graph and the content sets of the layers. User can use our tool to simultaneously create and edit composited presentation. During a presentation the content sets of the layers are successively distributed to the available displays.

In order to show the contents of a presentation we provide an assistance system that automatically maps contents to available displays and creates initial layouts. User may adapt layouts by adjusting graph properties or directly interact with contents on the display. Moreover a undo/redo-systems allows to revert unwanted changes or restore previous presentation states.

4.3 Privacy-aware Adaptive Query Processing in Dynamic Networks

Hannes Grunert (`hannes.grunert@uni-rostock.de`)
Supervisor: Prof. Dr. rer. nat. habil. Andreas Heuer

Smart environments are intended to assist their users in everyday life, whether at work (Ambient Assisted Working) or at home (Ambient Assisted Living). The current situation and the actions of the user are collected through various sensors which gather a vast quantity of information. This data is stored by the system and charged up with other information, such as with the social network profile of the user. Through the gained knowledge, preferences, behaviour patterns and future events can be calculated. Hence, the intentions and future actions of the user are derived and the smart environment reacts independently to the needs of the user.

Assistance systems often collect more information than needed. In addition, the user usually has no or only a very small influence on the storage and processing of his personal data. Thus his right to informational self-determination is violated. By amending the assistance system by a data protection component, which checks the privacy claims of the user against the information needs of the system, this problem can be managed.

An automated checking of different interests that may contradict or contain each other, is generally not easy to solve and requires further research. By applying an individually adapted solution to this application, the complexity of the problem can be reduced. A customized query processor, which modifies both the query and the preliminary result of the query, encourages adherence to the privacy settings of the user. Through a privacy-aware propagation of sensor and context information of the analytical tools of the assistance system not only the privacy-friendliness of the system is improved, but also its efficiency is increased.

My research is motivated by the following questions: Can privacy techniques be directly executed in database systems? Is it possible to execute them together with analysis functionalities without losing too much precision? Can the execution and response time of the system be reduced by processing less data?

Currently, I specify a privacy-aware query processor. The processor works in two main stages. During the preprocessing stage, the preliminary query is analysed, modified and checked against the privacy policy of the affected user. After retrieving the result from the database, the postprocessor applies anonymity concepts, like k-anonymity, to the data.

4.4 Efficient device oriented Plug and Play Middleware Architecture

Bjoern Konieczek (`bjoern.konieczek@uni-rostock.de`)
Supervisor: Prof. Dr.-Ing. Dirk Timmermann

In 1991 Mark Weiser formulated his vision of Ubiquitous Computing. Since then, a technical development has taken place, that makes the realisation of this vision achievable. The long-term goal is to build environments that assist the user, without the user's direct interaction with the devices. Therefore, the devices need to recognize the user's intention and take the corresponding actions. To minimise the costs and size of the devices, every device is only capable of fulfilling one particular task. Hence, the devices need to form an intelligent ensemble, whereby the intelligence mainly originates from high interoperability. RESTful architectures (REST = Representational State Transfer) are a promising solution to enable this interoperability. The Constrained Application Protocol (CoAP) tries to bring the quintessence of RESTful architectures to the realm of resource constraint devices.

However, in many cases not only interoperability but also timing is crucial. In order to avoid failures that may threaten life or property, the system must respond to external stimuli before a certain deadline. These types of systems are usually referred to as real-time Systems. Due to the broad distribution of applications over many devices, it is not only sufficient for one device to process it's part of the application before the deadline. The influence of the communication between the devices on the overall timing behaviour is rather high. In consequence, real-time capabilities must be enabled on the communication layer while maintaining high interoperability. Classical approaches to this problem, however, include the use of proprietary hardware and adaptations to lower layer protocols. This leads to separated and non-interoperable communication domains.

The goal of this thesis is to enable real-time communication purely through software adaptations, which would solve the interoperability problems of classical real-time approaches. In the scope of this research the jCoAP framework was developed. jCoAP is a platform independent implementation of CoAP that offer the most important features for machine-to-machine communication (M2M) and can be processed in real-time on the device level. To enable truly real-time capable communication, the network access of the devices needs to managed to avoid contention. The current work investigates a P2P-based TDMA approach to bring real-time behaviour to the network level. This approach will be compared to a direct integration of a TDMA mechanism into jCoAP.

4.5 Big Data Analytics for Efficient Activity Recognition and Prediction in Assistive Systems

Dennis Marten (`dm@informatik.uni-rostock.de`)
Supervisor: Prof. Dr. rer. nat. habil. Andreas Heuer

Smart environments are and will be a great part of our everyday lives. Such assisting systems usually consistx of multiple sensors, which gather worthy information, e.g. temperature. Due to technical improvements in this area, the amount of data that can be obtained has been drastically increased. Besides several advantages, like the possibility to create more detailed models, researchers often times experience heavy performance issues while running conventional, statistical software on this big data. This can lead to setbacks in the development step, since researchers have to put additional effort into finding and implementing alternative processing methods.

One key example for this situation is the widely used open source tool R, which is known for its easily usable and powerful statistics. However, the performance depends heavily on the servers' main memory. When data exceeds the main memory, R's processing speed slows down rapidly. There surely are plenty of possibilities to compensate this issue, e.g. use performance-enhancing R-packages, buy more memory, use more nodes or even switch to another processing method. However, it should not be the researchers' task to spend time or even money on solving this problem.

This is the entry point for my research topic: a framework that will transparently combine the statistical power of R, with the in- and output abilities of database technology and a parallel computation model. In this framework, experimental data is stored in the database, and parts of the R-code should be either processed on the database, in parallel on several nodes or in R itself, depending on what is most beneficial. The main aspect of this project, besides the performance improvement, is its transparent realization, meaning that the input remains the usual R script.

There are several problems that have to be investigated for this project. One of the questions that need to be researched on is: What parts of an R-code can be translated into SQL in a beneficial way? Other topics of interest are for example the development of a suited architecture, the parsing of the code or the choice of a fast and manageable database system.

Currently, I am working on a theoretical background for the parsing of an R-Code. Therefore R-methods have to be converted into directed acyclic graphs. Such graphs will build the basis for the determination of dependencies and submethods of an R-task. This will help to decide when and what parts can be processed on the database and maybe even on a cluster.

4.6 Adaptation Strategies in Smart Environments Based on Predictive User Models

Redwan Abdo A. Mohammed (`redwan.mohammed@uni-rostock.de`)
Supervisor: Prof. Dr. Oliver Staadt

Predicting user behavior is desirable in many application scenarios in smart environments. Based on signals collected from various sensors smart environments can react in a proactive manner in order to assist the user. Gaze represents one of the essential cues, which is important to understand these behavior. Being able to predict gaze locations, as compared to only measuring them, is desirable in many application scenarios such as video compression, the design of web pages and commercials adaptive user interfaces, interactive visualization, or attention management systems.

We focus on eye movements and the spatial location of visual attention as informative for intention recognition. The existing models for eye movement do not take contextual factors into account. This will be addressed using a systematic machine-learning approach, where user profiles for eye movements are learned from data.

Another approach proposed in this work is the modeling of eye movements as a Markov decision process(MDP).Therefore, the approach taken here is to formulate eye movements as a Reinforcement Learning (RL) problem, but to use Inverse Reinforcement Learning(IRL) to infer the reward function. We have examined different inverse reinforcement learning algorithms. The examined approach used information about the possible eye movement positions. We showed that it is possible to automatically extract reward function based on effective features from user eye movement behaviors using IRL. We found that the reward function was able to extract expert behavior information that fulfill to predict eye movements. This is valuable information for estimating the internal states of users such as in, for example, intention recognition, to adapt visual interfaces, or to place important information.

Using saliency maps generated from bottom up saliency models and the state value function from IRL models, along with an adaptive strategy, the application on the tiled large high-resolution displays (LHRDs), as an example, can be adapted to the predicted behavior.

4.7 Situation-Aware Control of Smart Meeting Rooms

Daniel Moos (`daniel.moos@uni-rostock.de`)
Supervisor: Prof. Dr.-Ing. Thomas Kirste

The vision of ubiquitous computing is becoming reality. Today's environments contain a diversity of devices to provide comfort to its users and ease daily life. Current research seeks for techniques to build ad-hoc ensembles out of these devices and enable inter-device cooperation to provide complex emergent behavior. This cooperation happens outside of the perception of users. Bellotti & Edwards argue that context-aware systems should not be black boxes and instead inform users about their details, inner workings, and decisions. Based on their argumentation they proclaimed two design principles: intelligibility and accountability. Intelligibility means the system "must be able to represent to their means what they know, how they know it, and what they are doing about it" and accountability ensures that users can override decisions made by the system.

In the last years various researchers in the field of ubiquitous computing picked up these principles and enabled smart environments to answer questions and provide control related to questions. Small user surveys showed that explanations help users to build a mental model of the environment and increase their acceptance of the system.

In other surveys among inhabitants of smart homes non-expert users expressed "discomfort with her inability to fix their system". Faults in smart environments pose a problem for intelligibility, because the correct behavior of the devices is implicitly assumed in order to provide explanations. Therefore we introduced *debuggability* as a third design principle that provides users with the ability to find the cause of a fault (*debug it*) in a context-aware system. In most cases a debuggability system won't be able to detect a fault without any additional information about what went wrong. In my thesis I am investigating how human-computer interaction can be used to guide the user through the task of collecting information that can identify the fault. My goal is to provide non-expert users with the capability to handle faults in smart environments without the help of (expensive) technicians.

4.8 InterLect - A lecture content interface

Robin Nicolay (`robin.nicolay@uni-rostock.de`)
Supervisor: Prof. Dr. rer. nat. Clemens H. Cap

Current university's lectures often are visited by a large amount of listeners. Large audiences complicate interactions between lecturer and student. Students differ in their individual abilities, such as comprehension, previous knowledge, level of attention and learning abilities. These differences lead to different conflicts with lecture material at different points in time. Solving these conflicts or furthermore the identification of these conflicts is a very challenging task for a lecturer. We aim to improve insights into individual students reflection processes during a lecture by observing students during reception of lecture material. Therefore we need to connect students to lecture material and provide appropriate ways to interact with lecture content.

To connect students and lecture material, we implemented a web based system named InterLect. InterLect consists of 2 parts. First the presentation client for the lecturer and second the audience client for the listeners. The presentation client essentially is used to provide a common presentation environment. Implemented as a web page, it allows the presentation of PDF-Slide based lecture material in a common way similar to PowerPoint. The audience client receives currently presented slides and displays them on either, the handy, tablet or laptop. The listener then is able to interact with lecture material as part of his intuitive reflection process on perceived information.

To define the appropriate set of interactions we looked into different "coding strategies" that are intuitively used in learning scenarios. We identified marking, linking and conflicting as appropriate metaphors to describe the set of supported interactions. Marking denotes the process of highlighting information for later processing, such as "look into later" or "important for exam". Marking furthermore allows a semantic attachment of keywords to specific chunks of lecture material. Linking allows students to relate single facts, slides or other sources to build overall comprehension structures, such as concept- or topic-maps. Conflicting allows the expression of open issues that occur while perception of lecture content, which have to be resolved, such as missing information or the need examples.

We currently are in the process of collecting and evaluating data. By observing marked content and expressed conflicts, we hope to identify correlations between student types and student groups in the level of comprehension and types of conflicts. Furthermore, we hope to get insights in emerged cognitive relation structures and contexts to identify different learning types, contexts and unrecognized problems such as the wrong contextual links leading to misconceptions.

4.9 Efficient Probabilistic Semantics for Symbolic Behavioural Models

Martin Nyolt (martin.nyolt@uni-rostock.de)
Supervisor: Prof. Dr.-Ing. Thomas Kirste

Supporting users inside smart environments requires software knowing (i. e. inferring) the current situation of the users and planning useful actions. The *situation* comprises the current *context* (state of the world), *activities* (what users are currently doing), and *intentions* (goals the users strive for).

In the literature, there is a variety of techniques for recognising each of these parts individually. Usually, sensory data is used for context recognition, context and context changes are then used as the basis for detecting activities. Intention recognition approaches then infer goals of the users using the sequence of detected activities. What is often missing is an integrated approach, for instance using high-level knowledge on the activity structure for inferring the current context.

Application scenarios cover a wide area of recognising real-life, everyday situations, for example meetings, kitchen activities, health care and ambient assisted living. We developed a joint situation recognition approach based on computational state space models of human behaviour. These models are used in a generative approach incorporating prior knowledge. The model comprises a rich state transition model, supports multiple agents as well as actions with arbitrary duration distributions.[1] Efficient reasoning needs well-suited models[2] [3] for describing human behaviour and their interactions with the environment.

However, the reasoning based on Bayesian inference is computationally expensive, making approximations necessary. A common approximation technique is the particle filter. However, the particle filter is unsuited for the behaviour models required for our applications. We developed the marginal filter to cope better with uncertain observations and discrete states.[4] While the marginal filter performs significantly better than the partical filter, its performance is still unsuited for real-time application with huge models. My research deals with techniques and algorithms to improve its performance. In particular, I develop an efficient representation and inference of action durations and incoporate state-space reduction techniques.

---

[1] Krüger, Nyolt, Yordanova, Hein, Kirste: *Computational State Space Models for Activity and Intention Recognition. A Feasibility Study.* PLoS One, 2014.

[2] Yordanova, Nyolt, Kirste: *Strategies for Reducing the Complexity of Symbolic Models for Activity Recognition.* Proc. AIMSA, 2014.

[3] Nyolt, Yordanova, Kirste: *Checking Models for Activity Recognition.* Proc. ICAART, 2015.

[4] Nyolt, Krüger, Yordanova, Hein, Kirste: *Marginal filtering in large state spaces.* International Journal of Approximate Reasoning (61), 2015.

4.10 Programming Abstractions for Ubiquitous Applications

Matthias Prellwitz (`matthias.prellwitz@uni-rostock.de`)
Supervisor: Prof. Dr.-Ing. habil. Gero Mühl

Ubiquitous computing pursues the vision to assist users in everyday life. For that, interconnected sensor devices or services are considered, which provide environmental or contextual data, as well as actuators, which control physical devices or trigger services. Ubiquitous environments often consist of distributed and varying ensembles of heterogeneous devices. Developing applications for such environments is challenging because, at design time, it is hard to predetermine and foresee all runtime aspects and eventual execution cases. Current programming abstractions do not adequately address these kinds of dynamics and uncertainty.

To ease the development of ubiquitous applications, I want to provide programming abstractions that better support developers and allow them to abstract from the heterogeneity and number of actual devices as well as from the large amount of produced low-level events.

Dynamic Sets subsume a dynamic collection of devices and allow developers to address these via a single device interface. In this manner, it is not required to know the actual number of present devices nor their interface particularities. Selection criteria, aggregation functions, and QoS constraints (e.g. failure semantics, timeout, and result quality) are declared by developers as metadata at design time, but are ensured by the hosting middleware system at runtime. A single function call at a dynamic set within an application is transparently forwarded to all member devices of the set while return values are aggregated into a single result. Here, the middleware chooses the most efficient way to update aggregations and adaptively switches between pull and push-based communication paradigms. To build reactive application components, methods can be annotated to be executed on changes within the dynamic set.

Composable Complex Events allow the specification of spatiotemporal event patterns and enable their composition to higher-level complex events that can be reused in a parametrizable fashion. Such complex events are well suited for detection of situations, contexts, and user intentions in ubiquitous environments. This way, developers can conveniently bind application logic to high-level events without needing to know the low-level events that triggered the execution. Here, the parametrization of event detection components for gradual reuse and recomposition, the on-demand instantiation of such detector chains, and the assembly of modular and meaningful event libraries are investigated.

4.11 Dynamic Optimization of Communication Resources and Communication Strategies in Wireless Mesh Networks

Michael Rethfeldt (`michael.rethfeldt@uni-rostock.de`)
Supervisor: Prof. Dr.-Ing. Dirk Timmermann

The vision of smart environments, known as the "Internet of Things", is characterized by the seamless integration of embedded, ambient devices for user assistance. Building highly cooperative ensembles with a broad spectrum of different device classes such as sensors, actors, smart displays and especially mobile nodes like smart phones or tablets leads to highly complex networks that provide distributed, context-based information services, e.g., in public facilities or smart offices.

The increasing number of WLAN-capable consumer devices lets WLAN mesh networks appear as a promising technology for this scenario, by providing redundant multi-hop network paths and therefore a higher scalability, flexibility and robustness compared to common, Access Point-based WLAN infrastructures. Besides these advantages, characteristics such as variable network topologies and link qualities due to mesh node mobility and the general performance limits of contention-based channel access imply new technical challenges for the management and real-world operation of WLAN mesh networks. IEEE 802.11s is a new WLAN standard amendment, enabling interoperable mesh networks based on the existing and widespread WLAN technology. Nevertheless, network-wide management mechanisms fall out of the standardization scope and are therefore not specified.

The aim of this thesis is the development of strategies for dynamic resource management and application-specific parameter optimization in 802.11s mesh networks to improve network properties such as mesh topology, channel interference, link throughput or latency for overlying, distributed applications and services. This requires the derivation of service requirements and the analysis of complex mesh topologies comprising a large number of mobile nodes.

A real-world testbed and a self-developed mesh management framework serve as basis for testing and verifying different cross-layer optimization approaches. The testbed will be combined with simulations to investigate performance trends and scalability in environments with very high node density and mobility. Already completed work includes a distributed management framework prototype, the integration of physical mesh network metrics into a logical peer-to-peer overlay for improved peer selection, an investigation of the cross-layer cooperation between WLAN and TCP flow/congestion control, and an initial performance evaluation considering traffic-aware multi-channel operation of 802.11s WLAN mesh networks.

4.12 ModFP - Fast message fingerprints for resource constraint devices

René Romann (`rene.romann@uni-rostock.de`)
Supervisor: Prof. Ralf Salomon

Research on smart environments, such as smart homes and smart offices, have recently received increasing attention. In addition to the design and functionality of those devices, current research also focuses on usability and security (privacy).

This Ph.D. thesis focuses on the security part of those environments. Message integrity and authenticity is one main topic within this research area. But with resource constraint devices, like embedded systems which are usually only equipped with micro controllers, the generation and verification of message authentication codes increases the systems reaction time.

To shorten the time needed for generation and verification, this Ph.D. thesis proposes a new method to generate and verify message authentication codes. This method lowers the reaction time by factor 10 compared to widespread approaches by splitting up the calculation into a pre-calculation and a finishing phase.

4.13 Mobile 3D Gaze Tracking Calibration

Christian Scheel (`christian.scheel@uni-rostock.de`)
Supervisor: Prof. Dr. Oliver Staadt

Eye gaze information is important for many application fields, such as human-computer interaction, usability advertising or industrial design. Recent advances in telepresence systems aim at supporting gaze awareness for multiple users at remote locations. Most eye gaze tracking systems do not allow the user to move freely, but require a static head position and orientation. Thus, they are not suitable for use in multiple display or large high-resolution display (LHRD) environments.

The goal is to devise system for eye gaze tracking that supports free movement of the user by combining a mobile eye tracker with an additional external six-degree-of-freedom (6-DOF) tracking system. Here a new and simple calibration procedure is propose for such a system based on observing multiple calibration points at varying distance to the user. While the calibration procedure requires the use of a chin rest to obtain a controlled head position/orientation, the calibration systems allows the user to move freely within the tracking volume of the external tracking system (e.g., maker-based infrared camera tracker) after the calibration procedure. The contribution of the work is the introduction of a novel calibration target that is also tracked using the external 6-DOF tracker. The eye position and the 3D gaze vector can be estimate in real time without requiring manual measurements, purkinje images, or glints. Also no assumptions about the anatomy/geometry of the eye are used in the calculations.

The novel calibration target is an off-the-shelf plastic box with 18 retro-reflective markers as calibration points. Nine calibration points are attached at the front side and nine at the backside. They are arranged in 3×3 grids, respectively. The number of calibration markers is trade off between obtaining sufficient calibration data, avoiding marker occlusion, and calibration speed. The aim of the calibration is to construct lines that go straight into the eye. The eye position is then the intersection point of these lines. For constructing a line as example one calibration point from the backside of the calibration target is taken and a corresponding point with the same pupil position is interpolated between the calibration points of the front side. After a successful calibration the current gaze vector of a user can be determined in real-time. For the calculation of the current gaze vector the current pupil position from the eye tracker, the head position and orientation and the calibration data are used. In the first step a gaze point is calculated in the head coordinate system and in the second step this gaze point and the eye position from the calibration step are transferred to the world coordinate system and the gaze vector is calculated with the help of this two points.

4.14 Data Collection and Data Processing for On-Line Simulation in Smart Environments

Johannes Schützel (`johannes.schuetzel@uni-rostock.de`)
Supervisor: Prof. Adelinde M. Uhrmacher

Smart environments assist users in their doing. For instance, a smart meeting room might continually optimize the mapping of multiple documents to multiple displays for multiple viewers, each with an orientation-dependent field of vision and certain interests. A smart environment can also be a congress center in which, for instance, network routers and servers automatically balance load to provide low latency audio/video streams for thousands of WiFi users. Those environments are formed by an inhomogeneous ensemble of stationary and brought along devices. To proactively assist humans in reaching their goals, situation-related actions have to be planned and carried out on the basis of context sensing and analysis.

Planning is to find action sequences that fulfill the users' goals and are—in a certain sense—optimal. Next to optimization with metrics applied to the plan only, plans may be also optimized under consideration of the prospective course of events. The latter is reminiscent of anticipatory thinking, which takes part in human planning and also in human valuation of plans. Simulation is a common method to examine a system's future. In on-line simulation, a model is computed under consideration of the system's state and the simulation's results are used to influence the system. Research on simulation workflows present prospect of support for the above execution scheme of on-line simulation. Also of importance is the collection and processing of data from the simulation and from the environment.

Data play a central role in on-line simulation applications as data that are extracted from the environment are prerequisite for the simulation and data that result from the simulation are prerequisite for making decisions in the environment. The environments considered in this work are typically subject to changes of the presence of devices and users, changes of the connectivity and state of devices, changes of the users' goals, and changes of environmental properties. Those changes in the environment may imply changes in the simulation model and thus may necessitate changes in the collection and processing of data. Consequently, a flexible data collection and processing approach promises to improve the feasibility of developing on-line simulation systems and deploying them to smart environments. Ongoing work is powered by the vision of an on-line simulation system that can be built on language-based instrumentation for collecting data from the simulation and the environment in the same way. This includes to manage and process data between both worlds. For that, a stream-based approach is pursued in this work.

5 GRK 1480: PUMA - Programm- und Modell-Analyse

Prof. Dr. Helmut Seidl
Email: seidl@in.tum.de
TU München and Ludwig Maximilian Universität München
Internet: http://puma.in.tum.de

The doctorate program (Graduiertenkolleg) PUMA brings together the four fundamental approaches of program and model analysis, namely, type systems, theorem proving, model-checking, and abstract interpretation. Its goal is to develop new analysis techniques through cross-fertilization. The new methods should prototypically be implemented and be evaluated on selected analysis problems of software-intensive systems.

In the last years, four competing approaches for program and model have been developed: verification through theorem proving, model checking, abstract interpretation and via type systems. 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.

5.1 Decidability of linear tree constraints

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

We have been working on linear constraints over infinite trees, as introduced by Hofmann and Rodriguez. [1]. Since the general problem is not efficiently solvable, we restrict our attention to a subcase. This subcase, in its original form, is solved for lists as well as for trees.

This is done by reducing the tree case to the list case and then comparing growth rates. The problem in this approach is, that it just proves pure decidability. In fact, we set many potentials in the nodes to infinity. For a real resource analysis, this is only helpful to rule out contradictions a priori. But there is still need to optimize.

We are currently working on a strategy for comparing the strength of several constraints on the same variables, including the case where we have mutual dependencies. Before that, we have simplified the problem in several steps. And before that, we have given a formal derivation of the problem, as we are using it, from dulma Rodriguez' doctoral thesis, where it is defined in a slightly different way.

---

[1] Linear constraints over infinite trees, M.Hofmann, D.Rodriguez, LPAR: 18th International Conference on Logic for Programming Artificial Intelligence and Reasoning, 2012

5.2 Solving Forall-Exists Quantified Horn Constraints: A Temporal Program Verification and Synthesis Approach

Tewodros A. Beyene (`tewodros@model.in.tum.de`)
Supervisor: Prof. Andrey Rybalchenko

Temporal verification of universal (i.e., valid for all computation paths) properties of various kinds of programs, e.g., procedural, multi-threaded, or functional, can be reduced to finding solutions for equations in form of universally quantified Horn constraints extended with well-foundedness conditions. Dealing with existential properties (e.g., whether there exists a particular computation path), however, requires solving forall-exists quantified Horn constraints, where the conclusion part of some Horn constraints contains existentially quantified variables. For example, a deductive approach to CTL verification reduces to solving such clauses.

In this work, a method for solving forall-exists quantified Horn constraints extended with well-foundedness conditions is presented. The method is based on a counterexample-guided abstraction refinement scheme to discover witnesses for existentially quantified variables. [1] The practical promises of our solving method are demonstrated by applying the method across a range of interesting problems in formal methods. These problems including verification of CTL and CTL+FO [2] properties, and solving games (possibly recursive) over infinite graphs with applications in program synthesis and repair. [3] In this work, a number of sound and relatively complete proof rules that encode these problems using forall-exists Horn constraints are also proposed. We also present experimental evaluation of the method using challenging examples such as `PostgreSQL pgarch`, `Software Updates`, and various drivers from the Windows OS .

---

[1] Solving Existentially Quantified Horn Clauses, Tewodros A. Beyene, Corneliu Popea, and Andrey Rybalchenko. In CAV, 2013.

[2] CTL+FO Verification as Constraint Solving, Tewodros A. Beyene, Marc Brockschmidt, and Andrey Rybalchenko. In SPIN, 2014.

[3] A Constraint-based Approach to Solving Games on Infinite Graphs, Tewodros A. Beyene, Swarat Chaudhuri, Corneliu Popeea, and Andrey Rybalchenko. In POPL, 2014.

5.3 A Verified Compiler for Probability Density Functions

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

In 2013, Bhat et al. presented a compiler that computes the probability density function of a program in the probabilistic functional language Fun. Fun is a small functional language with basic arithmetic, Boolean logic, product and sum types, conditionals, and a number of built-in discrete and continuous distributions. It does not support lists or recursion. They evaluated the compiler on a number of practical problems and concluded that it reduces the amount of time and effort required to model them in an MCMC system significantly compared to hand-written models. A correctness proof for the compiler is sketched.

Bhat et al. stated that their eventual goal is the formal verification of this compiler in a theorem prover. We have verified such a compiler for a similar probabilistic functional language in the interactive theorem prover Isabelle/HOL. Our contributions are the following:

- a formalisation of the source language, target language (whose semantics had previously not been given precisely), and the compiler on top of a foundational theory of measure spaces

- a formal verification of the correctness of the compiler

- executable code for the compiler using Isabelle's code generator

In the process, we uncovered an incorrect generalisation of one of the compiler rules in the draft of an extended version of the paper by Bhat et al.

Our work shows not only that the compiler given by Bhat et al. is correct (apart from this mistake), but also that a formal correctness proof for such a compiler can be done with reasonable effort and that Isabelle/HOL in general and its measure theory library in particular are suitable for it. A useful side effect of our work was the formalisation of the Giry Monad, which is useful for formalisations of probabilistic computations in general. This work has also served as a benchmark of the current state of Isabelle's measure theory library; the difficulties we encountered have led to improvements e.g. in the automatic measurability prover, which will help make similar projects in the future easier.

The full formalisation is available online in the *Archive of Formal Proofs*: `http://afp.sourceforge.net/entries/Density_Compiler.shtml`

5.4 Inter-procedural Two-Variable Herbrand Equalities

Stefan Schulze Frielinghaus (`schulzef@in.tum.de`)
Supervisor: Prof. Dr. Seidl

Inferring invariants in programs which make use of complex operators as e.g. taking the square root or if the meaning of operators is even unknown, obvious methods for instance based on linear algebra fail. However, a true Herbrand equality holds irrespectively of the meaning of the occurring operator symbols. Such an interpretation then enables us to infer invariants even if complex operators are used.

The problem of inferring Herbrand equalities is known since the 70s where it was introduced by Cocke and Schwartz[1] as the *value numbering* problem. Since then algorithms have been developed in order to infer all valid intra-procedural Herbrand equalities. However, in presence of recursive procedures very little is known. Seidl et al.[2] showed that the intra-procedural techniques can be extended to programs with procedures and local but no global variables. Furthermore, the presented techniques are strong enough to infer all valid Herbrand constants for programs with recursive procedures possibly containing local and global variables, i.e., invariants of the form $\mathbf{x} \doteq t$, where t is ground. Another feasible case of invariants is obtained if only assignments are taken into account where the right-hand side contains at most one program variable. That means an assignment as e.g. $\mathbf{x} = f(5, \mathbf{y})$ is considered while assignments as $\mathbf{x} = f(\mathbf{y}, \mathbf{y})$ or even $\mathbf{x} = f(\mathbf{y}, \mathbf{z})$ are ruled out. Petter[3] shows that for such programs all inter-procedurally valid Herbrand equalities can be inferred.

We prove that all valid Herbrand equalities can be inter-procedurally inferred for programs where all assignments are taken into account whose right-hand sides depend on at most one variable. The analysis is based on procedure summaries representing the weakest pre-conditions for finitely many generic post-conditions with template variables. In order to arrive at effective representations for all occurring weakest pre-conditions, we show for almost all values possibly computed at run-time, that they can be uniquely factorized into tree patterns and a terminating ground term. Moreover, we introduce an approximate notion of subsumption which is effectively decidable and ensures that finite conjunctions of equalities may not grow infinitely. Based on these technical results, we realize an effective fixpoint iteration to infer all inter-procedurally valid Herbrand equalities for these programs.

---

[1] Cocke and Schwartz. Programming Languages and Their Compilers: Preliminary Notes. 1970

[2] Müller-Olm, Seidl and Steffen. Interprocedural Herbrand Equalities. 2005

[3] Petter. Interprocedural Polynomial Invariants. 2010

5.5 Negotiation games

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

Negotiations have been recently introduced as a model of concurrency with multi party negotiation as primitive. The model allows one to describe distributed negotiations obtained by combining "atomic" multi party negotiations, or *atoms*. Each atom has a number of *parties* (the subset of agents involved), and a set of possible outcomes. The parties agree on an outcome, which determines for each party the subset of atoms it is ready to engage in next.

Ill-designed negotiations may deadlock, or may contains useless atoms, i.e., atoms that can never be executed. The problem whether a negotiation is well designed or *sound* was studied in [1]. The main result was the identification of a subclass called deterministic negotiations, for which the soundness problem is tractable: while the problem is PSPACE-complete for arbitrary negotiations, it becomes polynomial for this subclass.

The original proof shows that in the sound case, the reduction procedure will terminate in a polynomial number of steps. Unfortunately, the unsound case is not studied in detail. In particular, no bound on the number of steps is given. Currently we are working on a slightly modified set of rules that will always terminate after a polynomial number of steps.

---

[1] Negotiations as a concurrency primitive 1 and 2, Javier Esparza end Jörg Desel

5.6 Formalization of Rigorous Numerical Methods and Applications

Fabian Immler (`immler@in.tum.de`)
Supervisor: 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.

5.7 An Analysis of Universal Information Flow based on Self-Compositions

Christian Müller (`christian.mueller@tum.de`)
Supervisor: Prof. Helmut Seidl

In order to analyze the information flow properties of a program, information flow lattices can be used which assign security levels to the program variables. The program is then deemed "secure" if there is no information flow from variables with a higher security level to one with a lower security level. Recent work has shown that results for all possible security lattices can be obtained from a universal information flow lattice.

We introduce a novel way of proving information flow properties of a program based on its self-composition. Our approach is based on the observation that information flow can be formulated as a hypersafety property. It 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. Accordingly, the analysis result is independent of specific information flow lattices, and allows to derive information flow with respect to any of these.

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. We prove the correctness of our approach by relating it to a Hoare calculus on self-compositions. Also, we indicate how it can be smoothly generalized to an interprocedural analysis.

5.8 Decision procedures with certification

Christian Neukirchen (`neukirchen@tcs.ifi.lmu.de`)
Supervisor: 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 an *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 datastructures and has low runtime and memory complexity.

In a Master's thesis,[1] we have implemented this technique for the propositional μ-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] Christian Neukirchen. "Computation of winning strategies for μ-calculus by fixpoint iteration". MSc thesis, LMU München (November 2014).

[2] Martin Hofmann and Harald Rueß. "Certification for μ-calculus with winning strategies". In: *ArXiv e-prints* (Jan. 2014). arXiv: 1401.1693 [cs.LO].

[3] Marijn J. H. Heule, Warren A. Hunt, Jr., and Nathan Wetzler. "Verifying Refutations with Extended Resolution". In: *Automated Deduction – CADE-24*. Vol. 7898. Lecture Notes in Computer Science. 2013.

5.9 Formalisation of Traffic Rules for Accountability of Autonomous Vehicles

Albert Rizaldi (`rizaldi@in.tum.de`)
Supervisor: Matthias Althoff

One important but rarely studied area in the domain of automated driving is the liability aspect of autonomous vehicles. If there is a collision involving an autonomous vehicle, it is unclear who should be held accountable for the collision. We address this issue by viewing traffic rules from legal texts as requirements for autonomous vehicles. If autonomous vehicles are engineered in such a way that they *always* comply with the traffic rules then they cannot be held accountable for a collision. To check compliance with traffic rules, we must specify them precisely and unambiguously. We therefore propose to formalise traffic rules from legal texts.

We select six rules which apply for highway scenarios from the Vienna Convention on Road Traffic as examples. These rules concern avoiding damage to road infrastructures and other road users; driving in the rightmost lane except for overtaking; adhering to speed limits; maintaining a safe distance; performing braking; and priority vehicles. All of these rules except the rule concerning a safe distance are concrete enough to be formalised. We concretise the notion of safe distance by mathematically deriving the formula such that the collision can be avoided if this distance is maintained. All of these rules have been formalised in Isabelle/HOL.

In addition to the formalisation of these traffic rules, we formalise the behaviour of autonomous vehicles as hybrid traces. We can think of hybrid traces as an abstraction for the data recorded in a black box for the purpose of accountability. With these formalised hybrid traces and traffic rules, we show how to derive a procedure to check whether a hybrid trace satisfies a specific traffic rules or not. As an example, we derive the procedure to check the rule about performing braking, and prove that this procedure checks the rule rigorously in Isabelle/HOL.

Apart for automatically checking the compliance of traffic rules, our work can also be used to assess a plan in path planning for autonomous vehicles. A generated plan for an autonomous vehicle and the predicted behaviours of other traffic participants can be translated into hybrid traces, and then verified with the derived procedure to see whether it is safe (avoid damage rule) and complies with other traffic rules.

5.10 An implementation of the Deflate compression standard in Coq

Christoph-Simon Senjak (`christoph.senjak@ifi.lmu.de`)
Supervisor: Prof. Dr. Martin Hofmann

The compression format "Deflate" is defined in RFC 1951. It is probably the most widespread format for compressed data, used in other formats (ZIP, GZip, HTTP, PNG, TLS). It can utilize prefix-free codings and back references. The standard is written informally, and there are formal shortcomings, which we try to fix by giving a rigorous mathematical specification. However, as specifications are axiomatic, it can only be proved that the described format is in fact a lossless format for compression, but not that is actually how the world understands "Deflate".

We addressed this problem in two ways: On the one hand, a design pattern was to keep the definitions simple and put the complexity of the implementation into the proofs, therefore making it easier to audit the given relations. On the other hand, as a proof-of-concept, we made a verified implementation of a decompression algorithm in Coq, using program extraction. This implementation works on very small files, and gives us empirical evidence that the relations we defined actually describe Deflate.

Our implementation introduces the concepts of strong uniqueness of a relation, meaning that there is at most one initial segment of a byte stream that can be parsed according to that given relation, and strong decidability, meaning that it is decidable whether such an initial segment exists. These propositions are, when expressed as dependent types, type signatures one would expect from parsers. With them, is easier to modularize our proof, and from (constructive) proofs of these, parsers can be extracted directly.

However, this original implementation had nonlinear runtime behavior and could only realistically be used to extract files of about 1 Megabyte. Through the usage of more efficient data structures[1], we were able to boost the performance drastically. We are currently at about 136 KB/min. This is still several magnitudes worse than the current unverified imperative implementations, but the whole algorithm can be extracted from a constructive existence proof, and we believe that there is even more room for improvement, and we will try to push this further, as we believe that it is an interesting case study for program extraction.

Still, we do not expect an extracted purely functional implementation to ever have competitive runtime behavior compared to a direct imperative low-level implementation. We therefore also plan to give a verified low-level implementation of Deflate.

---

[1] Chris Okasaki, "Amortization, Lazy Evaluation, and Persistence: Lists with Catenation via Lazy Linking", http://goo.gl/B0Jun4

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

Salomon Sickert (`sickert@in.tum.de`)
Supervisor: 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 modelled as an automaton fulfils 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 (generalised) 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 approach outlined there to support other temporal logics as a source, such as linear alternation-free μ-calculus. Furthermore it is planned to investigate if the target formalism of the translation can be changed to a different kind of ω-automaton such as the parity automaton. This step would enable the use of parity games to synthesize systems. 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 formalised and mechanically verified using the proof assistant Isabelle/HOL.

---

[1] J.R. Büchi: Weak second-order arithmetic and finite automata. Z. Math. Logik Grundlagen Math. 6, pages 66–92 (1960)

[2] Alonzo Church: Applications of recursive arithmetic to the problem of circuit synthesis. In: Summaries of the Summer Institute of Symbolic Logic, vol. I, pages 3–50. Cornell Univ, Ithaca, N.Y (1957)

[3] Edmund M. Clarke, E. Allen Emerson: Design and synthesis of synchronization skeletons using branching time temporal logic, Logics of Programs, Lecture Notes in Computer Science Volume 131, 1982, pages 52–71

[4] Javier Esparza, Jan Kretínský: From LTL to Deterministic Automata: A Safraless Compositional Approach. CAV 2014: pages 192–208

5.12 Verified Decision Procedures within the Logic-Automaton Connection

Dmytro Traytel (`traytel@in.tum.de`)
Supervisor: Prof. Tobias Nipkow, Ph.D.

Monadic second-order logic on finite words (MSO) is a decidable yet expressive logic into which many verification problems can be encoded. Since MSO formulas correspond to regular languages, equivalence of MSO formulas can be reduced to the equivalence of some regular structures, traditionally finite automata. However, formal verification of automata in interactive theorem provers is a difficult task. Instead, recursive data structures (such as regular expressions or formulas) simplify the formalization, notably by offering a structural induction principle.

We develop decision procedures for two different existing semantics of MSO: M2L(Str) and WS1S, that are not employing automata, and formalize them using the Isabelle proof assistant.

The first pair of decision procedures reduces equivalence of MSO formulas to equivalence of regular expressions. Decision procedures for regular expression equivalence have been formalized before, usually based on some kinds of derivatives (Brzozowski, Antimirov, etc.). We unify the different existing approaches in a common framework that essentially constructs a syntactic bisimulation.

For a straightforward embedding of MSO formulas into regular expressions an extension of regular expressions with a projection operation is required. We prove total correctness and completeness of an equivalence checker for regular expressions extended in that way. We also define a language-preserving translation of formulas into regular expressions with respect to the two different semantics of MSO.

Inspired by Brzozowski derivatives, we devise a notion of derivatives operating directly on formulas. Using formula derivatives, we obtain a second pair of verified decision procedures for MSO that does not require a translation of the input formulas into automata.

6 GRK 1564: INM - Imaging New Modalities

Prof. Dr.-Ing. Andreas Kolb
Email: andreas.kolb@uni-siegen.de
University of Siegen
Internet: 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.

6.1 Efficient, Robust, and Scale-Invariant Decomposition of Raman Spectra

Julian Bader (`julian.bader@uni-siegen.de`)
Supervisor: Prof. Dr.-Ing Andreas Kolb

Using Raman spectroscopy a sample is excited by a focussed high-intensity laser beam. The material is subject to fluorescent behaviour which is material dependent. Since Raman spectra convey characteristic information about the sample's chemical structure, Raman spectroscopy is used to identify unknown constituent minerals and their abundances.

A method has been developed for the identification of constituting pure minerals in a mixture by comparing the measured Raman spectra with a reference large database (> 2000 spectra). The spectra usually are preprocessed (e.g. normalized). Furthermore, the database contains measurements from different acquisition setups and devices which imposes intensity variations and shifts of the spectral peaks. Thus, the spectra are not directly comparable.

Our method [1] comprises of two major components: Firstly, a scale-invariant spectral matching technique allows us to compare measured spectra with the reference spectra from the database even when the band intensities are not directly comparable. Secondly, we use an iterative unmixing scheme based on the ISRA [2] algorithm in order to decompose a measured spectrum into its constituent minerals and compute their abundances.

Still, the spectral peak shifts are an open problem since it severely influences the result of the linear spectral unmixing process. Thus, in order to obtain a reliable identification of unknown constituent minerals, these shifts have to be detected and corrected.

---

[1] S. Bayraktar, B. Labitzke, J. Bader, R. Bornemann, P. Haring Bolivar, A. Kolb, "'Efficient, Robust, and Scale-Invariant Decomposition of Raman Spectra'", Proceedings of Signal and Image Processing Applications (ICSIPA), 2013

[2] M. E. Daube-Witherspoon and G. Muehllehner, "'An iterative image space reconstruction algorthm suitable for volume ect'", IEEE Trans. Med. Imag., vol. 5, no. 2, pp. 61-66, 1986

6.2 Detection and Recognition of Articulating Objects Using Distinctive Feature Sets

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

The objective of the proposed dissertation topic is to detect and recognize 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 recognizing 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-recognizing 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).

6.3 Compressive Sensing for Photonic Mixer Device

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

Time of Flight (ToF) sensors gather a depth image of the scene, that is, the information captured by the camera is no longer 2D but 3D, which can be used for 3D reconstruction or security. Unfortunately, ToF cameras usually provide low resolution images, often affected by considerable noise, related both to the estimation method and to several scene-dependent factors, such as the multipath effect, translucent objects, specular objects, powerful light sources or sunlight illumination. The focus of our research is on the PMD[1] technology, which estimates the difference of phase between emitted and received light signal using dual pixels that internally perform a correlation with a reference signal. Depth is computed from several phase measurements using different delays for the reference signal. This method for depth estimation avoids the need for high resolution time measurements, required for conventional ToF, but add eventual noise sources, that are related to PMD hardware characteristics. In addition, the limited dynamic range of PMD cameras often lead to the activation of their SBI for very close objects when sensing a distant scene, or under excessive illumination conditions, decreasing the accuracy of the short range measurements.

The aim of this work is to overcome the main limitations of PMD-based ToF technology and offer a higher resolution depth image with improved 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. Indeed, the information contained in a scene is independent from the number of pixels used to sense it and, therefore, it might be possible to recover it from few measurements if the image is sparse in certain domain. The application of CS recovery methods is, if possible, strongly coupled with -and probably constrained by- the peculiarities of the hardware and the estimation process. We face a strongly non-linear depth estimation process. Deep knowledge of the acquisition process, including an accurate characterization of the PMD pixels, is required for generating a reliable sensing model.

Preliminary experiments showed that recovery of PMD raw images is possible from as few as 50% of the original number of measurements (pixels), using an orthonormal Daubechies 4 wavelet dictionary as sparsifying basis. Current research also includes applying High Dynamic Range (HDR) techniques to ToF imaging in order to avoid SBI-related noise and improve accuracy and lateral resolution of the depth images at the cost of a lower frame rate.

---

[1] Photonic Mixer Device

6.4 Recursive State Estimation using Multiple Sensors

Lukas Köping (`lukas.koeping@uni-siegen.de`)
Supervisor: 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 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.

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

6.5 3D Sensor Data Fusion

Damien Lefloch (`damien.lefloch@uni-siegen.de`)
Supervisor: Prof. Dr. Andreas Kolb

Real-time 3D reconstruction receives further interest since the last years due to the availability of inexpensive consumer depth cameras (such as time-of-flight cameras or Microsoft's Kinect). Common 3D systems usually assume static scene to reconstruct the environment which leads to different problems concerning the reconstruction of dynamic scenes. The current research addresses this limitation using robust segmentation of rigid moving objects in order to avoid possible misleading reconstruction. In fact, the camera pose estimation (or camera tracking) based on point-to-plane Iterative Closest Point (ICP) is greatly improved in different scenarios using our robust dynamic segmentation.

Furthermore, the uncertainty of specific depth sensors highly influences the quality of the surface reconstruction. For example, ToF cameras are well known for their wide variety of measurement errors such as wiggling error or intensity-related depth error. Thus, 3D reconstruction pipeline needs to take into account anisotropic noise of depth sensors in order to reconstruct high-resolution models. Having reliable surface reconstruction would allow to generate ground-truth geometry which is currently lacking for computer vision and computer graphic systems.

Additionally, 3D reconstruction methods suffer from drift effect which is inherently due to the accumulation of camera tracking errors. These errors can be reduced applying different strategies which are the current investigation of the thesis.

6.6 Understanding of Object and Image Features at Human Perceptual Level

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

My research goal is to help computers see and understand images at high level perception. I am studying on the features that can be combined and used to represent objects and images at human perceptual level such as shape, color, texture, structure, etc... A better way of representing objects and scenes can lead to significant improvement on many computer vision applications, to name a few: object detection, recognition, matching, classification.

The work that I have been achived so far is finding keypoints that are important in representing objects. The keypoints are defined in such a way to convey shapes of the objects. They are selected at the objects' contours with high curvature. At these keypoints, curvature, dominant color structure and SIFT feature are combined to used as a new feature to build a descriptor.

One of possible applications that I am developing is to create super resolution images. The system will automatically detects correspondent points between high resolution image and low resolution image of the same or similar objects (with slightly different views) using the keypoints and features extracted from the above method. Once the correspondent keypoints are registered, the high resolution image will be warped to align with the low resolution image. The final high resolution output will be obtained by transfering the high pass details from the high resolution image to the lower one.

Another branch of work that helps to understand objects' shapes is to use different lighting conditions on the same scene to derive the objects' shape edges. The technique helps to separate all the detected edges in an image into texture edges and shape edges. These shape edges are then used to enhance the depth map resolution. In detail, the algorithm to extract depth edges from various lighting configurations is used from the paper "Light Montage for Perceptual Image Enhancement" published in Eurographics 2014 by Vlad Hosu et al. From the depth edges returned by the algorithm, I fine tuned the depth edges to eliminate texture edges and extract the object contours. These object contours will be used to fill in the gap in the depth map. It will also be used as a criterion to segment and interpolate the depth map. The final goal is to increase the resolution of the depth map.

6.7 Processing and Visualization of THz-Data

Martin Pätzold (`martin.paetzold@uni-siegen.de`)
Supervisor: Prof. Dr. Andreas Kolb

The lack of physical scattering models for describing wave effects, where wavelength and surface roughness of objects are in the same regime, leads to an uncertain interpretation of THz-Data. To simulate, analyze and visualize scattering behaviour of THz radiation anyway, a sparse voxel tree structure is under development. It allows to describe surfaces and their corresponding roughnesses in high resolution while not storing empty space in the same high resolution.

To obtain such a sparse voxel tree representation of objects for simulation, a voxelization of triangle meshes is developed. It exploits the high performance of the GPU while not being limited to the available memory of the GPU. This out-of-core approach allows a grid-free processing of triangles in a streaming manner by a preprocessing of triangles and a pooling of generated voxels. The preprocessing consists of a triangle sorting and a subdivision of triangles leading to a better workload balancing on GPU and a more constant memory usage for the pooling. Additionally, the flexibility of this approach allows an attribute creation of voxels after all intersecting triangles are determined. Order-dependent operations for creating voxel attributes become possible.

After creation of the sparse voxel tree, a fast ray-traversal is used for processing. This processing is performant due to the use of bit operations. Since largest empty subspaces of the voxel grid are always encoded by a single bit, an efficient empty space skipping can be performed. After the hierarchy of the sparse voxel tree is traversed, the attributes of the intersected voxels are used for visualization. The next step is to adjust this voxel attribute handling for the evaluation of surface roughness properties.

6.8 High-Resolution Texture Transfer

Marcel Piotraschke (piotraschke@informatik.uni-siegen.de)
Supervisor: Prof. Dr. Volker Blanz

When fitting the 3D Morphable Model (3DMM)[1] to blurred input images, fine structures of hair or skin, including pores and slight dermal irregularities, are not recovered, since those structures are beyond the level of detail represented in the 3DMM. To cope with this drawback, we propose a method that adds details exactly above the spatial frequencies captured by the 3DMM. They are derived from a small database of high-resolution photos of faces, and then transferred to new individuals.

Since it is unusual that the extracted information of one face perfectly represents the missing details of another face it is necessary to locate pairs of textures that are similar to each other. Furthermore instead of searching for a face that fits the requirements as a whole, we also implemented an approach to assemble the details of different facial regions (eyes, nose, mouth, ears, etc.) by looking for best matching areas. To minimize color shifts at the transitions of different regions, a basic color adjustment is applied. Moreover, texture blending of neighbored segments is used.
The similarity estimation is made by determining the Mahalanobis distance between different facial textures[2].

Sometimes artifacts appear if a global similarity of two segments is co-occurring with strong local differences. This was occasionally observed in the region of the eyes or the eyebrows. One idea to handle these remaining imperfections is to ensure similarity not only on the scale of facial segments but even for smaller regions, i.e. per block or pixel.

[1] V. Blanz, T. Vetter, *A morphable model for the synthesis of 3D faces*, SIGGRAPH Conference Proceedings, pp. 187-194, 1999
[2] K. Scherbaum, T. Ritschel, M. Hullin, T. Thormahlen, V. Blanz, H.-P. Seidel, *Computer-suggested facial makeup*, Eurographics, pp. 485-492, 2011

6.9 Kinect Range Sensing: Structured-Light versus Time-of-Flight Kinect

Hamed Sarbolandi (`hamed.sarbolandi@uni-siegen.de`)
Supervisor: Prof. Dr.-Ing Andreas Kolb

Recently, the new Kinect One has been issued by Microsoft, providing the next generation of real-time range sensing devices based on the Time-of-Flight (ToF) principle. As the first Kinect version was using a structured light approach, one would expect various differences in the characteristics of the range data delivered by both devices. This paper presents a detailed and in-depth comparison between both devices. In order to conduct the comparison, we propose a framework of seven different experimental setups, which is a generic basis for evaluating range cameras such as Kinect. The experiments have been designed with the goal to capture individual effects of the Kinect devices as isolatedly as possible and in a way, that they can also be adopted, in order to apply them to any other range sensing device. The overall goal of this paper is to provide a solid insight into the pros and cons of either device. Thus, scientists that are interested in using Kinect range sensing cameras in their specific application scenario can directly assess the expected, specific benefits and potential problem of either device.

6.10 Thermal Infrared Textures of 3D Faces

Björn Schiefen (`bjoern.schiefen@uni-siegen.de`)
Supervisor: Prof. Dr. Volker Blanz

Thermal infrared face images have become an encouraging topic in medicine and computer vision in the last years. In this respect the analysis and interpretation of facial thermograms seem promising for a large number of applications. One of these is face recognition, a topic that belongs to the most highly researched fields in the computer vision domain. Current algorithms often still lack the robustness and accuracy required of a field deployable system, despite the enormous effort, that has been made in this direction. One reason for this is the fact that the methods based on RGB images strongly depend on comparable and favorable acquisition conditions. An attempt to circumvent these disadvantages is to use a multimodal facial recognition approach that employs the mentioned thermal infrared spectrum besides the visible one.

In this context a representation of thermal face images has been introduced. The reasons for this are seen in the improvement of the thermogram comparability and in the enablement of a detailed analysis of these images. To generate this representation an uncalibrated acquisition system containing a RGB camera besides the infrared sensor is proposed. The following processing steps employ the 3D Morphable Model[1] to transform the acquired face thermogram with the help of the RGB image into a 3D representation similar to a RGB texture of a face model. By this form correspondence of the thermal textures is created that enables a correct and pixelwise comparison of face thermograms.

In a first step to analyze these thermal textures a database has been been build. To this purpose, several facial thermograms of the same person under changing conditions has been acquired as well as infrared images of several persons exposed to the same external factors. On the basis of a so processed infrared database, first steps to learn a statistical model has been made. The model should be able to describe the influence of external and internal factors on the infrared texture of a person. One of the goals behind this is to develop a preprocessing step, for example for recognition methods, in which the acquired thermal data is brought into a uniform status.

---

[1] V. Blanz and T. Vetter, "A Morphable Model for the synthesis of 3D faces", *Computer Graphics Proc. SIGGRAPH '99*, pp. 187-194, 1999.

6.11 Face and Situation Recognition

Davoud Shahlaei (`davoud.shahlaei@uni-siegen.de`)
Supervisor: Prof. Dr. Volker Blanz

Extreme lighting situations play a deciding and usually underestimated role in analysis and synthesis of faces in real life images and arts. The focus of my thesis is on estimation of the lighting from input image and separating extreme light effects from the face appearance to have intrinsic face features which is modeled with a 3D Morphable Model. Face analysis under uncontrolled lighting conditions involve solving challenging and interesting problems in computer vision and graphics. Lighting effects, such as specular highlights and cast shadows which appear under multi-directional colorful light sources, need to be studied and analyzed to allow analysis by synthesis of the intrinsic object. To render faces, a realistic reflectance function must be combined with 3D shape and diffuse albedo under a realistic lighting model. With the help of such realistic rendering and superposition principle for light, the light intensities are estimated as optimized non-negative parameters for a mathematical model of rendered images. The estimated light intensities can be used to reconstruct the scene, deilluminate the face image, and predict information about the situation of the scene. The physically plausible lighting can also be used for graphics use-cases such as appearance transfer, realistic adding of objects to the scene and lighting design, while the intrinsic face model can be used for enhancement of face recognition algorithms against complicated unknown lighting conditions. So far, the lighting estimation has shown promising results and opened the horizon for more in-depth work.

6.12 Secure and Robust Image Hashing Algorithm for Content based Image Authentication

Jinse Shin (`jinsuh.shin@uni-siegen.de`)
Supervisor: Prof. Christoph Ruland / Prof. Marcin Grzegorzek

The rapid development of mobile communication infrastructure and the recent advances in consumer electronic devices have allowed individuals to easily produce, distribute, and enjoy multimedia contents in digital form from anywhere at any time. In this context, the needs for trustworthy multimedia data have been raised. However, the emerging security demands are difficult to be met by the standardized cryptographic methods since the security requirements for multimedia data are different in many ways. For this reason, this thesis focuses on content based multimedia authentication – particularly for image data – in order to provide perceptual integrity.

This thesis firstly defines high level requirements for image authentication systems, followed by introducing the basic framework of content based image authentication as an alternative solution that can fulfill the requirements. Afterwards, an intensive literature review and comparative study on the image hashing technique are conducted as a promising component for content based image authentication. These studies provide a comprehensive perspective on the potential feasibility and limitations of the image hashing technique.

This thesis investigates the potential vulnerabilities and possible attack points on content based image authentication systems. Based on this security threat model, the limitations of current security mechanisms are addressed, and then a new framework is proposed to cope with potential security hazards.

Finally, this thesis proposes and evaluates a novel image hashing algorithm with simple and efficient tamper detection and localization capability for content based image authentication. In particular, the image-dependent key derivation stage using coarse image representation is introduced to enhance discriminability and security while the key-dependent Histogram of Oriented Gradients (HOG) computation in conjunction with Image Intensity Random Transformation (IIRT) is proposed to construct a robust and secure hash. An extensive performance evaluation on both the classical benchmarking images and a real tamper image database is conducted. It is observed that the proposed method achieves excellent discriminability and security while still possessing good robustness against JPEG/JPEG 2000 compression and transmission errors. Furthermore, the experimental results and Receiver Operating Characteristics (ROC) analysis demonstrate that the proposed method outperforms four representative image hashing algorithms with respect to discriminability and security.

6.13 Face Verification using an Active Multispectral SWIR Camera System

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

Biometric face recognition is becoming more frequently used and resembles a very important and active research topic. However, it still faces problems with spoofing attacks using facial disguises ("fakes"), such as masks, which can be manufactured using very different materials. As human skin color and texture also varies strongly, distinguishing genuine human skin from fakes is a very difficult task using only standard RGB imaging sensors.

This research project proposes a novel approach for face verification based on spectral signatures of material surfaces in the short wave infrared (SWIR) range, which are well suited for the detection of skin independent from skin type, gender or age and allow to distinguish authentic human skin reliably from other materials.[1] An active multispectral SWIR imaging system has been developed that acquires four-band multispectral image stacks in real-time. The system uses LEDs with four different peak wavelengths to emit pulsed small band illumination synchronized to the exposure of a camera with a broad band SWIR sensor. Compared to prior work on similar multispectral camera systems, this approach allows for both fast image acquisition and high spectral resolution and renders it widely independent of ambient light.[2]

Spectral signatures are extracted from each pixel of the acquired multispectral image stack. In parallel, faces are located and recognized in the images using state of the art methods. If a face is recognized, the spectral signatures within the facial area are classified. A face is verified only if the parts of the facial area that have significant influence on the recognition are classified as "'skin"'. For this purpose, a two-stage classification process is used: first, computationally inexpensive thresholding-based different filters find areas with skin-like pixel values. Only these pixels are then further evaluated by a more complex SVM classifier.

In a study with more than 135 participants we were able to show that the approach is feasible and achieves very good results. A variety of fakes, made of different materials such as silicon, latex, resin, paper or plastics, have been tested and were rejected with a precision of 99.968%.

---

[1] H. Steiner, O. Schwaneberg, N. Jung: "Advances in active near-infrared sensor systems for material classification and skin detection for safety applications", Safety Science Monitor, Vol. 17, 1, 2013

[2] H. Steiner, O. Schwaneberg, N. Jung: "'Design of an Active Multispectral SWIR Camera System for Skin Detection and Face Verification"', Journal of Sensors, 2015 (in press)

6.14 Shape-based Object Matching and Classification

Cong Yang (`cong.yang@uni-siegen.de`)
Supervisor: Prof. Dr. Marcin Grzegorzek

Shape matching and recognition is a fundamental aspect of many problems in computer vision. While rigid shape matching is relatively well understood, finding correspondences between pairs of shapes undergoing non-rigid deformations, such as articulated motion, remains challenging. Especially, non-rigid shape deformations can be classified into the coarse-grained deformation and the fine-grained deformation, respectively the topology and geometry of shapes are either very dissimilar (dog and tree) or similar (dog and cat). This research aims to develop novel shape representation and matching methods to recognise shapes with coarse and fine-grained deformations.

For shape representation, we proposed a simple shape descriptor that can be easily fused with other meaningful descriptors like shape context, etc. This leads to a significant increase in descriptive power of original descriptors without adding too much computation complexity. To make the proposed shape descriptor more practical and general, a supervised optimisation strategy is employed. Moreover, we also introduced an approach by fusing object skeleton and contour segments. The object contour is partitioned into segments by skeleton endpoints. Each contour segment is represented by a rotation and scale invariant, 12-dimensional feature vector. This descriptor is insensitive to object deformation since fusing skeleton and contour segments can capture the object deformation from both interior and exterior features. In addition to skeleton, we also proposed a method to generate robust contour partition points and applies them to produce point context and contour segment features for shape matching. The main idea is to match object shapes by matching contour partition points and contour segments. In contrast to typical shape context method, we do not consider the topological graph structure since our approach is only considering a small number of partition points rather than full contour points.

For object matching, the similarity of two objects is determined by matching their contour segments using the Hungarian algorithm. For skeleton, the matching is done in analogy to the path similarity skeleton graph matching method. By using a modified Dijkstra algorithm as well as OSB function, the matching costs for all feature pairs are calculated. For object classification, a multi-class Support Vector Machine (mSVM) is employed.

The experimental results demonstrate that our methods are able to produce correct results in the presence of articulations, stretching, and contour deformations. In the next steps we will focus on developing the method for fine-grained object deformations. One possible way is object matching and classification by hierarchical skeletons and hierarchical features.

7 GRK 1651: SOAMED - Service-oriented Architectures for the Integration of Software-based Processes, exemplified by Health Care Systems and Medical Technology

Prof. Dr. Ulf Leser
Email: leser@informatik.hu-berlin.de
Speaker: Humboldt-Universität zu Berlin
Participating: Technische Universität zu Berlin,
Charite Universitätsmedizin Berlin,
Hasso-Plattner-Institut für Softwaresystemtechnik, Potsdam
Internet:
http://www.informatik.hu-berlin.de/de/forschung/gebiete/soamed.de

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.

7.1 Action Refinement for Dynamic Event Structures

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

Prime event structures as presented by Winskel[1] have been extensively studied. They have proven to be well suited to model concurrent systems. In Van Glabbeek and Goltz (2001)[2] 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.

Arbach, Karcher, Peters and Nestmann (2015)[3] present an extension to prime event structures that allows dynamic creation and deletion of action dependencies. This extension is useful to model real world processes e.g. medical procedures.

We combine these two extensions (action refinement and dynamic creation and deletion of action dependencies). This allows us to use the top down approach to model systems while maintaining different abstraction layers. In addition we have the expressiveness and simplicity of dynamic event structures.

---

[1] Glynn Winskel, Event Structures, in: Petri Nets: Applications and Relationships to Other Models of Concurrency, LNCS 255, Springer, 1987.

[2] Rob van Glabbeek and Ursula Goltz, Refinement of actions and equivalence notions for concurrent systems, Acta Informatica Vol. 37, Springer, 2001.

[3] Arbach, Karcher, Peters, and Nestmann, Dynamic Causality in Event Structures, Technical Report, arXiv:1504.00512, 2015.

7.2 Data Flow Control in Distributed Systems

Wladislaw Gusew (`gusewwla@informatik.hu-berlin.de`)
Supervisor: 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 visualization 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 them 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, grid clusters or a cloud environment. Here, 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.

7.3 Process Information and Guidance Systems for Medical Treatments in Hospitals

Marcin Hewelt (`marcin.hewelt@hpi.de`)
Supervisor: Prof. Dr. Mathias Weske

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), we find hospital-specific organizational processes, like patient admission, and standard operating procedures (SOP) for common tasks. 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 give a graphical overview of 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 enactment in the PIGS 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.

The usefulness of every IT system is heavily dependant on its user interface. I envision a unified user interface for PIGS that visualizes treatment history, current activities, as well as recommended next steps of the treatment. Recommended activities, when selected by medical practitioners, are added to the treatment case and thus extend it. In this regard the visualization serves as an alternative graphical task list that allows to order medical procedures and enter their results. This requires an integration with hospital information systems, which usually store information about examinations, medication, and patients. The overall vision developed in my dissertation is that of non-invasive process support for medical treatment processes.

7.4 Higher-Order Dynamics in Event Structures

David S. Karcher (`karcher@soamed.de`)
Supervisor: Uwe Nestmann, Sabine Glesner

Event Structures (ESs) are a concurrency model introduced by Winskel[1]. ESs address the representation of direct relationships between individual events, usually capturing the notions of causality and conflict. Up to now, such relationships have been static, i.e. they cannot change during a system run. Thus the common ESs only model a static view on systems.

We dynamise causality such that causal dependencies between some events can be changed by occurrences of other events. We first model and study the case in which events may entail the *removal* of causal dependencies, then we consider the *addition* of causal dependencies, and finally we combine both approaches in the so-called *Dynamic Causality ESs*. For all three newly defined types of ESs, we study their expressive power in comparison to the well-known *Prime* ESs, *Dual* ESs, *Extended Bundle* ESs, and ESs for *Resolvable Conflicts* by van Glabbeek and Plotkin[2]. Interestingly Dynamic Causality ESs subsume Extended Bundle ESs and Dual ESs but are incomparable with ESs for Resolvable Conflicts. More details can be found in our paper[3].

Caused by this incomparability result, and based on the requirements of a case study with the Deutsches Herzzentrum Berlin, in which the treatment process of a patient is modelled, we generalise the Dynamic Causality ESs, in two ways. First we allow set of events to be modifiers (in a conjunctive interpretation, i.e. the modification only takes place, if all of the events of the set have occurred). Second we introduce higher-order dynamics, instead of the first order from above, e.g. in second order dynamics a modifier may let other events become adder (or dropper) of causal dependencies.

If we combine those two generalisation of Dynamic Causality ESs we get a new structure *Set-Based Higher-Order Dynamic Causality ESs* (shDCESs), which is strictly more expressive than ESs for Resolvable Conflicts, which can give semantics to general Petri nets.

As future work for one thing we plan to compare the expressive power of shDCESs with different level of dynamicity and link this to the π-calculus, for another we plan to evaluate this new structure in the above mentioned case study.

---

[1] G. Winskel. An introduction to event structures. In Linear Time, Branching Time and Partial Order in Logics and Models for Concurrency, volume 354 of LNCS, pages 364-397. Springer, 1989.

[2] R. van Glabbeek and G. Plotkin. Event Structures for Resolvable Conflict. In Proceedings of MFCS, volume 3153 of LNCS, pages 550-561. Springer, 2004.

[3] Y. Arbach, D. Karcher, K. Peters, and U. Nestmann. Dynamic Causality in Event Structures. In Proceedings of FORTE, LNCS. Springer, 2015.

7.5 Concurrency-based Transition Refinement for Constructing Services

Andre Moelle (`andre.moelle@informatik.hu-berlin.de`)
Supervisor: Prof. Dr. Wolfgang Reisig

A goal of service-oriented architectures (SOA) is structuring complex IT systems. The basic building block of a SOA is a *service*, which provides a clearly defined functionality via an *interface*. By cooperating, services add new functionality. As an example, let us consider an ordering process. This process uses services, for instance, to check the products' availability, to estimate the customer's trustworthiness or to arrange shipping. The latter service in turn addresses acquisition, packaging and transportation by using suitable services. Hence, a service often uses services of a lower level of abstraction.

Analogously, we can construct service along their level of abstraction: At first, we model an abstract service, which cannot be executed but already specifies the desired functionality. Then we repeatedly transform the model so that it can be decomposed into executable services. To prove that the repeatedly transformed model still specifies the desired functionality, we prove that each transformation preserves the desired functionality. A transformation preserving the desired functionality is called *refinement*. Consequently, services constructed by refinement are correct by construction.

The goal of my thesis is develop a theory for the construction of services by refinement. To this end, a service is modeled as Petri net and functionality is specified by temporal logic. That is, a Petri net N specifies a desired functionality if N satisfies the formula φ that corresponds to the desired functionality (Notation: $N \models \varphi$). A transformation corresponds to replacing a transition t of a Petri net N by another Petri net N_t; performing the transformation yields another Petri net $N[N_t/t]$. Furthermore, a transformation is a φ-refinement if $N \models \varphi$ implies $N[N_t/t] \models \varphi$.

We study refinements that satisfy the *block-condition* as introduced by Sibylle Peuker in her dissertation. The block-condition is stated in terms of concurrent runs. A *concurrent run* ρ of N is a Petri net that represents occurrences of transitions and their causal relation (Notation: $\rho \in Runs(N)$). Transforming a concurrent run by replacing each occurence of t by each concurrent run of N_t yields new runs. If we transform each concurrent run of N we obtain a set $Runs(N)[N_t/t]$. Then, the block-condition holds if $Runs(N)[N_t/t] = Runs(N[N_t/t])$.

We address the following research questions: (1) how to efficiently decide whether the block-condition holds, and, (2) how to efficiently decide whether a transformation preserves a formula φ. At last, we ensure the feasibility of our approach by validating them against case studies.

7.6 Privacy Aware Data Exchange in Distributed Health Infrastructures

Jan Hendrik Nielsen (`nielsen@soamed.de`)
Supervisor: Prof. Johann-Christoph Freytag, Ph.D.

Clinical trials allow for great insight into development of new treatments. They play a key role in the verification of medical findings. Generally, a clinical trial is being conducted on patients suffering a specific disease. In addition, healthy subjects, serving as a control group, are being involved to validate the assumption of a study. Usually, the amount of healthy and unhealthy individuals participating in a study is small. Often multiple research entities, such as hospitals, contribute to a study forming a *distributed health infrastructure* to increase the quality of gathered data. Commonly, the data is being released to maintain comprehensiveness of different studies.

Due to the sensitive nature of medical data, it cannot be released entirely. The detailed *microdata* imposes great privacy risks on the individuals represented by it when made public. Typically, data is being altered prior to release, i.e., such that individuals cannot be identified. One possible process of manipulating the microdata to meet certain privacy aspects is *anonymization*. The literature identifies two main approaches for data anonymization: (1) *Privacy-preserving data publishing* (PPDP) and (2) *privacy-preserving data mining* (PPDM). Recent developments of PPDM, like *differential privacy*, empower data holders to put a definite privacy constraint on the release of data. However, differential privacy deals with privacy protection at database query level—which makes it undesirable for clinical trials. In contrast, the the concepts of PPDP allow for releasing data collections as a whole while maintaining a high degree of privacy. The concepts of PPDP are well understood and being actively used in real life applications. Most notably, the concept of *k-anonymity* along with it's extensions *ℓ-diversity* and *t-closeness* has gained a lot of attention from the scientific community. These privacy concepts divide the microdata into *identifying* and *sensitive* information represented by *attributes* in a table-like data structure. While leaving the sensitive attributes unchanged, the identifying attributes are being altered such that they are becoming indistinguishable to a certain amount of individuals contained in released data.

However, little progress has been made in adapting the concepts of PPDP to protect more than one sensitive attribute. In a distributed health infrastructure, this scenario is induced by the existence of multiple entities. In this dissertation, we are going to identify demands of a distributed anonymization protocol and develop an algorithm tailored to these specific needs.

7.7 On the alignment of Business Models and Business Processes

Adriatik Nikaj (`adriatik.nikaj@hpi.com`)
Supervisor: Prof. Dr. Mathias Weske

The information technology is a key element of enterprises, facilitating and lowering the costs of the coordination and communication between the partners. For arriving at information systems of enterprises, the enterprises should be seen from three perspective: The business model perspective, which represent "what" the enterprises do to create, capture and deliver value; The business process perspective, which describes "how" value creation, capture and delivery is implemented on the operational level; And lastly, the information technology perspective which describes the underlying IT infrastructure that supports the business processes. Currently I am investigating in bridging the gap between business models, which focus on the value exchange among different enterprises (like e3-value), and the BPMN choreography diagram, which expresses the messages exchanged between enterprises at the operational level. The conceptual gap between the two is vast, but keeping them aligned is an important factor for the success of the enterprises. Additionally, in order to bridge the gap between the choreography model and its implementation, I am investigating the relationship of the choreography models and the implementation of RESTful interactions in the context of developing RESTful Web Services

7.8 Analysis of Services with shared Database

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

In a hospital typically many business processes, such as diagnosis, treatment, medication, etc. are executed. Often, all these business processes are as independent as possible and interact by asynchronous communication. Yet, all processes may share the same database, which stores e.g. information about the patients, available resources etc. As in these examples, not only communicating business processes, additionally a shared database, have to be considered, when analyzing business processes as they often work on underlying business data. In service-oriented architectures this is a typical scenario: many services use a shared database.

In the last few years the analysis of communicating services has been established and several analysis techniques as well as tools for practical purposes have been developed using formal methods, e.g. Controllability, Adaptability or Substitutability. All these techniques do not consider an underlying shared database. They focus on the behavior and communication of the services. On the other hand, it is known that if services can communicate data and are able to make data-dependent choices, many verification problems become undecidable.

Yet the analysis of services with a shared database can be tackled as follows: The interaction of the services and the database is restricted. E.g. by the assumption that no data-dependent choices by the services are made, it may be possible to adapt existing analysis techniques for services.

Furthermore, the access of many services to one database arises new characterizations of correct systems. Not only correctness of behavior, additionally correctness of the database, such as consistency and integrity of data may be considered. The behavior and interaction with the database of the system determines the data. Therefore, the analysis of the behavior can give new insights about the database to analyze and verify data correctness using formal methods.

7.9 Congestion Control for Routing Overlays

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

Distributed services and their requirements become more complex. In order to offer advanced services intermediary hosts, which for example perform additional calculations on the data, are introduced. Thus, instead of a direct connection between source and destination, traffic gets forwarded to intermediary hosts before delivering it to its original destination. 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 an overlay-aware algorithm which locally performs what we call joint congestion control for all flows traversing an overlay node. This needs to be combined with some form of end-to-end congestion feedback to avoid excessive queuing. Again, it seems wise to make use of the fact that intermediary overlay nodes already maintain per-flow status information: nodes in an routing overlay can (and should) actively contribute to per-flow congestion control by appropriate feedback and queue management. We believe that a hop-by-hop, backpressure-based congestion control scheme which actively handles per-flow backpressure between neighboring hops is a promising direction.

8 GRK 1763: QuantLA - Quantitative Logics and Automata

Franz Baader
Email: baader@tcs.inf.tu-dresden.de
TU Dresden and Universität Leipzig
Internet: 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 soft-skills courses offered by the participating universities.

8.1 Quantitative automata and logics for infinite discrete structures

Parvaneh Babari (`babari@informatik.uni-leipzig.de`)
Supervisor: Prof. Dr. Manfred Droste, Prof. Dr. Heiko Vogler

Both automata and logics are applied as modelling approaches in Computer Science. Since the early nineteen sixties, the connection between finite automata and monadic second-order logic has been established by Büchi and Elgot. Recently, a quantitative version of this result was shown for a new semiring weighted monadic second-order logic[1]. This new concept of logic was successful and soon was extended not only to words but also to other structures such as trees, traces, pictures, nested words or timed words. In 2009, a new kind of weighted automata was introduced which compute objectives like the average cost or the long-time peak power consumption. These automata are not semiring weighted anymore. The connection between such new kind of weighted automata and weighted logic was established both for finite and infinite words[2]. In this research, we mainly focus on two different structures: Pictures and data words.

The theory of picture languages as a generalization of formal string languages was motivated by problems arising from image precessing and pattern recognition, and also plays a role in the theory of cellular automata. The family of recognizable picture languages was defined in nineties and characterized by many different devices. The first part of this research is devoted to introduce a new kind of weighted automata operating on both finite and infinite pictures which can model average and long-time behaviors. In addition, we establish a new weighted monadic second-order logic and we show that a suitable fragment of this logic and our new weighted automata are expressibly equivalent [3].

In the second part of this research, we deal with the class of data languages which is a more general framework than timed languages. They are languages considered over a finite set of alphabets and a set of data, and have been characterized in several ways such as logic, monoid and an automata device equipped with a set of registers[4]. We establish an extension of these results to a weighted setting. In addition, we show a connection between the quantitative data languages and quantitative timed languages.

---

[1] M. Droste, P. Gastin. Weighted automata and weighted logics. Theoretical Computer Science, 380(1-2), 69-86 (2007).

[2] M. Droste, I. Meinecke. Weighted automata and weighted MSO logics for average- and longtime-behaviors. Information and Computation, 220-221, 44-59 (2012).

[3] P. Babari, M. Droste. A Nivat theorem for weighted picture automata and weighted MSO logic, in: LATA, Lecture Notes in Computer Science, 8977, 703-715 (2015).

[4] P. Bouyer, A. Petit, D. Thérien, An algebraic characterization of data and timed languages, in: CONCUR, Lecture Notes in Computer Science, 2154, 248-261 (2001).

8.2 User-Definable Concrete Domains

Claudia Carapelle (`carapelle@informatik.uni-leipzig.de`)
Supervisor: Prof. Dr. Markus Lohrey, Prof. Dr. Franz Baader

Aim of this PhD project is to investigate how to successfully include *concrete domains* (CDs) in logic formalisms to express *quantitative* statements.

A CD can be an arbitrary relational structure whose domain elements and relations we want to use to build the atomic formulas of our chosen logic formalism. According to what kind of *concrete properties* one needs to express, different domains are considered. Suppose we need to describe a program which manipulates integer values, then we can use the structure $\mathcal{Z} = (\mathbb{Z}, <, =)$ to express equality or order requirements on these values. Typical CDs include structures over $\mathbb{N}$, $\mathbb{Z}$ or $\mathbb{Q}$, strings, intervals and many others, and are often found in literature in relation to Description Logics[1].

Our main focus is on satisfiability: how do CDs affect the computational problem when integrated into a logic? The choice of the specific domain is crucial. For example, while the temporal logic LTL with local constraints over $\mathcal{Z}$ has a decidable (PSPACE-cpl.) satisfiability problem, replacing the order relation with the successor function $(\mathbb{Z}, =, =_{+1})$ leads to undecidability[2].

We study the branching time logics CTL* and ECTL*[3] with local constraints[4] and identify sufficient conditions on an arbitrary concrete domain $\mathcal{D}$ which guarantee that the satisfiability problem for such logics is decidable: (1) the relations of $\mathcal{D}$ should satisfy a negation closure condition, and (2) the relational structures which allow homomorphism to $\mathcal{D}$ can be characterized by a boolean combination of MSO and WMSO + B sentences[5].

We can show that $\mathcal{Z}$ satisfies both properties and therefore CTL* and ECTL* with constraints over such structure is decidable. As a consequence, we settle the open question by Demri and Gascon[6].

We then explore other possible domains to which our method results applicable, and identify more domains which enjoy property (1) and (2), as the class of *trees of fixed height, semi-linear orders* and *ordinal trees*.

We also prove that $\mathcal{T} = (\{0,1\}^*, \leq_p, \not\leq_p)$ ($\leq_p$ is the prefix relation) does not satisfy condition (2): using an EF-game we show that WMSO + B and MSO cannot give a characterization of those $\{\leq_p, \not\leq_p\}$-structures which allow homomorphism to $\mathcal{T}$. Note that this does not imply undecidability of the logic, only that our method cannot be applied in this case.

---

[1] See: Lutz, *Description Logics with Concrete Domains – A Survey*, 2003.

[2] D.Demri and D.D'Souza, *An Automata-Theoretic Approach to Constraint LTL*, FST TCS 2002.

[3] W.Thomas, *Computation tree logic and regular ω-languages*, Pr. Log. of Progr., 1983.

[4] L.Bozzelli and R.Gascon, *Branching-time temporal logic extended with qualitative presburger constraints*, Proc. LPAR 2006.

[5] M.Boyańczyk and S.Toruńczyk, *Weak MSO+U over infinite trees*, Proc. STACS, 2012.

[6] S.Demri and R.Gascon, *Verification of qualitative $\mathbb{Z}$ constraints* Th. Comp. Sci., 2008.

8.3 Quantitative Automata and Logics on Graphs

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

Recently, there has been much interest in quantitative features for the specification and analysis of systems. These features can be modelled by using quantitative automata and quantitative logic, which generalize classical automata respectively logics using weights.

We investigate these models and their relationship. For this, we use syntax and semantics of a quantitative logic; the semantics counts 'how often' a formula is true in a given word. For a survey on quantitative automata see the handbook[1]. The main result of Droste and Gastin[2], extending the classical result of Büchi, shows that if the weights are taken from an arbitrary semiring, then quantitative automata and a syntactically defined fragment of the quantitative logic are expressively equivalent. A corresponding result holds for infinite words and trees and extends to quantitative automata investigated by Henzinger et al.[3] with (non-semiring) average-type behaviors, or with discounting or limit average objectives for infinite words .

We investigated quantitative features of finite and infinite nested words in the form of weighted automata and weighted logics. We succeeded in proving an equivalence of quantitative automata and a suitable MSO logic over these structures and presented these results[4] at the 8th International Conference on Language and Automata Theory and Applications (LATA 2014).

Our goal is now to extend these results to more general settings and bigger classes of quantitative automata. For this, we recently introduced a weighted version[5] of Thomas'[6] graph acceptors and succeeded in extending Büchi- and Nivat-like results to this setting. As a consequence, we obtain corresponding Büchi-type equivalence results known from the recent literature for weighted automata and weighted logics on words, trees, pictures, and nested words. Establishing such a general result has been an open problem for weighted logic for some time.

---

[1] Droste, M., Kuich, W., Vogler, H. (eds.): Handbook of Weighted Automata. EATCS Monographs in Theoretical Computer Science, Springer (2009)

[2] Droste, M., Gastin, P.: Weighted automata and weighted logics. Theor. Comput. Sci., vol. 380, pp. 69-86 (2007)

[3] Chatterjee, K., Doyen, L., Henzinger, T.A.: Quantitative languages. In: Kaminski, M., Martini, S. (eds.) CSL. LNCS, vol. 5213, pp. 385-400, Springer (2008)

[4] Droste, M., Dück, S.: Weighted automata and logics for infinite nested words. In: Dediu, A.H., Martín-Vide, C., Sierra-Rodríguez, J.L., Truthe, B. (eds.) LATA. LNCS, vol. 8370, pp. 323-334, Springer (2014)

[5] Droste, M., Dück, S: Weighted automata and logics on graphs, submitted

[6] Thomas, W.: On logics, tilings, and automata. In: ICALP 1991. LNCS, vol. 510, pp.441-454, Springer (1991)

8.4 Quantitative methods for similarity and generalization in Description Logics

Andreas Ecke (`ecke@tcs.inf.tu-dresden.de`)
Supervisor: Prof. Dr.-Ing. Franz Baader

Description Logics (DLs) are a well-established family of knowledge representation formalisms, used to describe and reason about concepts and individuals. Given an ontology written in a particular DL, a DL system can be used to infer implicit knowledge from the ontology. Traditionally, such inference services, like subsumption and instance checking, only provide crisp answers, e.g., either one concept is subsumed by another one or it is not. However, one may also want to differentiate between concepts that are independent from each other: a concept may be more similar to certain concepts than to others, even though none of them are in a subsumption relation. *Concept similarity measures* (CSMs) may be used to compute those quantitative relations between concepts. Besides similarity measures between concepts, other measures to compute the similarity between individuals or ontologies have also been introduced and have many interesting applications.

While a lot of ad-hoc measures have been introduced and used for various purposes in DLs, formal properties used to classify those measures have only been investigated recently. My aim is to extend these results and study similarity measures and their applications. In particular, similarity measures can be used to generalize the crisp inferences available in traditional DL systems. For example, instance querying is an inference service that returns all those individuals in a given knowledge base that are instances of the query concept. Given an appropriate CSM, one may want to generalize the query to additionally return those individuals that are instances of concepts similar to the query concept[1]. These *relaxed instance queries* are useful for finding alternative solutions for many tasks. Another aim of my project is to investigate how similarity measures can be incorporated into the DL itself, e.g., as a concept constructor that is interpreted as the set of all individuals that have a certain similarity to a given prototype.

---

[1] A. Ecke, R. Peñaloza, and A.-Y. Turhan. Similarity-based Relaxed Instance Queries. In *Journal of Applied Logic*, 2015.

8.5 The Expressiveness and Path Checking Problems of MTL and TPTL over Data Words

Shiguang Feng (shiguang.feng@informatik.uni-leipzig.de)
Supervisor: Prof. Dr. Markus Lohrey, Prof. Dr. Manfred Droste

MTL (metric temporal logic) and TPTL (timed propositional temporal logic) are two extensions of LTL. In MTL, the temporal operators until (U) are indexed by time intervals. TPTL is a more powerful logic that is equipped with a freeze formalism. Alur and Henzinger[1] proved that MTL and TPTL are equally expressive over monotonic data words. Bouyer et al.[2] showed that TPTL is strictly more expressive than MTL over timed words.

We study the expressive power and complexity of TPTL and MTL over non-monotonic data words. We show that TPTL is strictly more expressive than MTL. As a tool for showing this, we introduce quantitative versions of Ehrenfeucht-Fraïssé (EF) games for MTL and TPTL. Etessami and Wilke[4] introduced the EF game for LTL and used it to show that the Until Hierarchy for LTL is strict. We prove a number of results concerning the relation between the expressive power of MTL and TPTL, as well as between different fragments of both logics. We investigate the effects of restricting the syntactic resources. We also use EF games to show that the problem whether a TPTL-formula is equivalent to an MTL-formula is undecidable.

Freeze LTL is a fragment of TPTL which can only do the equality test. Whereas freeze LTL model-checking for non-deterministic one-counter machine (OCM) turned out to be Σ_1^1-complete, the problem becomes PSPACE-complete for deterministic OCM[3]. We extend the PSPACE-completeness result for freeze LTL to TPTL over non-monotonic data words. We show that model-checking for TPTL over deterministic OCM is PSPACE-complete. The PSPACE-hardness already holds (i) for the fragment of TPTL with only two register variables and (ii) for full TPTL, where all constraint numbers are encoded in unary. On the other hand, if we restrict TPTL to (i) a constant number of register variables and unary encoded numbers in constraints, or (ii) one register variable but allow binary encoded numbers, then model-checking over deterministic OCM is P-complete.

[1] Rajeev Alur & Thomas A. Henzinger (1993): Real-Time Logics: Complexity and Expressiveness. Inf. Comput. 104(1), pp. 35–77.

[2] Patricia Bouyer, Fabrice Chevalier & Nicolas Markey (2010): On the expressiveness of TPTL and MTL. Inf. Comput. 208(2), pp. 97–116.

[3] S. Demri, R. Lazić, & A. Sangnier (2010): Model checking memoryful linear-time logics over one-counter automata. Theor. Comput. Sci. 411(22-24), pp. 2298–2316.

[4] Kousha Etessami & Thomas Wilke (1996): An Until Hierarchy for Temporal Logic. In: LICS, IEEE Computer Society, pp. 108–117.

8.6 Adding Threshold Concepts to the Description Logic $\mathcal{EL}$.

Oliver Fernández Gil (`fernandez@informatik.uni-leipzig.de`)
Supervisor: Prof. Dr. Gerhard Brewka and Prof. Dr.-Ing. Franz Baader

Description Logics (DLs)[1] are a well-investigated family of logic-based knowledge representation formalisms. They can be used to represent the relevant concepts of an application domain using *concept descriptions*, which are built from sets of *concept names* and *role names* using certain concept constructors. Using concept descriptions one can define important concepts of interest, by expressing the necessary and sufficient conditions for an individual to belong to the concept.

In particular the lightweight DL $\mathcal{EL}$, which offers the concept constructors *conjunction* ($\sqcap$), *existential restriction* ($\exists r.C$) and the *top concept* ($\top$), has shown to be of great interest. In $\mathcal{EL}$ we can, for example, define the concept of a *happy man* as a male human that is healthy and handsome, has a rich and intelligent wife, a son and a daughter, and a friend:

$$\mathsf{Human} \sqcap \mathsf{Male} \sqcap \mathsf{Healthy} \sqcap \mathsf{Handsome} \sqcap$$

$$\exists \mathsf{spouse}.(\mathsf{Rich} \sqcap \mathsf{Intelligent} \sqcap \mathsf{Female}) \sqcap$$

$$\exists \mathsf{child}.\mathsf{Male} \sqcap \exists \mathsf{child}.\mathsf{Female} \sqcap \exists \mathsf{friend}.\top$$

Since concept descriptions are interpreted using the classical semantics from first-order logic, for an individual to belong to this concept, it has to satisfied all the stated properties. However, maybe we would still want to call a man happy if most, though not all, of the properties hold.

In this thesis, we study extensions of $\mathcal{EL}$ that allow to define concepts in such an approximate way. The main idea is to use a *membership degree* function, which instead of giving a value in $\{0, 1\}$ to evaluate the membership of an individual into a concept, gives a value in the interval $[0..1]$. Then, from an $\mathcal{EL}$ concept description C, we can build the *threshold concept* $C_{\geq t}$ for $t \in [0..1]$ which collects all the individuals that belong to C with degree at least t. In addition, we also allow the construction of lower threshold concepts of the form $C_{\leq t}$ and the use of strict inequalities.

Finally, we investigate the computational properties of extending $\mathcal{EL}$ with threshold concepts using such membership degree functions. Basically, we look at standard reasoning tasks in DLs, e.g., *concept satisfiability*, *subsumption*, *ABox consistency* and *instance checking*.

---

[1] Baader et. al. The Description Logic Handbook: Theory, Implementation, and Applications, 2003

8.7 Weighted Automata Models over Discrete Structures

Doreen Heusel (`doreen.heusel@informatik.uni-leipzig.de`)
Supervisor: Prof. Dr. Manfred Droste

The topic of this research are weighted automata which model quantitative aspects of systems like the average consumption of resources. In particular, we investigate the support of these weighted automata, i.e., the language of all words which are evaluated to a non-zero value. We will consider the support of several weighed automata models over different structures like words, ranked trees, and unranked trees. As weight structure we will resort to valuation monoids which enable us to cope with average and which form a very general class of weight structures including semirings. The concept of valuation monoids is based on the ideas of Chatterjee, Doyen, and Henzinger.

Moreover, we present a new class of weighted unranked tree automata over valuation monoids and give a logical characterization for them. These new weighted unranked tree automata are expressively equivalent to a weighted MSO logic for trees, this solves an open problem of Droste and Vogler. Finally we wish to show a Kleene-type result for weighted tree automata over valuation monoids.

8.8 Stochastic Hybrid Systems

Daniel Krähmann (`kraehmann@tcs.inf.tu-dresden.de`)
Supervisor: Prof. Dr. Christel Baier

Since modern server clusters consume a huge amount of energy and the demand of computing power still increases, performance analysis of server farms is becoming an important area of research nowadays. To understand the sensitive interrelation between different resource allocation techniques and various mechanisms for dynamic power management, such as dynamic frequency scaling of processors and migration of virtual machines, a rigorous theoretical modeling and analysis framework is needed. We aim to provide a stochastic framework that enables probabilistic model checking for the design and quantitative analysis of heterogenous systems to exploit the full potential of dynamic adaption techniques.

The thesis will focus on developing such a framework based on stochastic hybrid system models. A hybrid system captures both, discrete and continuous behavior. The latter permits to model complex processes and phenomena (e.g., server cooling strategies or the lifetime and recovery time of a battery) using differential equations as well as differential inclusions.

As an integral feature, our framework to be developed aims to support compositional modeling, thus, we can model complex heterogenous systems out of components. Using the notion of signatures, one can specify properties of components and their interaction among themselves and with the environment in a separate fashion. On this basis, we seek for a notion of compositionality and compatibility of systems to capture the various communication layers in complex hardware and software systems. A challenge of the thesis is to establish several algebraic and congruence properties for the introduced formalism.

The known undecidability results for stochastic hybrid systems make it essential to study abstraction techniques. The challenge is to develop suitable approximation methods and algorithms that allow probabilistic model checking based on Markovian stochastic processes, and thus, a fine-grained analysis of large scale systems as server clusters and suited dynamic adaption strategies. We also consider the stability of our approximation methods with respect to our composition operator.

8.9 Compositionality in Probabilistic Model Checking

Linda Leuschner (`leuschner@tcs.inf.tu-dresden.de`)
Supervisor: Prof. Dr. Christel Baier

Probabilistic model checking (PMC) is a verification technique that aims to verify qualitative and quantitative system properties such as failure probabilities, energy consumption, system utility, or resilience.

Unfortunately, standard PMC techniques suffer from the well-known state-space-explosion problem: models of real-world systems often become infeasible large, which results in too much time and memory consumption when applying PMC to these models. One approach to cope with this problem is compositional verification, which benefits from the compositional structure that is inherent in most real-world systems. The compositional approach investigated in this thesis is probabilistic assume-guarantee reasoning (AGR). AGR is a two-step procedure: First, one states and verifies a quantitative assumption on one system part. Second, the verification of a system property is done on another system part using the assumption on the first system part.

One central goal of this thesis is to develop a new quantitative AGR approach based on conditional probabilities and Bayesian decomposition. This includes proof rules for approximating probabilities and expectations for various types of properties. The applicability of the rules will be shown by investigating several real-world examples, including an inter-process communication protocol with capability-based rights management, a security mechanism for control-flow checking, self-adaptive systems with interchangeable components, and a new nanowire-based transistor design.

First evidence the usability of our framework have been made by applying several proof rules on the inter-process communication protocol. We were able to decrease both, time and memory consumption while still providing sufficiently accurate probability bounds.

A further goal is to find more quantitative proof rules, targeting other classes of probabilistic properties, costs and rewards, and better approximations. We will show the applicability of these rules by applying them to the previous mentioned case studies, and we will use our framework for the analysis of more real-world systems.

---

[1] Christel Baier, Clemens Dubslaff, Sascha Klüppelholz, Marcus Daum, Joachim Klein, Steffen Märcker, Sascha Wunderlich, "Probabilistic Model Checking and Non-standard Multi-objective Reasoning". Proc. of the 17th International Conference on Fundamental Approaches to Software Engineering (FASE), volume 8411 of Lecture Notes in Computer Science, pages 1-16. 2014

[2] Christel Baier, Sascha Klüppelholz, Linda Leuschner, "Energy-Utility Analysis for Resilient Systems Using Probabilistic Model Checking". In Proceedings of the 35th Conference on Application and Theory of Petri Nets and Concurrency (PETRI NETS), volume 8489 of Lecture Notes in Computer Science, pages 20-39. 2014.

8.10 Alternative automata-based approaches to probabilistic model checking

David Müller (david.mueller@tcs.inf.tu-dresden.de)
Supervisor: Prof. Dr. Christel Baier and Dr. Karin Quaas

The growing complexity and dependence on computational systems in our every day life requires formal methods for verification to ensure liveness and safety. Classical model checking analyses whether a system satisfies certain properties. Probabilistic model checking (PMC) determines the likelihood of properties.

A common way for PMC is to model the system as a finite-state probabilistic automaton and a linear temporal logic (LTL) formula as specification. The standard approach for model checking converts the LTL formula to an equivalent deterministic automaton which can enforce a double-exponential blowup.

To relieve this double-exponential blowup, alternative automata formalisms with a restricted form of non-determinism have been discussed recently. This thesis will analyse the suitability of such automata in the context of PMC.

Benedikt et al.[2] have shown how unambiguous automata over finite and infinite words can be used to model check Markov chains. We will research this work by evaluating exhaustive case studies. A further goal is to introduce a new method for generating unambiguous ω-automata from LTL formulas.

Henzinger and Piterman introduced the good-for-games (GFG) property for nondeterministic ω-automata[3]. A GFG automaton does not need look-ahead to complete a finite run fragment. We have shown how a GFG automaton can be used to analyse Markov chains and Markov decision processes. Additionally we evaluated our method with a series of experiments[4].

Last year, the Hanoi Omega Format (HOA) has been developed[1]. The main purpose of HOA is a flexible exchange format for ω-automata. There exists already a preliminary integration into PRISM. This thesis will expand this integration and perform comparative experiments with several tools.

A further goal of the thesis is to develop the theoretical foundations and to perform comparative experiments with several acceptance conditions and automata with quantitative annotations.

---

[1] T. Babiak, F. Blahoudek, A. Duret-Lutz, J. Klein, J. Křetínský, D. Müller, D. Parker, and J. Strejček, "The Hanoi Omega-Automata Format", to appear

[2] M. Benedikt, R. Lenhardt and J. Worrell, "Two Variable vs. Linear Temporal Logic in Model Checking and Games", in LMCS 9(2), 2013

[3] T. Henzinger and N. Piterman, "Solving games without determinization", in CSL 2006, LNCS 4207

[4] J. Klein, D.Müller, C. Baier and S. Klüppelholz, "Are Good-for-Games Automata Good for Probabilistic Model Checking?" in LATA 2014, LNCS 8370

8.11 Weighted Automata and Logics
for Natural Language Processing

Johannes Osterholzer (`johannes.osterholzer@tu-dresden.de`)
Supervisor: Prof. Dr.-Ing. habil. Heiko Vogler

In syntax-based natural language processing (NLP), one uses trees to express the linguistic structure of an input sentence s. Thus the problem of determining the best linguistic analysis of s amounts to constructing a weighted tree language L which captures the linguistic understanding of the respective human language adequately, and devising an efficient search procedure for parse trees in L with maximal weight. The syntax-based approach to machine translation builds upon this premise by the application of a weighted tree transformation τ to the weighted tree language L_s of all parse trees of s in L. Many current translation systems employ (formalisms closely related to) regular tree grammars to model L, and (variants of) weighted extended top-down tree transducers for τ.

However, there is good evidence that human language exhibits phenomena that can only be captured by *mildly context-sensitive* formalisms. Their parse tree languages are no longer regular, but definable by (weighted) *context-free tree grammars (cftg)*[1,2]. These allow second-order substitution, i.e., the substitution of a symbol *within* a tree by a tree with variables. While the formal properties of cftg, and their associated automaton model, pushdown tree automata[3], were thoroughly investigated with regard to the theory of recursive program schemes, their application to NLP gives rise to several new questions. These comprise, i.a., closure properties of certain restrictions of cftg, as well as the precise relation of cftg to existing NLP formalisms, and lend themselves for a theoretical treatment.

Second-order substitution also promises an improvement in the quality of the tree transformation τ, and several transformation formalisms that make use of it have been proposed, such as *synchronous context-free tree grammars*[4]. Again, these new formalisms give rise to a number of research topics, regarding closure properties, relation to existing grammars and transducers, and their automated extraction from large sets of linguistic data.

[1] W.C. Rounds (1969). Context-Free Grammars on Trees. In *Proc. of STOC 1*, ACM, pp. 143-148

[2] S. Bozapalidis (2001). Context-Free Series on Trees. *Inform. and Comput.* 169(2), pp. 186-229

[3] I. Guessarian (1983). Pushdown Tree Automata. *Math. Systems Theory* 16(1), pp. 237-263

[4] M.-J. Nederhof and H. Vogler (2012). Synchronous Context-Free Tree Grammars. In *Proc. of TAG+11*, INRIA, pp. 55-63

8.12 Multi-weighted Automata Models and Quantitative Logics

Vitaly Perevoshchikov (`perev@informatik.uni-leipzig.de`)
Supervisor: Prof. Dr. Manfred Droste

In automata theory, the classical Büchi-Elgot theorem states that finite automata and monadic second-order (MSO) logic have the same expressive power. On the one side, MSO-logic gives a concise and intuitive way of specifying formal languages. On the other side, finite state automata enjoy interesting algorithmic properties. Recently, Droste and Gastin[1] introduced a weighted counterpart of MSO-logic. Their semiring-weighted MSO-logic can be considered as a weighted extension of classical MSO-logic by adding constants taken from a semiring. It was shown[1] that although, in general, weighted MSO-logic is more expressive than weighted automata, a syntactically restricted fragment of this logic is expressively equivalent to weighted automata. Thus, decidability results for weighted automata can be transferred to decidability results for weighted MSO logic.

Recently, multi-priced timed automata[2] have received much attention for real-time systems. These automata extend priced timed automata by featuring several price parameters. This permits to compute objectives like the optimal ratio between rewards and costs. Arising from the model of timed automata, the multi-weighted setting has also attracted much notice for classical nondeterministic automata[6].

The present thesis develops multi-weighted MSO-logics on finite[3], infinite[7] and timed words which are expressively equivalent to multi-weighted automata, studies decision problems for them. In addition, a Nivat-like theorem for weighted timed automata was proved[4]; this theorem establishes a connection between quantitative and qualitative behaviors of timed automata. Moreover, a logical characterization of timed pushdown automata was given[5].

---

[1] Bouyer, P., Brinksma, E., Larsen, K.G.: Optimal infinite scheduling for multi-priced timed automata. Formal Methods in System Design, 32(1), 3–23 (2008).

[2] Droste, M., Gastin, P.: Weighted automata and weighted logics. Theoret. Comp. Sci., 380(1-2), 69–86 (2007).

[3] Droste, M., Perevoshchikov, V.: Multi-weighted automata and MSO logic. In: CSR 2013. LNCS, vol. 7913, pp. 418–430. Springer (2013).

[4] Droste, M., Perevoshchikov, V.: A Nivat theorem for weighted timed automata and weighted relative distance logic. In: ICALP 2014. LNCS, vol. 8573, pp. 171-182. Springer (2014).

[5] Droste, M., Perevoshchikov, V.: A logical characterization of timed pushdown languages. To appear in CSR 2015.

[6] Fahrenberg, U., Juhl, L., Larsen, K.G., Srba, J.: Energy games in multiweighted automata. In: ICTAC 2011. LNCS, vol. 6916, pp. 95–115. Springer (2011)

[7] Perevoshchikov, V.: Weight assignment logic. To appear in DLT 2015.

8.13 Grammar-based statistical machine translation

Markus Teichmann (`markus.teichmann@mailbox.tu-dresden.de`)
Supervisor: Prof. Dr.-Ing. habil. Heiko Vogler

The aim of machine translation, a research field of natural language processing, is to use automated methods to translate from one natural language into another. Machine translation generally consists of three steps: i) Modeling: choosing a suitable formal representation of the natural languages and their connections; ii) Training: analyzing existing bilingual data to find the connection between the source and target language; and iii) Decoding: given a sentence in the source language, computing a translation in the target language.

In the syntax-based approach of machine translation weighted grammars play a fundamental role. The source-channel model uses a weighted grammar as a source language model to measure the grammaticality of sentences, and a synchronous grammar is used to derive sentence pairs of source and target language representing possible translations.

Traditionally, weighted grammars on strings were used for machine translation. Regular string languages, which are easy to compute, do not provide the required accuracy for good translations and were generalized to context-free string languages. The latter are closely connected to regular tree languages which additionally model the grammatical structure of sentences. Since natural languages are inherently compositional in its linguistic constituents, trees are a natural choice as the underlying data structure. Context-free tree grammars can be used to capture even more linguistic phenomena and thus improve the translation process. The flexibility of context-free tree grammars comes with high computational complexity which might render the use of such formalisms infeasible for current applications in natural language processing. Hence, a tradeoff between modeling capabilities and the computation costs is required, e.g. using restricted tree adjoining grammars[1]. Instead of restricting the formalism, context-free tree languages may be approximated by means of simpler formalisms. For example, regular tree languages might be used to overapproximate and thus reduce the search space of the translation process.

Furthermore, it is desirable to investigate the limitations of (restricted) context free tree grammars in their application to natural language processing. The identified boundaries motivate to extend existing formalisms and investigate new grammar formalisms which can capture such linguistic phenomena or allow for better translations.

---

[1] A.K. Joshi and Y. Schabes. 1997. Tree-adjoining grammars. In G. Rozenberg and A. Salomaa, editors, *Handbook of Formal Languages*, volume 3, pages 69–123. Springer

8.14 Probabilistic Logic and Probabilistic Automata

Thomas Weidner (`weidner@informatik.uni-leipzig.de`)
Supervisor: Prof. Dr. Manfred Droste

Probabilistic automata on finite words were introduced in the 1960s by Rabin. They are well-studied with manifold applications. Probabilistic automata on infinite words, investigated in 2005 by Baier & Grösser, also gained a lot of research interest. We introduce an extension of MSO logic by employing a new second-order expected value operator. We show a Büchi-result for this logic on both finite and infinite words. Extending the ideas of probabilistic regular expressions on finite words, we also obtain a Kleene-result for probabilistic automata on infinite words.

We then turn towards finite trees and give similar Kleene-result. For an extension of Büchi's theorem it turns out that probabilistic tree automata are not expressive enough to capture all semantics of probabilistic MSO on trees. Therefore we introduce bottom-up probabilistic tree automata instead of the usual top-down approach. Using this automata model, we obtain the desired Büchi result.

8.15 Model Checking and Weight Monitoring

Sascha Wunderlich (`wunder@tcs.inf.tu-dresden.de`)
Supervisor: Prof. Dr. Christel Baier and Prof. Dr. Markus Lohrey

Model checking is a well-established method for automatic system verification. Besides the extensively studied qualitative case, there is also an increasing interest in the quantitative analysis of system properties. Many important quantities can be formalized as the accumulated values of weight functions. These measures include resource usage such as energy consumption, or performance metrics such as the cost-utility-ratio or reliability guarantees. Different accumulation techniques like summation, averaging and ratios[1] are necessary to cover different quantities.

This thesis relies on weighted extensions of well-known modeling formalisms. Besides weighted Kripke structures, we investigate weighted probabilistic models such as Markov chains and Markov decision processes. Furthermore, we provide a specification language in the form of an extension of temporal logic with new modalities that impose restrictions on the accumulated weight along path fragments. These fragments are regular and can be characterized by finite automata.

In particular, we augment linear temporal logic (LTL) with accumulation constraints.[2] The resulting logic covers many of the properties expressible by formalisms that were introduced in the literature, e.g., the temporal logic extensions by Boker et al.[3] and the game-based mechanism by Chatterjee et al.[4]. We integrate an implementation for our logic with accumulation monitored by acyclic automata into the probabilistic model-checking tool PRISM. Currently, we are considering the decidability of flat automata as monitors as well as a corresponding formalism based on branching time logic.

The main goal of the thesis is to provide a general framework for the formalization and verification of system models and property specifications with accumulative values. This framework allows variation to weaker formalisms, like non-negative or integral weight functions and bounded accumulation. We study the border of decidability of the model-checking problem for different combinations of these restrictions and give complexity results and algorithms for the decidable fragment.

---

[1] C. Baier, C. Dubslaff, J. Klein, S. Klüppelholz, S. Wunderlich, "Probabilistic Model Checking for Energy-Utility Analysis", in Horizons of the Mind - A Tribute to Prakash Panangaden, LNCS 8464. Springer 2014.

[2] C. Baier, J. Klein, S. Klüppelholz, S. Wunderlich, "Weight Monitoring with Linear Temporal Logic: Complexity and Decidability", in Proc. of CSL-LICS. IEEE Computer Society 2014.

[3] U. Boker, K. Chatterjee, T. A. Henzinger, O. Kupferman, "Temporal specifications with accumulative values", in Proc. of LICS. IEEE Computer Society 2011.

[4] K. Chatterjee, L. Doyen, M. Randour, J.-F. Raskin, "Looking at mean-payoff and total-payoff through windows", in Proc. of ATVA, LNCS 8172. Springer 2013.

9 GRK 1765/1: SCARE - System Correctness under Adverse Conditions

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

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.

9.1 Decentralized Energy Conservation Techniques for Wireless Sensor Networks

Mohamed Abdelaal (`mohamed.abdelaal@informatik.uni-oldenburg.de`)
Supervisor: Prof. Dr.-Ing. Oliver Theel and Prof. Dr. Daniela Nicklas

The crux behind this work is to extend the lifetime expectancy of wireless sensor networks (WSNs). In particular, we target exploiting the trade-off between reducing certain quality-of-service (QoS) measures to a degree still tolerable by the application (such as, for example, precision and latency) and extending the application's lifetime. These approaches are classified into three main roots: Energy-cheap"' data aggregation, Virtual Sensing and Lifetime Planning. Currently, we have already achieved a reasonable progress as can be seen below.

In the first category, we propose a new data compression technique based on the so-called fuzzy transform, referred to as FuzzyCAT. It has been refined to minimize the recovery error even with high compression ratios via hybridizing the approximating function. Currently, we work on a cooperative prediction model through which a continuous data stream is guaranteed at the sink node. Next, we introduce a general module for pre-conditioning the sensor data prior to compression. The crux is to quick-sort the sensor data prior to being lossy-comprised. This idea bases on the fact that lossy compressors prominently resemble the behavior of low pass filters. The recovery mechanism comprises encoding the data indices using a lossless approach.

In the second category, virtual sensing is proposed a novel technique for decreasing the sensing unit energy consumption and simultaneously slashing the event-miss probability. Earlier, a technique, referred to as EAVS, has been proposed and a case study of gas leaks detection was given. Reliability of such systems composed of virtual and real sensors should be improved. An ontology on sensor-environment relationships is utilized to automatically generate rules before deployment to switch between real and virtual sensors.

Finally, we propose a novel method to (1) meet the expected network lifetime, and (2) achieve the best efforts QoS requirements. Our methodology here is to divide and conquer, where the entire node lifetime is viewed as a successive phases of fixed length. The core idea is to allow for a graceful degradation of the energy consumption throughout the entire lifetime. At each phase, the energy consumption as well as the QoS parameters of the previous phase are evaluated. Accordingly, the system reconfigures its parameters to wisely consume the allocated energy during the current phase. A predictive self-adaptive mechanism is required to perform such adaptations.

9.2 Verification Techniques for Dynamically Typed Programs

Björn Engelmann (`bjoern.engelmann@uni-oldenburg.de`)
Supervisor: 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 (1) 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.

9.3 Characterisation of synthesisability by Petri nets

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

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 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), we study necessary and sufficient conditions for (un)solvability of this transition system by a Petri net. 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.

9.4 Structure-Changing Systems as a Model of Adverse Conditions

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

Many discrete, concurrent systems can be modelled with Petri nets. When the system structure is not fixed but subject to change, extended formalisms are required. Graph transformation systems are among those formalisms that extend Petri nets to allow the explicit representation of structured states, and a dynamic connectivity. The expected operational behaviour (Sys) is described as a set of firing. Beyond that, adverse conditions by the action of the environment (Env) reflect the fault model. They can be modelled by structure changes in the net, and also represented as a set of rules. The goal of the proposed thesis is to provide a theoretically founded formalism for specifying properties of such systems subject to adverse conditions, and a proof-based approach to verifying these properties.

To this aim, we extend existing work on the correctness of graph transformation systems and graph programs. Correctness here is understood with respect to specifications consisting of pre- and postconditions in the form of graph conditions. Graph conditions, which exist in several variants, are graphical / algebraic expressions akin to formulae of graph logics. An important part of the thesis will be dedicated to the examination of the expressivity of new kinds of spatio-temporal graph properties, 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. There may be grades of correctness, and under certain adverse conditions it may be permissible to relax a specification. To address adverse conditions, it is further important to understand how to present an integrated view of the interplay of the environment and the system. It would not be reasonable to impose a sequentialisation or alternation on system operation and faults, as this does not do justice 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 via a shared state.

Case studies include data structures that are being concurrently modified by several processes, and where only consistent states, or such fulfilling some relaxed specification of consistency, should be reachable.

We have investigated language-theoretic notions of correctness and found that even very restricted structure-changing Petri nets have undecidable language inclusion in a given regular language. We are investigating methods for reasoning about state assertions, especially under the assumption of intermittent faults.

9.5 Verification of Stochastic Systems by Stochastic Satisfiability Modulo Theories with Continuous Domain

Yang Gao (`yang.gao@uni-oldenburg.de`)
Supervisor: Prof. Dr. Martin Fränzle

The idea of modelling uncertainty using randomized quantification was first proposed within the framework of propositional satisfiability (SAT) by Papadimitriou, yielding Stochastic SAT (SSAT)featuring both classical quantifiers and randomized quantifiers. This work has been lifted to Satisfiability Modulo Theories (SMT) by Fränzle, Teige et al. in order to symbolically reason about reachability problems of probabilistic hybrid automata (PHA).Instead of reporting true or false, an SSAT/SSMT formula Φ has a probability as semantics, which denotes the probability of satisfaction of Φ under optimal resolution of the non-random quantifiers. SSAT and SSMT permit concise description of diverse problems combining reasoning under uncertainty with data dependencies. Applications range from AI planning to analysis of PHA. A serious limitation of the SSMT-solving approach pioneered by is that all quantifiers (except for implicit innermost existential quantification of all otherwise unbound variables) are confined to range over finite domains. As this implies that the carriers of probability distributions have to be finite, a large number of phenomena cannot be expressed within the current SSMT framework, such as continuous noise or measurement error in hybrid systems. To overcome this limitation, relaxing the constraints on the domains of randomized variables (now also admitting continuous probability distributions in SSMT solving) is necessary. As PhD work, I am aiming at working out:

- a solving procedure for SSMT with continous domain (CSSMT), which can obtain safer bounds for approximating the probability of satisfaction w.r.t. CSSMT formulas. This work has partially been done by integrating classical SMT framework (DPLL) and Interval Constraints Propagation (ICP) with probability consideration.

- an efficient and scalable implementation of the CCSMT solver, which will be partially built on the iSAT/SiSAT tool sets.

- more case studies and application scenarios by applying CSSMT in particular to problems of highly automated driving maneuvers under uncertain perception, as pertinent to automotive assistance systems relying on complex sensors like computer vision.

9.6 Geometry-Predicting Ad-Hoc Routing Protocols for Car2X Applications

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

The present work is focus on the dissemination of warning and control information. This allows a vehicle to obtain and disseminate information about road accidents, traffic jam, and road surface conditions coming from other vehicles. Regarding this, we propose a new routing protocol named 'Traffic-Aware Segment-based Routing protocol (TASR)' which is based on evaluating traffic density and its connectivity in the next-to-next segment. TASR is a fully distributed protocol without the need of any pre-installed infrastructure, just relying on the mobile nodes. Its mechanism is designed to improve the success probability of routing protocols by dynamically estimating the multi-hop forwarding capabilities of road segments and the network connectivity among them. In this work, we in particular study the problem of efficient data delivery in VANETs subject to signal loss due to shadowing caused by obstacles in urban environments. Specifically, when a vehicle issues a delay-tolerant data query to some site, we propose techniques to efficiently route the packet to that site and receive the reply within a reasonable delay. We use a novel metric called estimated connectivity degree (ECD). This estimated connectivity correlates with connection probability, as it estimates connectivity of nodes on the segments, and can thus be employed to assess the connection quality of each candidate path between the source and destination. Geographical forwarding is then used to transfer packets between any two intersections or segments within the path. The selection of the road segments is made in a way that maximizes the connectivity probability of the selected path while satisfying quality-of-service (QoS) constraints on the tolerable delay within the network, bandwidth usage, and error rate. Simulations are performed which are indicate that the proposed technique is more accurate compared to the existing techniques and yields increased packet delivery ratio while reducing end-to-end delay. The future part of this work will focus on V2V and V2I communications where keys questions are still open, for example one possibility to provide better performance evaluation under diverse scenarios. These are two open questions for future work;

1. How average case performance evaluation in the present work for communication networks actually correlated to traffic statement? For example in emergency situation/safety related domain.

2. Also, a new cross-layered, hybrid protocol architecture that situationally selects different routing protocols will be considered.

9.7 Handling Delay Differential Equations in Automatic Verification of Hybrid Systems

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

Hybrid systems are mathematical models for real life systems whose behaviors involve a mixture of discrete and continuous dynamics. As the major focus in computer science is on 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]. 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 will 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. Hence, we can develop an automatic tool for safely analyzing and verifying hybrid systems involving DDEs [2]. Moreover, different kinds of DDE will be considered, like DDE with multiple different discrete delays, DDE with randomly distributed delay, or DDE with time-dependent or more generally state-dependent delay. Beyond that, Egger's method can be extended for integrating safe ODE enclosures into a SAT modulo theory (SMT) solver from ODE enclosures to DDE enclosures [3].

---

[1] Andreas Eggers, Martin Fränzle, and Christian Herde. SAT modulo ODE: A direct SAT approach to hybrid systems. In Automated Technology for Verification and Analysis, Springer 2008.

[2] Liang Zou, Martin Fränzle, Naijun Zhan, and Peter Nazier Mosaad. Automatic stability and safety verification for delay differential equations. In Computer Aided Verification CAV 2015.

[3] Andreas Eggers, Nacim Ramdani, Nedialko S Nedialkov, and Martin Fränzle. Improving the SAT modulo ODE approach to hybrid systems analysis by combining different enclosure methods. Software & Systems Modeling, pages 1-28, 2012.

9.8 Robust Spatio-Temporal Logic for Mobile Agents

Heinrich Ody (`heinrich.ody@uni-oldenburg.de`)
Supervisor: 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] Martin Hilscher, Sven Linker, Ernst-Rüdiger Olderog, and Anders P. Ravn. An abstract model for proving safety of multi-lane traffic manoeuvres. In *ICFEM*, pages 404–419, 2011.

[2] Martin Fränzle and Michael R. Hansen. A robust interpretation of duration calculus. In *ICTAC*, pages 257–271, 2005.

9.9 Graph Transformation Games as a Model for Systems under Adverse Conditions

Christoph Peuser (christoph.peuser@informatik.uni-oldenburg.de)
Supervisor: 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[1][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

$$Asm \vdash (Sys \parallel Env) \texttt{ sat } Spec$$

is instantiated with a system Sys and environment Env consisting of attributed graph transformation rules. Their composition $\parallel$ is a game with the specification $Spec$, a temporal graph condition, as the winning condition and $\texttt{sat}$ is the satisfaction of this condition, i.e. the existence of a winning strategy for Sys. Finally, the assumption Asm is a temporal formula, specifying the frequency with which the environment may interfere with the system.

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

---

[1] Karl-Heinz Pennemann. Development of Correct Graph Transformation Systems. PhD thesis, Universität Oldenburg, 2009.

[2] Christopher M. Poskitt. Verification of Graph Programs. PhD thesis, University of York, 2013.

9.10 Graph Conditions with Variables and their Application in Metamodel Instance Generation

Hendrik Radke (`hendrik.radke@informatik.uni-oldenburg.de`)
Supervisor: Prof. Dr. Annegret Habel, Prof. Dr. Ernst-Rüdiger Olderog

Increasing complexity in software systems calls for design concepts that allow an intuitive overview of a system. We model states by graphs and state changes by graph transformation systems. Structural system properties can be described by nested graph conditions [1].

Nested graph conditions cannot describe non-local properties (connectedness, circle-freeness). We propose HR* *conditions* [2], an extension of nested graph conditions by variables in the form of hyperedges, which can be replaced by graphs, according to a hyperedge replacement system.

The expressive power of HR* conditions lies between counting monadic second-order and second-order logic [3]. Thus, it is possible to express properties like the existence of paths, circle-freeness, or that a graph has as many *a*-labeled as *b*-labeled nodes.

We apply HR* conditions in the generation of UML metamodel instances. A type graph, specifiecd by an UML diagram, can be transformed into a graph grammar. HR* conditions can be used as application conditions for graph grammar rules. Our goal is to transform the OCL constraints attached to the UML model into HR* constraints and further to application conditions, allowing easy generation of metamodel instances [4].

---
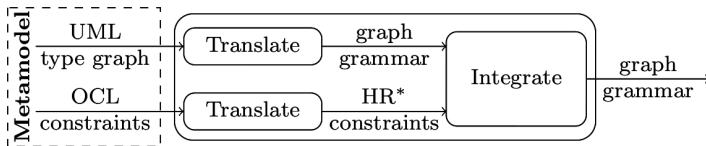
[1] A. Habel, K.-H. Pennemann. Correctness of high-level transformation systems relative to nested conditions. *Mathematical Structures in Computer Science*, vol. 19, pages 1–52, 2009.

[2] A. Habel, H. Radke. Expressiveness of graph conditions with variables. In *Int. Colloquium on Graph and Model Transformation*, vol. 30 of *Electronic Communications of the EASST*, 2010.

[3] H. Radke. HR* graph conditions between counting-monadic second-order and second-order graph formulas. *Electronic Communications of the EASST*, 2013. To appear.

[4] Arendt, Habel, Radke, Taentzer: From core OCL invariants to nested graph constraints. LNCS 8571, 97-112, 2014.

9.11 SGeoDTN+Nav: Secure Geographic DTN Routing with Navigation Prediction for Car2X Communication

Md Habibur Rahman (`md.habibur.rahman@uni-oldenburg.de`)
Supervisor: Prof. Dr. Werner Damm

Car2X communication based on IEEE802.11p is a specific kind of Vehicular Ad-Hoc Networks (VANETs) that provides road safety, and traffic efficiency for drivers including it distributed, self-organized, high speed, and vehicular mobility patterns. The basic idea is to allow cars to send traffic information to roadside units (RSU) or other car to communicate with each car using efficient routing protocols and maintaining vehicular mobility information. The position-based hybrid routing protocol is considered to be a very promising routing mechanism for the Car2X communication.

GeoDTN+Nav[1] is a position-based hybrid geographic and delay tolerant network (DTN) routing protocol with navigation assistance which uses GPS, digital map, global traffic, prediction, real-time vehicular density, and forwarding methods (restricted greedy forwarding, perimeter forwarding, and DTN forwarding) for VANETs. Our research to explore the GeoDTN+Nav routing protocol for the security and the data privacy issues such as jamming, manipulating routing algorithms, honeypot and sybil attack in city and highway environments.

In the evaluation of realistic and accurate Car2X communication solution through simulation, the mobility models play an important role in the reliability of the simulation results. Otherwise, non-realistic mobility models may overestimate the performance of protocols and algorithms. Usually, mobility models deal with speed, position, acceleration, deceleration, trip origin and destination, the number of vehicles departing within given time interval, and vehicles travel distance and time, among others. For the creation of realistic vehicular mobility models, microscopic and macroscopic characteristics are equally important. Many research studies neglected the macroscopic aspects such as Origin-Destination (O-D) model[2]. We employ realistic traffic simulation by integrating macroscopic and microscopic features with large scale scenarios by O-D metrics from the real-world road networks using SUMO. In the future, we will compare the performance between GeoDTN+Nav and SGeoDTN+Nav routing protocols using OMNeT++ which combine position, map and vehicular mobility for the Car2X communication.

---

[1] P. Cheng, K. Lee, M. Gerla, and J. Härri (2010). GeoDTN+Nav: Geographic DTN routing with navigator prediction for urban vehicular environments. Mobile Networks and Applications, 15(1), 61–82.

[2] J. Harri, F. Filali, and C. Bonnet (2009), Mobility Models for vehicular ad-hoc networks: a survey and taxonomy. IEEE Communication Survey Tutorial 11 (4), 19-41.

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

Dilshod Rahmatov (`dilshod.rahmatov@informatik.uni-oldenburg.de`)
Supervisor: 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:[2] 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] 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), Oct. 2013.

[2] M. Herlihy and J. M. Wing, "Specifying Graceful Degradation in Distributed Systems," in *Proc. of the ACM Symposium on Principles of Distributed Systems (PODC'87)*, F. B. Schneider, Ed., 1987, pp. 167–177.

9.13 Petri net synthesis and modal transition systems

Uli Schlachter (uli.schlachter@informatik.uni-oldenburg.de)
Supervisor: 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: Find an implementation 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 sends it. Initially the system is waiting for a request. This is depicted in the left part of the figure at the end.

In Petri net synthesis, the desired system is a Petri net and the state space is its reachability graph. Ehrenfeucht and Rozenberg introduced in 1989 region theory for solving this problem for elementary nets. 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.

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 chosing between several algorithms based on the input, so that simpler problems are solved via faster algorithms.

Based on this, the synthesis problem for modal transition systems is investigated and currently being solved. 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.
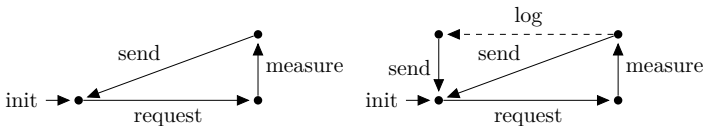
9.14 Intelligent Cyber Physical Social System

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

A cyber physical system is a collection of physical process in close coordination with automated workflows and processes to achieve a common global goal. Cyber physical systems are complex systems which monitor, sense or interact with the environment, gather information with the help of different types of sensors or mobile devices, propagate the sensed data to a processing unit via WAN, LAN, MANET, VANET or overlay network, the processing unit process, analyze and store the received data, and based on the nature of the data or input send instructions to actuators to alter or try to alter the environment, or raise alarm, or send notifications to concerned devices or peoples already registered with the CPS for a particular type of event. Designing such a complex system is not an easy task and there are a number of important factors that should be taken care while designing these systems. The problem area is divided into two parts. 1) Environment and 2) Human behavior modeling. Environmental challenge: Environment is meant to change and such kind of change is the biggest challenge for a CPS. Data for the CPS grows enormously with the passage of time and these tombs of data can be used to identify the patters of the environment change and the change frequency as well. Now-a-days, sensor, computing and storage technology is the more robust, cost-effective, less-intrusive and easy to install. By using both the data and technology in hand, CPS can be equipped with reasonable amount of artificial intelligence and learning. By enabling learning and intelligence in the CPS, real time decisions for alarming conditions can be made by CPS itself to some extent and this can reduce human supervision and will encourage unsupervised learning and monitoring. Human behavior modeling: Another important challenge for a CPS is human beings. According to FOGG behavioral modeling, personalities of human beings can be mapped into a personality matrix. Behavior of each personality type varies with a certain type of action. Now how a CPS can deal with this? How the CPS can identify the action for person? How the CPS will identify the personality type of a person? There are many other question in this regard which requires research to find out the answers.

9.15 Quality of Service Optimization in Self-adaptive Sensor Networks

Peilin Zhang (`peilin.zhang@uni-oldenburg.de`)
Supervisor: 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 decades, a wide range of WSN applications has been proposed such as environmental monitoring, forecasting systems, health monitoring, and so forth. In most of these 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 WSN is a challenging task, where these parameters are typically contradicting. Moreover, WSN resources such as power source, processing power, and memory are taxed.

In this work, we propose a self-adaptive planning strategy to optimize the application-relevant QoS parameters. Assuming the environmental dynamics, the node's entire lifetime is planned at design time. Specifically, this initial strategy ensures two aspects: (1) meet the expected lifetime; (2) achieve the best-effort QoS. Afterwards, as long as the current assumption is shattered, the lifetime of the sensor node would be re-planned at run time. Consequently, according to the acquired knowledge from the previous period, the local parameters such as transmission power, duty cycle, sampling rate, could be re-adjusted to attain the most acceptable QoS. Besides, we carry out the implementation and evaluation in our TelosB sensor nodes. At last, we compare the result of our approach to other related work in which the QoS provision is also closely considered.

10 GRK 1773: Heterogeneous Image Systems

Prof. Dr. Marc Stamminger
Email: marc.stamminger@informatik.uni-erlangen.de
University of Erlangen-Nuremberg
Internet: 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.

10.1 Motion Correction for Weight-Bearing C-arm CT of Knees

Martin Berger (martin.berger@cs.fau.de)

Supervisor: Prof. Dr.-Ing. Andreas Maier, Prof. Dr.-Ing. Joachim Hornegger, Prof. Rebecca Fahrig, PhD

It was shown that knee-joint kinematics are significantly different when using a weight-bearing instead of a non-weight-bearing acquisition protocol[1]. However, weight-bearing computed tomography (CT) or magnetic resonance tomography (MRT) remains difficult as the systems' geometry does not allow for a natural standing position of the patient. Recent advances in the design of C-arm Cone-beam CT scanners have enabled us to perform weight-bearing scans of the knee-joint in an upright, standing or even squatting position[2].

One of the main difficulties in weight-bearing C-arm CT imaging is patient motion. Fast shaking motion of the knee-joint results in motion artifacts in the reconstructed 3D image which can be observed as streaks or blurring. So far the motion was estimated by tracking externally attached metallic markers in the 2D projection images. However, the markers cause metallic artifacts and might not reflect the exact internal joint motion as they are attached to the skin. The goal is a motion correction approach that is purely based on acquired data and does not need an additional surrogate signal.

In a recent work we had access to a prior, motion-free volume acquired in a supine patient position[3]. After segmenting left and right Tibia and Femur in the motion-free scan we performed 2D/3D registration of each segmented bone to each of the weight-bearing projection images. We estimated 6 degrees-of-freedom for each bone and projection, by optimizing a gradient correlation similarity measure. Overall $6 \times 4 \times 248 = 5952$ parameters were estimated that fully describe the rigid motion of each bone over time. After combining the bone motions to a global motion field we were able to perform a motion compensated reconstruction. Qualitative and quantitative evaluation showed a substantial reduction of motion artifacts. For future work we plan to further improve the registration accuracy by a suitable regularization.

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

---

[1] Powers et al., "Patellofemoral kinematics during weight-bearing and non-weight-bearing knee extension in persons with lateral subluxation of the patella: a preliminary study.," JOSPT, vol. 33, no. 11, pp. 677–85, Nov. 2003.

[2] Choi et 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, p. 061902, Jun. 2014.

[3] Berger et al., "2D/3D Registration for Motion Compensated Reconstruction in Cone-Beam CT of Knees Under Weight-Bearing Condition," in World Congress on Medical Physics and Biomedical Engineering June 07-12, 2015, Toronto, Canada. (in press).

10.2 Vision-based Autonomous Navigation of Quadrotors in Unstructured Environments

Sergiu Dotenco (`sergiu.dotenco@fau.de`)
Supervisor: Elli Angelopoulou Ph.D., Akad. Rat, Prof. Dr.-Ing. Florian Gallwitz

In the past few years, unmanned aerial vehicles (UAVs) have become very popular due to their wide range of applications. In particular, UAVs are often used in locations that are inaccessible for ground vehicles, and especially for tasks that can be dangerous for humans, such as search and rescue, inspection and exploration, surveillance.

Today, most UAVs are operated remotely. However, often autonomy is desired or even necessary, especially if the connection between the UAV and the ground station is either unstable, or even impossible to establish. Limited bandwidth and communication delays are additional reasons why UAVs should be able to operate autonomously in unknown environment—both indoor, and outdoor.

The goal of this project is to enable a quadrotor UAV to autonomously explore and navigate in unknown, unstructured, GPS-denied environment. As the main vision sensor, we target monocular RGB cameras mounted on the quadrotor. Monocular cameras not only have a virtually infinite range, but also low power consumption, are lightweight and inexpensive. This is especially important, since most quadrotor UAVs have a flight time that typically ranges between 8 to 15 minutes.

In our latest work[1], we developed a method that enables a low-cost, off-the-shelf Parrot AR.Drone 2.0 quadrotor micro aerial vehicle (MAV) to detect a helicopter landing spot, autonomously approach it, and land on it. For this, we detect the landing spot using a forward-facing camera mounted on the MAV. As the landing spot, we use a heliport-like marker of known size. We estimate the distance between the quadrotor and the landpad, and employ a monocular simultaneous localization and mapping (SLAM) framework to let the quadrotor follow a trajectory in an accurate manner. Since the monocular SLAM framework is subject to drift, we recover from possible trajectory deviations by centering the quadrotor over the landpad once the MAV has reached the landing spot. Here, we use the quadrotor's downward-facing camera. Once the quadrotor has stabilized its position, it performs the landing.

---

[1] Sergiu Dotenco, Florian Gallwitz, and Elli Angelopoulou. "Autonomous Approach and Landing for a Low-Cost Quadrotor Using Monocular Cameras.". In: *Computer Vision – ECCV 2014 Workshops*. Ed. by Lourdes Agapito, Michael M. Bronstein, and Carsten Rother. Vol. 8925. Part I. Lecture Notes in Computer Science. Zürich, Switzerland: Springer International Publishing, 2015, pp. 209–222. ISBN: 978-3-319-16177-8.

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

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

In video surveillance and automotive applications, cameras with a very wide field of view of above 180 degrees are employed in order to survey a large area with a single camera. These so-called fisheye cameras produce images and videos which exhibit characteristics that are quite different from conventional rectilinear image and video data. The most prominent characteristic is radial distortion, which results directly from the fisheye projection function. Here, a hemisphere is mapped onto the image plane, leading to straight lines appearing curved in the captured image.

Typical signal processing techniques are not designed for this kind of data. In hybrid video coding, for example, motion estimation and compensation methods are usually based on a translational motion model, as translation is the most likely motion to occur in a moving scene. In the course of this project, the effect of radial distortion on video coding via H.265/HEVC was examined by comparing two different processing chains.[1] One processing chain applied distortion correction as a pre-processing step to the radially distorted video sequences. The other chain coded the original sequences, with distortion correction applied as a post-processing step, so that, in the end, the fisheye sequences were rectified. It could be shown that radial distortion adversely affects the coding efficiency since both intra-frame as well as inter-frame prediction techniques do not take such distortions into account. It was further concluded that exploiting the knowledge about the inherent fisheye characteristics should lead to gains in coding efficiency.

In the context of video coding, it was furthermore investigated how translational motion estimation can be efficiently modified towards equisolid fisheye video sequences, resulting in an adapted motion estimation technique.[2] Current investigations to that end also include applications to both error concealment[3] and super-resolution.

[1] Andrea Eichenseer and André Kaup, "Coding of Distortion-Corrected Fisheye Video Sequences Using H.265/HEVC," *Proc. IEEE International Conference on Image Processing (ICIP)*, pp. 4132–4136, Paris, France, October 2014

[2] Andrea Eichenseer, Michel Bätz, Jürgen Seiler, and André Kaup, "A Hybrid Motion Estimation Technique for Fisheye Video Sequences Based on Equisolid Re-Projection," accepted for *IEEE International Conference on Image Processing (ICIP)*, Québec City, Canada, September 2015

[3] Andrea Eichenseer, Jürgen Seiler, Michel Bätz, and André Kaup, "Temporal Error Concealment for Fisheye Video Sequences Based on Equisolid Re-Projection," submitted to *European Signal Processing Conference (EUSIPCO)*, Nice, France, September 2015

10.4 IP-Core Library for Designing Image Processing Operators on Reconfigurable Hardware

Konrad Häublein, Marc Reichenbach ({`konrad.haeublein,`
`marc.reichenbach`}`@cs.fau.de`)
Supervisor: Professor Dr. -Ing. Dietmar Fey

Porting image processing algorithms to reconfigurable hardware or ASICs is a challenging task. Especially when certain constraints, like real-time capability or limited hardware resources, need to be considered. In many cases the hardware designer has to invest quite much development time by mapping an algorithm into an application specific HDL code like Verilog or VHDL.

To tackle this issue the leading FPGA manufacturer started to push High Level Synthesis tools to the marked. These tools allow the developer to describe the target algorithm by a high level language like C++. Unfortunately, this form of code generation may lead to suboptimal resource utilization, and intensive long synthesis time, especially when the design gets more complex. In addition to that, the developer is bound to one FPGA fabric or family.

Therefore, we want provide an alternative approach for fast mapping of image processing operations to configurable hardware. With our IP-Core library we provide several blocks, which can be concatenated in order to form entire image processing operators. We define so called basic blocks, as a general structure for our operators. Since most local operators share similarities like neighborhood pixel access or convolution operations, such blocks can be reused for several operations. Adding scalable parameters to the blocks, like data width, filter or image size, allows even more flexibility. How even more complex operations, like the stereo matching technique, can be build in a scalable structure, has been demonstrated [1]. On top of this, we will provide structures for parallelization and resource sharing, in order to meet given non-functional constraints. Since each block is described in form of VHDL code, synthesis and implementation times remain low. Also, the library is supposed to target any FPGA architecture and may be even used to design ASICs.

In the future we would like to utilize our library to build more sophisticated operators like bilateral filterers or optical flow. Furthermore, we want to couple our blocks to an on-chip bus system like AXI-Stream, in order to provide a common interface for the IP-Blocks.

---

[1] Häublein, K., Reichenbach, M., Fey, D., "Fast and generic hardware architecture for stereo block matching applications on embedded systems", Proceedings of the International Conference on Reconfigurable Computing and FPGAs (ReConfig), Cancun,Mexico, 2014

10.5 Image Processing Architecture Synthesis (IPAS)

Christian Hartmann (`christian.hartmann@cs.fau.de`)
Supervisor: Professor 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. Due to continuous rising requirements on the one hand, and physical limitations of embedded applications concerning area, time and energy, embedded image processing systems become more heterogeneous for fulfilling their functions. These restrictions do not allow the use of oversized general purpose hardware architectures. It would lead to an approach of using more application-specialized computing architectures like GPUs 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. Therefore, the Image Processing Architecture Synthesis (IPAS) describes a new way for image processing design, [1] by considering the algorithm access pattern. 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, accurary) in the abstract specification the designer has the opportunity to alter the system architecture for their purposes.

[1] Hartmann, C., Yupatova, A., Reichenbach, M., Fey, D., German, R., "A Holistic Approach for Modeling and Synthesis of Image Processing Applications for Heterogeneous Computing Architectures", Proceedings of the HIS Workshop. Design, Automation and Test in Europe (DATE), Grenoble, 2015

[2] Hartmann, C.,Reichenbach, M., Fey, D., "IPOL - A Domain Specific Language for Image Processing Applications", Proceedings of the International Conference on Systems (ICONS), Barcelona, 2015

10.6 Estimating non-functional properties of embedded hardware

Arne Hendricks (`arne.hendricks@fau.de`)
Supervisor: Prof. Dr. Fey

In a world where processors and systems are shrinking continously both in size and energy consumption, energy awareness is not a plus but a must. Nowadays a hardware designer has to focus on making the hardware as energy efficient as possible while still maintaining suitable performance for the desired application. This can of course be difficult in some cases, and utmost care has to be taken. Our group of the RTG is working on methods of estimating time and energy consumption of a given software solution, without having to rely on the use of a traditional Cycle Accurate Simulator (CAS). A developer has to develop complicated test setups majo in order to obtain these non-functional properties of an application. Thus the code has to be compiled, executed on the target platform and measured using a power meter. He can also utilize Simulation Tools to achieve exact. These could be RTL (Register-TransferLevel) simulations or gate level simulations, where a CAS is simulating each clock-cycle within a microarchitecture. By counting glitches and transitions, very accurate power estimations can be achieved. Moreover, multiplying the simulated clock cycles with the clock frequency, the exact execution time can be determined. Unfortunately, CAS leads to very slow simulation speeds, due to the fact that they simulate the whole architecture. We propose to utilize a combination of functional simulation with a mechanistic extension to include non-functional properties. Estimations are obtained by combining results of a virtual execution unit with mechanistic modeling: Specific instruction counts relate to corresponding specific energies and times. Simulation results indicate that energy and time can be estimated with a mean relative error of less than 3 percent. Moreover, a test case shows that the results can also help choosing a suitable hardware for a given algorithmic solution. Our current status is that we are updating our simulation tool to include more sophisticated features of an architecture in the simulation. Since we focus on embedded hardware, right now the simualation is only taking into account very simple RISC based processors, such as the LEON3, which implements the sparc-v8 architecture. The LEON3 does however not include a branch predictor nor does it perform out of order execution. Our model has been recently updated with the goal to include cache effects in the non-functional property estimation and we have an upcoming publication during the RAW2015, to be released in the proceedings of the IPDPS2015. Further publications are planned. Future Work will include out-of-order executing processors such as newer ARM derivates as well as multi-core support.

10.7 Energy Consumption of Video Decoding Systems

Christian Herglotz (`christian.herglotz@FAU.de`)
Supervisor: André Kaup

Nowadays, systems being capable of replaying videos are used all over the world. Examples are portable devices like tablet PCs and smartphones or fixed devices like classical TV-sets and desktop PCs. Especially for portable devices that are battery driven, energy saving algorithms are highly desirable to extend operating times. In our work we investigate the state-of-the-art video codec HEVC[1] with respect to energy consumption on the decoder side.

In the first part of our research, we investigated how the energy consumption of different devices can be estimated. Therefore, a model has been proposed that is capable of accurately estimating the energy consumption of an HEVC decoder implementation.[2]

Furthermore, our research showed that, although video decoding is a highly complex and variable process, the decoding time provides a nearly proportional relation with the decoding energy.[3] The cited publication explains in detail under which conditions this linear relationship holds and confirms this result by testing various different decoder systems.

In another work, we focus on the architecture of a processor and try to derive a model for estimating the energy consumption of the processor core.[4] Recently, we have shown that we are capable of estimating the energy for cacheless CPUs, where current research aims at incorporating the cache into our estimation model.

In future work, we aim at utilizing this information to optimize the energy consumption of the processing systems. To this end, we plan to exploit the information provided by the decoder energy model in the encoding process to generate energy-saving video bit streams. Likewise, the processor model can, e.g., be exploited for creating energy-saving compilers.

---

[1] G. Sullivan, J. Ohm, W.-J. Han, T. Wiegand, and T. Wiegand, "Overview of the high efficiency video coding (HEVC) standard," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 22, no. 12, pp. 1649-1668, Dec. 2012.

[2] C. Herglotz, D. Springer, and A. Kaup, "Modeling the energy consumption of HEVC P- and B-frame decoding", *Proc. International Conference on Image Processing (ICIP),* pp. 3661 - 3665, Paris Oct. 2014.

[3] C. Herglotz, E. Walencik, and A. Kaup, "Estimating the HEVC Decoding Energy Using the Decoder Processing Time", *Accepted for International Symposium on Circuits and Systems (ISCAS),* 2015.

[4] C. Herglotz, A. Hendricks, M. Reichenbach, J. Seiler, D. Fey and A. Kaup, "Estimation of Non-Functional Properties for Embedded Hardware with Application to Image Processing", *Accepted for 22nd Reconfigurable Architectures Workshop (RAW),* 2015.

10.8 Scalable Global Illumination

Benjamin Keinert (`benjamin.keinert@fau.de`)
Supervisor: 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[4] we present methods to enhance performance and quality for the ray casting of procedural distance bounds. We propose a safe, over-relaxation-based method for accelerating sphere tracing. Second, a method for dynamically preventing self-intersections upon converting signed distance bounds enables controlling precision and rendering performance. In addition, we present a method for significantly accelerating the sphere tracing intersection test for convex objects that are enclosed in convex bounding volumes. We also propose a screen-space metric for the retrieval of a good intersection point candidate, in case sphere tracing does not converge thus increasing rendering quality without sacrificing performance. Finally, discontinuity artifacts common in sphere tracing are reduced using a fixed-point iteration algorithm.

Further research includes the development of efficient data structures and memory access schemes, which can be used to improve the sampling and data storage requirements of recent techniques (e.g. Rich VPLs[5]).

[1] James T. Kajiya. The rendering equation. In *Proceedings of the 13th Annual Conference on Computer Graphics and Interactive Techniques*, SIGGRAPH '86, pages 143-150, New York, NY, USA, 1986. ACM.

[2] Eric P. Lafortune and Yves D. Willems. Bi-directional path tracing. In *Proceedings of the Third International Conference on Computational Graphics and Visualization Techniques (COMPUGRAPHICS '93)*, pages 145-153, 1993.

[3] Eric Veach and Leonidas J. Guibas. Metropolis light transport. In *Proceedings of the 24th Annual Conference on Computer Graphics and Interactive Techniques*, SIGGRAPH '97, pages 65-76, New York, NY, USA, 1997. ACM Press/Addison-Wesley Publishing Co.

[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*, pp. 1-8. Cagliari, Italy: Eurographics Association, 2014.

[5] Florian Simon, Johannes Hanika, and Carsten Dachsbacher. Rich-VPLs for Improving the Versatility of Many-Light Methods. In *Proceedings of Eurographics 2015*.

10.9 Development of Image Guided Surgical Procedures

Jessica Magaraggia (`jessica.magaraggia@cs.fau.de`)
Supervisor: Prof. Dr.-Ing. Andreas Maier, Elli Angelopoulou Ph.D., Dipl.-Ing.
Gerhard Kleinszig

Fracture reduction and fixation are still usually performed on a free-hand basis. In the standard surgical workflow, the correct position of the implant and the screws can be performed under solely fluoroscopic control by means of a C-arm. The lack of 3D spatial information often leads to a trial-and-error process before screws can be properly positioned. Several navigation solutions were presented in the literature to support the surgeon during the procedure. However, standard navigation systems require the use of bulky markers, which need to be attached to both the surgical instrument and the patient.

The goal of this project is the application of our compact guidance solution[1] as mean of planning transfer during fracture reduction and fixation. The physician is provided with the possibility of planning the desired screw numbers and positions required for fracture fixation. The planning is based on X-ray images which can be acquired from the physician in the preferred direction. In our work, the transfer of the planning is then solely provided by a combination of local markers fixed onto a conventional drill guide used for drilling, which are seen from a camera fixed onto a standard surgical drill. No bulky markers for reference are required to be attached neither during the planning nor during the planning transfer. During the planning transfer, our framework allows the visualization in real-time of the reconstructed current instrument position and its offset w.r.t the planned one. For the calibration of the augmented drill sleeve and the camera-drill system, custom made calibration plates were developed.

The use of our compact guidance solution, as a mean of planning transfer for screw fixation, is expected to reduce the trial and error process and allows guidance support also for fractures at body locations for which the placement of bulky markers used in standard navigation systems would be cumbersome.

---

[1] Magaraggia, J., Kleinszig, G., Wei, W., Weiten, M., Graumann, R., Angelopoulou, E., and Hornegger, J., "On the Accuracy of a Video-Based Drill-Guidance Solution for Orthopedic and Trauma Surgery: Preliminary Results," in SPIE Medical Imaging 2014: Image-Guided Procedures, Robotic Interventions, and Modeling, 9036 (2014)

10.10 Thread Migration for Heterogeneous Coprocessor Systems for Image Processing Applications

Rainer Müller (`raimue@cs.fau.de`)
Supervisor: Prof. Dr.-Ing. 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 ineffient 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. This is also more flexible for applications with parallel workload largely depending on the input data, e.g. raytracing. Various thread migration strategies are possible for this approach, which also need to take shared memory between the host and possibly even multiple coprocessors into account. As the current common programming model forces the programmer to strictly decide which sections to be executed on which device before compilation, the resulting binary is also only usable for a single system. Instead, the binary for an application could contain code for different corprocessors 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.

10.11 Processing Architectures for Heterogeneous 3D-ICs

Benjamin Pfundt, Marc Reichenbach ({`benjamin.pfundt,`
`marc.reichenbach`}`@cs.fau.de`)
Supervisor: Prof. Dr.-Ing. Dietmar Fey

Stacking and connecting planar ICs has been researched for years, but technological advances made it a reality only today. Individual chips can be joined to a multi-layered chip and can be connected by thousands of so called through-silicon vias (TSVs). Many advantages arise from this assembly. First of all, a high bandwidth can be achieved by the massively parallel transmission utilizing TSVs. At the same time, the footprint of the chip decreases while parallel processing is increased. Furthermore, the interconnect length is reduced, thus low latencies can be realized.

However, an advantage which is essentially important for heterogeneous image systems is the tightly coupling of dies which were fabricated in different technologies. The combination of an analog image sensor on top and a digital processing unit on the next layer becomes possible. In this context we investigate the design of smart sensor chips together with mixed signal designers. Image acquisition, analog pre-processing and digital processing will be united into one compact IC. As a consequence, these chips could be employed in high-speed smart camera environments, where image processing algorithms should already be applied to the video stream.

Our focus in the research training group is the digital processing layer. To cope with the possibilities of 3D ICs, new processing architectures have to be developed. Currently, we concentrate on pre-processing algorithms which are applied directly on the raw sensor data. Especially filtering and simple feature detection tasks are commonly executed as first step. Since only a small area is required as input for the operations due to local data dependencies, parallelism can be exploited easily. Therefore, we developed an architecture which employs a partitioning scheme: an appropriate image sensor is divided into tiles which are read out and processed in parallel. Due to the parallel transmission and the low latency of the short interconnects, high frame rates can be achieved which are required for real-time processing[1]. Unfortunately, the high integration density in chip stacked systems renders heat dissipation and thermal stress critical. In our design approach, we try to alleviate these problems from the architectural side. The amount of used resources, i.e. logic, memory and TSVs, has to be kept minimal. For pre-processing algorithms a minimal temporary storage has been realized utilizing full buffering as only a certain image area is needed.

---

[1] Pfundt, B., Reichenbach, M., Fey, D., Söll, C., "Novel Image Processing Architecture for 3D Integrated Circuits", Proceedings of the 26th Workshop on Parallel Systems and Algorithms (PARS), Potsdam, 2015, to appear

10.12 Consistent Programming Models and Tools for Designing Heterogeneous Image Systems

Oliver Reiche (`oliver.reiche@fau.de`)
Supervisor: Dr.-Ing. Frank Hannig and Prof. 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 acellerator 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. 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 investigating novel parallelisation methods and code generation techniques, it is essential to consider new target architectures, e. g., embedded heterogeneous devices or FPGAs[1] for existing approaches like the HIPA^{cc} framework[2] for medical image preprocessing.

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] O. Reiche, M. Schmid, F. Hannig, and J. Teich, "Code Generation from a Domain-specific Language for C-based HLS of Hardware Accelerators." *In Proceedings of the International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), New Dehli, India, October 12-17, 2014.*

[2] R. Membarth, O. Reiche, F. Hannig, J. Teich, M. Körner, and W. Eckert, "HIPAcc: A Domain-Specific Language and Compiler for Image Processing." *In IEEE Transactions on Parallel and Distributed Systems, PP(99), 14 pp., [Early Access Article], 2015.*

10.13 Efficient Visibility Estimation

Kai Selgrad (`kai.selgrad@informatik.uni-erlangen.de`)
Supervisor: Prof. Marc Stamminger

An important component of global illumination systems is the determination of visibility between different scene positions. Employing this information the transport of light can be determined. Computing visibility between arbitrary scene elements is, however, a global problem and as such computationally very challenging. This is in contrast to "local illumination" which does not include visibility, or, equivalently, occlusion. The lack of such global illumination strongly decreases visual quality and the search for efficient solutions to the problem of visibility determination is, since long, an active area of research. Established fields of algorithms are, e.g., Ray Casting, Shadow Mapping Techniques and Voxelization.

Visibility can be computed by directly accessing scene geometry (Ray Casting), which is accurate, but suffers from being computationally expensive. Recent advances improve performance by better adaption to hardware, both on CPUs[1] and GPUs[2], as well as by algorithmic considerations[3].

Shadow Mapping[4] schemes are fast and used to estimate visibility between scene positions and a light source. Such approaches use a discretized subset of the scene geometry visible from the light source.

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

Our advances regarding 'fuzzy visibility', i.e. computation of soft shadows[5] and out-of-focus blur[6] show that this is a promising research direction.

---

[1] Manfred Ernst and Sven Woop, Embree: Photo-realistic ray tracing kernels, http://software.intel.com/en-us/articles/embree-photo-realistic-ray-tracing-kernels/, 2011

[2] Timo Aila, Samuli Laine, and Tero Karras. Understanding the efficiency of ray traversal on GPUs – Kepler and Fermi addendum. NVIDIA Technical Report NVR-2012-02, NVIDIA Corporation, June 2012

[3] Michal Hapala, Tomas Davidovic, Ingo Wald, Vlastimil Havran, and Philipp Slusallek, Efficient stack-less bvh traversal for ray tracing, In *27th Spring Conference on Computer Graphics (SCCG 2011)*

[4] Elmar Eisemann, Ulf Assarsson, Michael Schwarz, and Michael Wimmer, Casting shadows in real time, In *ACM SIGGRAPH ASIA 2009 Courses*, 2009

[5] Kai Selgrad, Carsten Dachsbacher, Quirin Meyer, and Marc Stamminger, Filtering multi-layer shadow maps for accurate soft shadows. In *Computer Graphics Forum*, 34(1):205–215, 2015

[6] Kai Selgrad, Christian Reintges, Dominik Penk, Pascal Wagner, and Marc Stamminger. Real-time depth of field using multi-layer filtering. In *Proceedings of the 19th Symposium on Interactive 3D Graphics and Games*, i3D '15, pages 121–127, New York, NY, USA, 2015. ACM.

10.14 Concept for a CMOS Image Sensor Suited for Analog Image Pre-Processing

Lan Shi (`lan.shi@fau.de`)

Supervisor: Prof. Robert Weigel and Prof. Marc Stamminger

From a scene to a digital image, an digital camera converts the light information to a digital electrical information through an image sensor. In the current digital camera market, image sensors are required to have higher performance but lower energy consumption, at higher speeds but smaller size than ever.

A digital camera with a CMOS image sensor offers significant advantages over traditional CCD in terms of low-power consumption, low-voltage operation use and monolithic integration. Otherwise, a CMOS sensor enables signals from each pixel in the sensor array to be read with simple row-column addressing techniques, which is not possible with CCD technology. With this advantage, the CMOS image sensor provides the Possibility of variations and improvements of data acquisition and image processing for computational CMOS image sensor, which integrates imaging elements and image processing circuitry at the focal plane.

A concept for analog image pre-processing based on CMOS image sensor is presented in our research [1]. A novel sensor data acquisition parallelism suited for real time image pre-processing is proposed. An image restoration algorithm for reducing image noise is applied as an example image pre-processing in the analog domain. Through simulation models, the image pre-processing is able to improve image quality in comparison to image pre-processing in the digital domain. Analog 2D signal processing prior to the A/D converter allows a better custom-tailored and more efficient filtering orientated to the detected kind of determined noise.

In our future work, some effective image restoration filters with different filter size will be designed in the analog domain. The analog image pre-processing at the frond-end of an image sensor and digital image processing can be integrated in 3D chips stacks for enhancing real time image precessing in smart cameras.

---

[1]Shi, L.; Soell, C.; Baenisch, A. Weigel, R.; Seiler, J. and Ussmueller, T. *Concept for a CMOS Image Sensor Suited for Analog Image Pre-Processing* In: DATE Friday Workshop on Heterogeneous Architectures and Design Methods for Embedded Image Systems (HIS),2015. pp. 16–21, March 2015

10.15 Integrated Circuits for Analog Signalprocessing in Heterogeneous Image Systems

Christopher Soell (christopher.soell@fau.de)
Supervisor: A. Baenisch, 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. Therefore, an image sensor system is developed and modified, so that it is able to execute analog computations[1]. Thereby, occurring overflows constitute a special challenge and have to be handled adequatley. Possible algorithms include tone mapping, de-noising, debayering and edge detection. As these do not only need the values of one pixel, but also take spatial informations 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. This will be done in collaboration with subproject A.2, whose digital chip is aimed to be connected to the image sensor by 3D chip stacking with the help of *Through Silicon Vias*[2]. Thus, not only a comparison of digital and analog processing operations is made possible, but also a decision whether it is more efficient to process the data in the analog or the digital domain, according to given constraints. Moreover, the analog operations can be controlled and changed by the digital processor, forming a mixed signal processor for smart camera systems.

---

[1] Lan Shi, C. Soell, A. Baenisch, J. Seiler, T. Ussmueller and R. Weigel, "Concept for a CMOS Image Sensor Suited for Analog Image Pre-Processing", Workshop on *Heterogeneous Architectures and Design Methods for Embedded Image Systems. Design, Automation & Test in Europe (DATE)*, Mar. 2015

[2] B. Pfundt, M. Reichenbach, D. Fey and C. Soell, "Novel Image Processing Architecture for 3D Integrated Circuits", accepted for Workshop on *Parallel-Algorithmen, - Rechnerstrukturen und -Systemsoftware (PARS)*, May 2015

10.16 Resource-aware Computer Vision Algorithms on Heterogeneous MPSoC Architectures

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

Here, of great importance are computer vision algorithms used to obtain information about the spatial position of objects in a scene. However, the efficient exploration of their capability to adapt to different environment conditions in real-time is still a challenge. Therefore, in order to provide applications more flexibility, a self-organizing computing paradigm can be used to support different mapping strategies. Our study presents the benefits of resource-aware computing by showing the efficiency and utilization improvements at real-time by algorithmic selection of different resources, such as TCPA (tightly coupled processor array) and RISC processors. More specifically, we investigate a dynamic load balancing between multiple RISC cores and a TCPA in order to satisfy different requirements as quality (e.g., accuracy of edge or corner detection) or throughput. The results are validated using experimental evaluation for different algorithms from video processing domain.

However, in such scenario where multiple processors accessing shared resources, such as cache, memory, and bus, leads to significant contention on them and the system performance might decrease. Moreover, the effect of shared resource contention worsens in the presence of multiple application scenarios with different execution and communication bandwidth requirements. To mitigate this problem, we propose a runtime reconfigurable arbitration technique[1] and a dynamic bus reconfiguration policy[2] that decides when to reconfigure a shared bus between Non-Preemptive Fixed Priority (NP-FP) and Time-Division Multiple Access (TDMA) scheduling. The required TDMA slot sizes are computed on-the-fly before NP-FP to TDMA reconfiguration such that deadlines of all hard real-time applications are satisfied and all soft real-time applications are serviced evenly. Our proposed dynamic bus reconfiguration policy has been implemented on a real MPSoC platform consisting of cores connected by the Advanced Microcontroller Bus Architecture (AMBA). The case studies demonstrate that reconfiguration of bus arbitration ensures that communication deadline constraints of hard real-time applications are maximally satisfied with low hardware and reconfiguration overhead.

[1] E. 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). pp. 74–81, Verona, Italy, Aug. 27-29, 2014

[2] D. Gangadharan, E. Sousa, V. Lari, F. Hannig, and J. Teich. Application-driven Reconfiguration of Shared Resources for Timing Predictability of MPSoC Platforms. In Proceedings of Asilomar Conference on Signals, Systems, and Computers (ASILOMAR). pp. 398–403, Pacific Grove, CA, USA, November 2-5, 2014

10.17 Real-time Facial Reenactment

Justus Thies (`justus.thies@cs.fau.de`)
Supervisor: Prof. Dr. Günther Greiner

The ongoing research in the field of Real-time Facial Reenactment results in new methods for interactive markerless reconstruction of human heads and photo-realistic expression transfer for real-time facial reenactment. These methods leverage the high computational performance of modern graphics cards and consumer level RGB-D sensors like Microsoft's Kinect or the PrimeSense Carmine. Nowadays, even smartphones and notebooks are equipped with such RGB-D sensors which allow a whole new brand of interactive applications. These applications have the focus on virtual/augmented reality and interactive reconstruction of objects (e.g. Real-time 3D reconstruction at scale using voxel hashing[1]).

To reenact the face of a target actor, the neutral face (identity) has to be reconstructed. Our reconstruction algorithm uses a statistical model as a prior (Interactive model-based reconstruction of the human head using an RGB-D sensor[2]). The statistical model is also called morphable model and has a known topology. Using this property a blendshape model is rigged to the morphable model which allows us to represent facial expressions in a reduced linear space.

To track the facial expressions of a source actor, these parameters of the reduced expression space are estimated by a GPU-based analysis-by-synthesis approach for each frame. Using these estimated parameters and the blendshape model, the identity of the target actor can be altered such that it replicates the expressions of the source actor. Finally, the modified face of the target actor is blended on top of the input RGB stream. A major challenge is to achieve a photo-realistic output. Thus, the blending method has to be chosen properly and a person specific texture has to be used.

We demonstrate our method in a live setup,where we modify a video conference feed such that the facial expressions of a different person (e.g. translator) are matched in real-time.

---

[1] Matthias Nießner, Michael Zollhöfer, Shahram Izadi, and Marc Stamminger. 2013. Real-time 3D reconstruction at scale using voxel hashing. ACM Trans. Graph. 32, 6, Article 169 (November 2013)

[2] Michael Zollhöfer, Justus Thies, Matteo Colaianni, Marc Stamminger, and Günther Greiner. 2014. Interactive model-based reconstruction of the human head using an RGB-D sensor. Computer Animation and Virtual Worlds. Volume 25, Issue 3-4, pages 213–222, May-August 2014

10.18 Indexbuffer Reordering for predefined Camera Routes

Christoph Weber (`christoph.weber@informatik.uni-erlangen.de`)
Supervisor: 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. For certain manufacturers, this kind of interactive dashboards has become the single selling point when advertising the car. 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. Finally we implement a depth sorting algorithm, that allows for an efficient but uncommon anti-aliasing technique, e.g. hardware based polygon smoothing.

---

[1] Weber, Christoph and Stamminger, Marc. Stateless Level of Detail Lighting for Automotive Visualization. Proc. Smart Tools and Apps for Graphics, 2014.

10.19 Mapping Data-flow Programming Model to Heterogeneous CPU-GPU Systems

Hao Wu (`haowu@cs.fau.de`)

Supervisor: Prof. Wolfgang Schröder-Preikschat and Prof. Marc Stamminger

Heterogeneous systems combining multi-core CPUs with many-core GPUs are commonly used for efficiently accelerating applications. To facilitate programming these heterogeneous systems and provide portable performance, data-flow programming model is an attractive approach. This model decouples logical dependencies among tasks and architecture topologies, which enables programmers to focus on application expression. For example, a number of image processing applications are composed of large graphs of many different operations, which can be described as a data-flow structure. This research work focus on the challenges of efficiently mapping this model to CPU-GPU systems which have discrete physical memory space.

Regarding exploiting computation resources, schedulers should maintain load balancing between CPUs and GPUs and avoid frequent data movements due to its non-trivial expense, especially when complexities of task dependency increase. In our previous work[1], a graph-partition-based policy is used to dispatch workload between a CPU and a GPU based on computation and data movement performance. With the global dependency and weight information, the scheduler can find out the partition solution in order to minimize connections between task sets on different processors. Compared to other queue-based scheduling policies, this approach is able to achieve a state-of-the-art performance and alleviate data movements when this overhead occupies a high ratio in throughput.

In terms of complex memory hierarchies on GPUs, using on-chip memory efficiently is important for achieving high performance during image processing. However, this on-chip memory with a small size requires immense effort for performance tuning. Therefore, a data-flow library to facilitate this on-chip memory usage is necessary for image processing applications. The challenges include how to separate data based on their access patterns, as well as operation fusions of different steps in order to raise the ratio of computations and data movements. Currently a library for partitioning image data and a prototype of computed tomography (CT) reconstruction have been implemented. The next step will integrate operation fusions and extend tests by more types of image applications.

---

[1] A Graph-Partition–Based Scheduling Policy for Heterogeneous Architectures, DATE Friday Workshop on Heterogeneous Architectures and Design Methods for Embedded Image Systems (HIS 2015)

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

Anna Yupatova, Vitali Schneider (`anna.yupatova@fau.de`,
`vitali.schneider@fau.de`)
Supervisor: Prof. Dr. Reinhard German and Dr. Winfried Dulz

Due to the increasing complexity of today's image processing applications as well as short response times and physical restrictions, image systems are becoming more heterogeneous, containing different compute resources such as general-purpose processors, custom hardware elements, and programmable logic units. Because of this heterogeneity, non-functional properties like execution time, or memory consumption need to be validated as early as possible, long before a system is available. Therefore, new methodology and simulation-based techniques, that improve the overall quality of the design process and enables the validation of no-functional properties, are desirable.

Our research focuses on the application of model-driven engineering (MDE) techniques in main phases of the development process: from system specification and design down to code generation, and validation. The key requirement for MDE techniques is to have a modeling language and a methodology that enable the design of system models. To specify widely diverse aspects of a multidisciplinary domain like image systems we propose a modeling methodology based on UML as a common language and several extension profiles standardized by the OMG group. The generic nature of UML allows to be additionally tailored by adding specific semantics for the simplifying and improving modeling of the image processing systems. Thus, based on UML modeling concepts, we are working on the Heterogeneous Image Processing Modeling Language that enables representing image processing directly in UML and refining them with special offerings captured by dedicated UML profiles[1]. We aim to realize our modeling approach as an UML conform language that is based on library, profiles, and templates.

Besides our ongoing work on the modeling approach, 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[2]. To better illustrate how the proposed modeling approach complements UML, and how it can be used, we provide a case study of camera-based Unmanned Aerial Vehicles (UAVs) system.

---

[1] A.Yupatova, V.Schneider, W.Dulz and R.German "Test-Driven Agile Simulation for Design of Image Processing Systems". In Pr.of 16th International Congerence on Advances in System Testing and Validation Lifecycle, Nice, France, Oktober 2014

[2] V.Schneider, A.Yupatova, W.Dulz and R.German "Merging OMG Standards in a General Modeling, Simulation, and Testing Framework". (to appear) In Pr.of the 8th International Conference on Simulation Tools and Techniques (SIMUtools 2015)

11 GRK 1780: CrossWorlds - Connecting Virtual And Real Social Worlds

Prof. Dr. Maximilian Eibl
Email: maximilian.eibl@informatik.tu-chemnitz.de
Technische Universität Chemnitz
Internet: 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.

11.1 Technisation of the Social in Social Robotics

Andreas Bischof (`andreas.bischof@phil.tu-chemnitz.de`)
Supervisor: Prof. Dr. Claudia Fraas (Chair of Media Communication)

Following recent publications on robotics - whether popular[1] or scientific[2] - robots are just about to populate our everyday life. Although this is rather a vision than a short term future, the popularity and presence of this term stands for the expansion of efforts in the field of social robotics. Scientists and engineers in the field of human-robot interaction (like before in HCI) turned to a broad variety of disciplines of social and life sciences to find and analyze structures and rules of everyday life that can be computed in complex machines like robots. But there is one perspective that is missing in almost every social robotics project: The social implications of designing and engineering such machines itself.

Therefore this PhD project focuses empirically on the design and construction of social robots as a crucial part of the answer to the question: How do social robots become social? Two dimensions critical to the social formation of such technologies are center of the research a) the discursive conditions of the possibility of social robots, and b) the modes of practice of undertaking social robotics. Following an ethnomethodological approach[3] the main sources for this empirical research are participant observations and expert interviews within social robotics research teams from Germany, the Netherlands, Denmark and the United States. The reconstruction of the socio-technological intertwining of their work is introduced by a historico-genetic contemplation: When and how became social scenarios emerged as a crucial interest of robotics?

The further research questions follow the procedure of 'sociality' in social robotics projects: Which theoretical paradigms are common in social robotics and how do they conceptualise sociality? How are these concepts translated in technical designs? How is the ensemble robot, (test) environment and (test) user made work? How are subsequently relevance and compability to the field of social robotics generated? Is there reversible Blackboxing[4] in the end? These questions aim to a reconstruction of the current answers to social robotics' central problem: to reduce the complexity of social reality. The study aims to be a contribution to both the social study of science and technology (STS) and human robot interaction (HRI).

---

[1] The Economist. New roles for new technologies: Rise of the robots (04/2014).

[2] Häselich, M. (2014). Aspects of Long-Term Autonomy of Social Robots and Their Potential Impact on Society.

[3] Garfinkel, H. (2002). Ethnomethodology's Program. Rowman and Littlefield.

[4] Latour, B. (1999). Blackboxing means that a functioning machine makes its internal complexity invisible. Pandora's hope: essays on the reality of science studies. Harvard University Press.

11.2 Digital Tangibles – Connecting Digital Worlds to their Physical Environments

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

Tabletops have been in the focus of Human-Computer Interaction for about 20 years. They proved to be of high value when it comes to attracting attention or bringing together larger user groups. By arranging user interfaces on public or semi-public displays, these devices create environments that enable users to operate applications both alone or in 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. Sensors like cameras or RFID readers even support the inclusion of secondary objects.

In a first study, this architecture will be tested in a museum. The use case, which was developed for this use case, requires visitors to first explore their physical environment and then import certain aspects of it as tools into their handheld devices. These can be used to manipulate information or objects that are part of the context of the tabletop.

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

---

[1] Müller-Tomfelde, C., Fjeld, M. (2010) A Short History of Tabletop Research, Technologies, and Products. In: Müller-Tomfelde, C. Tabletops - Horizontal Interactive Displays. Springer London. p. 1-24.

[2] Ishii, H., Ullmer, B. (1997) Tangible Bits: Towards Seamless Interfaces Between People, Bits and Atoms. In: Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems. ACM New York, NY, USA. p. 234-241.

[3] Weiss, M., Hollan, James D. & Borchers, Jan (2010) Augmenting Interactive Tabletops with Translucent Tangible Controls. In: Müller-Tomfelde, C. Tabletops - Horizontal Interactive Displays. Springer London. p. 157-180.

11.3 Physical Practice in Virtual and Real Environments

Steve Funke (`steve.funke@phil.tu-chemnitz.de`)
Supervisor: Prof. Dr. Peter Ohler

Research summary. Information and communication technology (ICT), that allows visualisation of and interaction with virtual three-dimensional worlds, is already commercially available for a broader audience than a few years ago. That what makes them interesting are the three-dimensional user interfaces (3D UI). They allow the user to interact with virtual objects, environments, or augmented information by direct three-dimensional input in the virtual and / or physical space [1].

With 3D UIs motor tasks can be accomplished without any conventional input devices (i.e. mouse, keyboard, joystick). The interaction techniques performed directly in the 3D spatial context can be treated as movements. Whole as well as partial body movements can be performed to accomplish the specific tasks in the virtual environment (i.e. throwing a virtual object into a target). Explanations about why people perform different skills to solve a motor task are provided by theories of motor control and motor learning [2]. Several approaches of motor research from cognitive psychology (i.e. schema theories [3]) as well as a few action-approaches (i.e. synergetic theories [4]) prefer quantitative analysis of simple and complex structured forms of movements. To compare the degree of match between the user's solutions of a motor task provides insight into the mechanisms of the human motor system as well as the motor learning process. We suppose that physical practice in virtual environments can support the user to solve motor-equivalent real world tasks in accordance to variations within physical practice.

The general assertion is that nothing about the human motor system has yet been learned through any prior user studies that involve manipulation in virtual environments because they forgot the systematic variations of the motor tasks and the conditions of practice. From this content-wise focal point we start a discussion of the need to consider how motor learning occurs, and the cognitive effort [5], when designing studies of user interaction.

---

[1] Bowman, D.A., Krujiff, E., LaViola, J. J. (2005). *3D user interfaces: theory and practice.* United States of America: Addison-Wesley.

[2] Magill, R. A. (2011). *Motor learning - concepts and applications.* Louisiana: McGraw-Hill.

[3] Schmidt, R. A. (1975), A schema theory of discrete motor skill learning. *Psychological Review, 82*, pp. 225-280.

[4] Schöner, G., Haken, H. & Kelso, J. A. S. (1986). A stochastic theory of phase transition in human hand movement. *Biological Cybernetics, 53*, pp. 247-257.

[5] Guadagnoli, M. A. & Lee, T. D. (2004). Challenge point: a framework for conceptualizing the effects of various practice conditions in motor learning. *Journal of Motor Behaviour, 36*(2), pp. 212-224.

11.4 Situating Interactive Systems within Cultural Spaces - A Practice-Based Recalibration of HCI-Theories and Methods

Michael Heidt (`michael.heidt@informatik.tu-chemnitz.de`)
Supervisor: Jun.-Prof. Dr. Paul Rosenthal

The expressiveness of any formal discipline hinges on its ability to relate its own concepts to the social domains it wants to operate in. Correspondingly, the expressiveness of any engineering activity hinges on its ability to situate produced artefacts within the designated target domain. Adequate methods are needed in order to process the concerns of said domains during processes of analysis and evaluation, to structure development efforts and guide negotiations. Adequate theories are needed in order to inform processes of communication, to reason about relevant objects and relationships. In the case of HCI, much of the discipline's theoretical and methodical inventory evolved within contexts such as work, formal education or, more recently, with a focus on developing consumer products. Contexts within the realm of culture, neither instrumentally goal-oriented nor focussed on entertainment, are not adequately addressed by contemporary theories and methods.

Exhibition contexts constitute a space of this kind. They lend themselves to be explored in a playful way, creating a unique ensemble of interactional-communicative situations, thereby facilitating specific forms of experience. Supporting these forms of experience calls for a reevaluation of paradigms such as Slow Technology [1], Embodied Interaction[2], Computers as Theatre[3], and Interface Ecology[4].

The outlined problematic is explored in the course of practice-based research studies conducted in cooperation with the School of Interactive Arts and Technology at Simon Fraser University. Digital prototypes developed arrange content accessible through the social web in the context of interactive installations realised via full-body tracking. The project's goal is a contribution to the recent 'turn to practice' within HCI[5], through specification of a generative theory-methods package aimed at development for cultural contexts.

---

[1]Hallnäs, L., & Redström, J. (2001). Slow Technology - Designing for Reflection. Personal Ubiquitous Comput., 5(3), 201–212.

[2]Dourish, P. (2004). Where the Action is: The Foundations of Embodied Interaction. The MIT Press.

[3]Laurel, B. (2013). Computers as Theatre. Addison-Wesley.

[4]Kerne, A. (2005) Doing Interface Ecology: The Practice of Metadisciplinary. ACM SIGGRAPH 2005 Electronic Art and Animation. 181–185

[5]Kuutti, K., & Bannon, L. J. (2014). The Turn to Practice in HCI: Towards a Research Agenda. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 3543–3552). New York, NY, USA: ACM.

11.5 Detection of emotions as coded by FACS in video streams by employing motion detection as found in the visual pathway of the mammalian brain

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

In everyday talks emotions are an essential part of the conversation. Even small changes of facial expression may indicate a shift in the communication. On the contrary human-machine-interfaces are not aware of the emotion expressed by facial actions. So it is crucial for a machine interface aware of emotions, to extract motion from relevant parts of the face. In this project a system will be implemented which extracts relevant emotions out of video data. The underlying method to extract motions which show the facial expressions are based on motion detection as found in the visual pathway of the mammalian brain.

There exists a physiologically grounded theory for emotions expressed in faces. This system called Facial Action Coding System (FACS) is driven by the movement of individual facial muscles. Each facial movement is coded by a specific Action Unit (AU) which roughly corresponds to the muscles producing the facial expression. Current research is mainly based on the idea to extract certain facial features algorithmically and decode them to Action Units. With this action units an estimate of the expressed emotion is possible.

Such algorithms are mainly tuned and trained on still images which show a face in nearly perfect frontal view. But video streams not only show global motion e.g. moving or turning the head but also minor movements as the twitching of an eye brow or curling the lips. Such muscular activities should be detected by a motion detection based on the motion as found in the brain of mammals and combined to a neural net which decodes them into Action units. This motion detection system is related to the retinal processing of light stimuli and a learnable neuronal net which uses space-time receptive fields.

This project aims on decoding the Action Units out of video streams which show facial expressions. In the motion is to be extracted out of video streams. Where current technologies focus on algorithmically induced search for features this project tries to use the adaption of a neuronal not to determine and extract the relevant features. This features will be used to generate Action Units and determine the emotion exposed in the video.

11.6 Processes of Heterogeneous Cooperation in the Design of Tabletops for Museums

Kalja Kanellopoulos (`kalja.kanellopoulos@phil.tu-chemnitz.de`)
Supervisor: Prof. Dr. Claudia Fraas (Chair of Media Communication)

This PhD project explores from a social scientific perspective how processes of heterogeneous cooperation[1] arise and unfold around multitouch tables designed for exhibitions. It focuses on cooperations between system designers as well as cooperations between system designers and users. Therefore it becomes possible to analyze intertwinements between system development and system use. With this orientation the research places itself in the tradition of Labour Studies[2] and Workplace Studies[3].

Large interactive displays like tabletops hold great potential for simultaneous engagement and cooperation of several persons, which makes them attractive for the use in work contexts as well as semi-public places like museums. Studies on the nature of social interaction and cooperation around tabletops are typically conducted as user studies in the course of the design process.[4] They focus on what is going on between users, often blackboxing the design work that underlies the construction of a certain prototype. This project brings together system development and system use by means of ethnography, basing on a large corpus of empirical research carried out on a long-term basis.

In an ethnographic case study the development of two tabletops for different exhibitions is accompanied throughout the process. Apart from conducting evaluations of prototypes in the museum setting the ethnographer takes actively part in the design work and decisions. The data corpus implies field diaries, written protocols of participant observations, photographs, videotaped prototyping sessions and debriefing meetings as well as videotaped user studies in the museum. Data acquisition and analysis follow the principles of Grounded Theory methodology. The project situates at the intersection of Science and Technology Studies (STS), Human Computer Interaction (HCI) and Computer Supported Cooperative Work (CSCW).

---

[1] Heterogeneous cooperations are forms of cooperation that involve participants from different local and disciplinary contexts, who act across different places or subject areas. Strübing, J. (2012). Pragmatistische Wissenschafts- und Technikforschung. Frankfurt a.M.: Campus.

[2] e.g. Latour, B.; Woolgar, S. (1986 [1979]): Laboratory Life. Princeton University Press.

[3] e.g. Suchman, L. (1993): Technologies of Accountability: On Lizards and Aeroplanes. In Graham Button (Ed.): Technology in Working Order. London: Routledge, 113-126.

[4] e.g. Clarke, L.; Hornecker, E. (2013): Experience, Engagment and Social Interaction at a Steam Locomotive Multimodal Interactive Museum Exhibit. CHI'13

11.7 Cooperative multi-user interaction in virtual worlds

Vincent Küszter (`vincent.kueszter@informatik.tu-chemnitz.de`)
Supervisor: Prof. Dr. Guido Brunnett

I am working on the development of a prototyping platform for exploring interaction between multiple users in a virtual reality environment. Although there is extensive research regarding the matter of interaction in "conventional" virtual worlds [1], the addition of a stereoscopic view for all users and the resulting consequences for interaction have been a focus of a lot less examination [2]. New interaction types like swapping views or the ability to display different information to each user, while they still occupy the same space in the real world form interesting research topics. To enable user studies on those topics, an easy to use prototyping platform is needed.

To realize a multi-user VR, each user needs to have an own perspective-correct view on the VE. This is done by utilizing the same image separation techniques that are used to produce stereoscopic images, in our case we combined shutter glasses and Infitec-filters. Our system projects the images at a power wall, a table add-on for better face-to-face interaction is currently planned. This prototyping platform supports an array of different input methods to realize the collaborative interaction with the virtual world, so that complements real-world user interactions like talking and communicative gestures. Apart from the standard keyboard/mouse input, the system can be operated with a multitude of input devices, for example the Razer Hydra, a magnetically tracked device with two controllers and 6 DOF , the Novint Falcon, a 3 DOF haptic input device, and the Leap Motion finger-tracker.

Two test scenarios are currently implemented. The first one is a block puzzle game, in which the users have to recreate a color pattern on the floor with simple blocks. A second test requires one user to hold a nameplate to a door. The other user is tasked to screw the plate in from the back (so the screw heads are not visible). Since the door is in the way, both have to communicate and switch views to avoid drilling in the holding user's hand. The scene composition and system details are easily modifiable by changing a set of XML-Files that describe game entities.

---

[1] Bowers, J. , O'Brien, J. & Pycock, J. (1996). Practically Accomplishing Immersion. In Proceedings of the 1996 ACM Conference on Computer Supported Cooperative Work - CSCW '96, 380–389. New York, New York, USA: ACM Press.

[2] Agrawala, M., Beers, A. , McDowall, I. , Fröhlich, B. , Bolas, M. & Hanrahan, P. (1997). The Two-User Responsive Workbench. In Proceedings of the 24th Annual Conference on Computer Graphics and Interactive Techniques - SIGGRAPH '97, 327–332. New York, New York, USA: ACM Press.

11.8 Cognitive and Emotional Processing of Virtual Environments

Benny Liebold (`benny.liebold@phil.tu-chemnitz.de`)
Supervisor: Prof. Dr. Peter Ohler

Research summary. With more and more consumer-grade VR technology becoming available, immersive virtual environments are at the verge of a qualitatively new level of media experiences in our lives. Given that they are a rather young phenomenon, they put forth a large body of research with contributions from various disciplines. As part of these efforts, research on the user perspective set out to investigate human cognition during HCI to explain user behavior in virtual environments and derive implications and evaluation criteria for HCI design. The concept of presence (i.e. the feeling of being there) and related concepts (e.g. self-presence, social presence) were presented to explain the cognitive processes involved in the interaction with these technologies and received a lot of research attention. However, presence theory faces several issues regarding the proposed mechanism of becoming present and the methodology of assessing the user's degree of presence.

To address these issues the thesis presents a revised theory of presence that is based on fundamental psychological processes: Presence is closely tied to attention allocation processes that interact with fundamental cognitive capacities, such as spatial or social cognition. As a consequence, cognitive processing of virtual environments does not require the user to suppress the mediated nature of their experiences. Rather, virtual environments address the same cognitive capacities as real stimuli do due to their resemblance. The theory predicts that breaks in these experiences (so called breaks in presence) draw attention to the virtual environment as an artifact, thereby triggering analytical processing. To investigate, whether these breaks in presence correspond to distinct psycho-physiological reactions that could be used to identify these breaks, we introduced breaks in presence into a virtual environment and measured various body reactions and user behaviors.

Because we argue that the involved cognitive processes are identical, behavioral patterns acquired in virtual environments should facilitate real world outcomes. To test this prediction, we investigated virtual motor skill learning, which can be considered the most demanding form of skill acquisition in virtual environments, and trained users in driving virtual racing cars. Later, users were asked to drive a go-kart for 10 minutes on a real racing track. We found that virtual training increased real world performance lending support to the assumption of identical cognitive processes.

11.9 Sensor-Assisted Mobile Learning

Kai-Uwe Martin (`kai-uwe.martin@informatik.tu-chemnitz.de`)
Supervisor: Prof. Dr. Wolfram Hardt

Over the last years "smart" mobile devices reached a significant market share. These devices use special interaction mechanisms like touchscreens and accelerometers which offer a broader and more natural human to computer interaction than previous desktop computers[1]. With increasing success they are used as e-learning devices, which is the focus of this research in the research field mobile learning.

However almost all e-learning contents and interaction mechanisms are aimed at desktop devices. For this reason an adaptation to the special characteristics of mobile devices is required to better support mobile learning processes. Especially for interaction purposes mobile devices offer more possibilities and channels than most desktop e-learning environments[2]. Several sensors, primarily used in the mobile interaction and communication processes, have a high potential for mobile learning[3]. In addition, the interaction with the environment, personalization and continuous reachability in social networks can be used to promote learning purposes.

This work describes, realizes and evaluates a systematic approach to collect sensor data from mobile devices, apply rules on it to identify certain learning situations and evoke assistance actions and recommend suitable learning content based on the recognized situation[4]. It serves as a framework to enhance mobile learning applications by sensor-based assistance.

A combination of collected sensor data can be seen as typical for a special situation the user is experiencing. By defining a range of conditions to match certain situations it is possible to categorize, save and later to recognize them. Some of these situations are more suitable for mobile learning purposes and some need an adaption of the content or the device parameters to maximize the learning support. Based on a recognized learning situation a content proposal mechanism, interaction mechanisms or device parameter adjustments to support the learning process are activated.

---

[1] Roschelle, J. (2003). Keynote paper: Unlocking the learning value of wireless mobile devices. Journal of Computer Assisted Learning 19.3. 260-272

[2] Sharples, M., Taylor, J., Vavoula, G. (2005). Towards a theory of mobile learning. Proceedings of mLearn 2005 1.1. 1-9.

[3] Martin, K.-U., Wuttke, M., Hardt W. (2014) Sensor based interaction mechanisms in mobile learning, In: Learning and Collaboration Technologies., 16th International Conference HCI International 2014, pp. 165-172

[4] Martin, K.-U., Hardt, W. (2013). Delivering complex learning content on mobile devices. In: AACE (Ed.) E-Learn 2013, World Conference on E-Learning, (Vol. 2013, No. 1, pp. 161-166)

11.10 Spatial Mapping in virtual environments: The effects of stereoscopy and natural mapping on user experience

Daniel Pietschmann (`daniel.pietschmann@phil.tu-chemnitz.de`)
Supervisor: Prof. Dr. Peter Ohler

Research summary. The thesis focuses on spatial cognition in virtual environments. The effects of natural input and output information are analyzed in form of natural mapping and stereoscopic presentation. In particular, the thesis discusses the combination of input and output modalities as a function of the interactions performed by the users. Mental models are used to conceptualize the transfer of knowledge and skills from real to virtual interaction. The new concept of spatial mapping is introduced as a spatial congruency of both perceived real world space (e.g. user position within VR setup) and virtual space (e.g. user position within virtual landscape). Spatial mapping is used as a holistic extension of the natural mapping concept, with the additional focus on spatial relations. The term defines the degree of mapping of physical and virtual environments. Ideally, an isomorphic mapping of both perceived interaction spaces occurs, minimizing required cognitive transformation processes for the user. As a result, more cognitive resources are available to actually process the content of the environment. Often, stereoscopy is used for existing media content without adjusting the content accordingly (e.g. commercial video games, film industry). Creating a higher quality of spatial information should only be beneficial, if it is relevant for the user's interaction.

Based on the spatial mapping approach, a theoretical path model was constructed and tested empirically. Two experiments were conducted to study effects of natural mapping and stereoscopic presentation in scenarios using high degrees of spatial mapping. In the first experiment, a commercially available video game was used as stimulus. High degrees of spatial mapping were present, but not essential for the interaction within the environment. In contrast, the second experiment used a VR simulator were the interaction benefitted significantly from high degrees of spatial mapping. As expected, the experiments showed no effect of stereoscopy on user experience and performance when the available spatial mapping is not relevant to the user's interaction.

The thesis discusses the application of stereoscopy and natural mapping as a function of the interaction type and offers an explanatory approach considering both input and output modalities.

11.11 Speech based Interfaces for robot communication

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

Nowadays boundaries between the real social world and the virtual world become ever less distinct. One well known example are service robots, like pool cleaner and vacuum cleaner. However, a rising field of research are robots, which are used as museums guides. There are already a lot examples regarding this topic, like RHINO[1], Minerva[2], Robotinho[3] and I²MSAS[4], just to name a few. The economic interests are also increasing drastically. The IFR, for example predicts a double-digit percentage growth in the upcoming years.[5] All the mentioned robots are optimized to guide visitors through the museum, but do not interact with the visitors to maximize the learning effect during the guide.

The research idea is to optimize the learning effect by using an interactive conversation between the robot and the visitors. For this purpose a full speech analysis is necessary. In order to generate an interactive conversation, an absolute necessity is to communicate face to face, this means it is necessary to localize the speaker as a part of speech analysis. The next step is to understand questions and to answer them. To realize this, a speech recognition has to be performed and different speaker have to be separated. Based on this analysis different approaches to understand the context of the question have to be evaluated. Another part to optimize the learning effect, is to include information of the emotional state about the visitors, like interest or boredom for the shown exhibits. To gather information about the emotional state, it has to be evaluated if this information can be extracted by the voice, or whether other sensors have to be added.

In order to verify these theses, an interdisciplinary collaboration is inevitable. Another question to be answered during the research, is the question of the correct voice, such as the gender of the voice and the speaking rate.

[1] Burgard, W.et al., "The Interactive Museum Tour-Guide Robot",in Proc. of the Fifteenth National Conference on Artificial Intelligence (AAAI-98), Madison, Wisconsin, 1998.

[2] Thrun, S.et al.„Probabilistic Algorithms and the Interactive Museum Tour-Guide Robot Minerva", in International Journal of Robotics Research, Vol. 19, No. 11, 2000, pp.972-999.

[3] Faber, F.et al., "The Humanoid Museum Tour Guide Robotinho", The 18th IEEE International Symposium on Robot and Human Interactive Communication, Toyama, Japan, 2009.

[4] Hellbach S., et. al. "Learning as an essential ingredient for a tour guide robot",in Machine Learning Reports 02/2013, Workshop New Challenges in Neural Computation 2013.

[5] Schraft, R. D.; Hägele, M.; Wegener, K. „Service Roboter Vision" München, Carl Hanser Verlag, 2004.

11.12 Creating Multi Touch Tabletops for In-The-Wild Settings

Michael Storz (`michael.storz@informatik.tu-chemnitz.de`)
Supervisor: Prof. Dr. Maximilian Eibl

A milestone in the history of multi-touch was when in 2005 Jeff Han presented a low-cost solution for multi-touch tabletops.[1] He stated that the technology itself not the new and important thing but the things that can be done with it. One of those things that comes inherently with multi-touch is the possiblity of multi-user interaction on these tabletops.

These devices hold a great potential since groups of users are no longer forced to partial passivity or turn taking. Instead they can interact collectively with a digital interface at the same time and in natural communication with each other. My project evolves around such a multi-touch tabletop which is intended to enrich a museum exhibition with interactive applications.

The multi-user property of tabletops also leads to challenges in interaction design. For one, the orientation of content and the sharing of interface space needs to be appropriate for the available users. Furthermore such devices are still rarely seen in public spaces so that multi-user capabilities have to be mediated and in order to overcome reluctancies, users need to be encouraged to use it and to share it with others.[2]

To tackle these challenges this project focused on creating tabletop and application prototypes in an interative process incorporating in-the-wild studies to measure the acceptance of the artifacts in realistic settings. During the course of the project two tabletop prototypes were developed that allow different arrangements of seating elements that give up to six users and several onlookers a good view and a comfortable access point to the interface.[3] Furthermore three studies, two in a museum and one in an exhibition were conducted. Preliminary results show that the tables were very well received, indicated e.g. by long staying times, sometimes exceeding an hour.

---

[1] Han, J. Y. (2005). Low-cost multi-touch sensing through frustrated total internal reflection. In UIST '05

[2] Hornecker, E. (2008). "I don't understand it either, but it is cool" – Visitor Interactions with a Multi-Touch Table in a Museum. In Tabletop '08

[3] Storz, M., Kanellopoulos, K., Fraas, C. & Eibl, M. (2014). ComforTable - A Tabletop for Relaxed and Playful Interactions in Museums. In ITS '14

11.13 Sensor-based Perception of non-verbal Communication

Anke Tallig (`anke.tallig@informatik.tu-chemnitz.de`)
Supervisor: Prof. Dr. Wolfram Hardt, Prof. Dr. Maximilian Eibl

Robots in environments which are dominated by human beings need more comprehensive social awareness. At present robots perceive gestures as a special kind of communication and facial expression as emotion. This happens at a closer distance to the robot or systems in general. Perception in such a close environment is important to individualizing a human-robots communication. But, when a human being or a user is in this environment the first perceptions of this social situation are already gone.

For the first impression there is no second chance.

The aim of my project is the perception of social situations at a distance. With the help of this special information the robot appears on the scene as the mediator. The mediator is designed for museum environments, especially in the reception area. In this area the wellbeing of the visitors will be decided. After entrance they will orient themselves and in this period of time social signals can be perceived.

With a verbal reaction which is emitted by the mediator, depending on the interpreted social situation, the mediator will be a helpful device for visitors and the museum, also. This early information can also be suitable for individual personal communication. Near and far contact of the visitors will be a helpful component of comprehensive social awareness.

11.14 Modeling Vision

Michael Teichmann (`michael.teichmann@informatik.tu-chemnitz.de`)
Supervisor: Prof. Dr. Fred H. Hamker

Research summery. Understanding the human visual system and the underlying learning mechanisms is a vital need for computational models of perception. Requirements for our intended model are at first the ability to recognize different object categories. Secondly, the integration of feedback signals to guide the processing. Finally, the biological plausibility of the processing.

Our first research question was how the visual system achieves its ability to recognize objects invariant to various transformations. To study potential mechanisms for learning this invariant processing, we created a model of the primary visual cortex (V1), simulating the so-called simple-layer (V1-layer 4), and complex-layer (V1-layer 2/3). We found that trace learning is a suitable mechanism for learning the responses of V1 complex-cells[1]. Subsequently, we show that a single learning rule can account for the development of simple- as well as complex-cell properties. We apply this learning rule to exploit the temporal continuity of the visual input, using a short-term trace for neurons in the simple-layer and a longer-term trace in the complex-layer.

To build more plausible and more advanced networks, we modeled a circuit of excitatory and inhibitory units, having cortical like connectivity. Further, to address the problem of stable unsupervised and biologically plausible learning in deeper networks, we employed intrinsic plasticity. This mechanism regulates the local activity range of a neuron by controlling the amount each neuron participates in encoding patterns. With these mechanisms at hand, we developed a multilayer model of V1 and V2 and show that the recognition accuracy increase with each layer while the model neurons still have biologically plausible properties[2]. To increase the flexibility and reduce the modelers bias, we introduced spatial and activity dependent structural plasticity[3]. Enabling the neurons to change their connectivity structure to be optimally adopted to the input. This reduces the need for a priori knowledge of the exact connection structures of the network. Beside biological plausibility, we evaluated the object recognition performance and robustness to occluded stimuli. We found that networks employing more advanced competitive mechanisms, when calculating their output activities, show more robust recognition accuracies[4].

---

[1] Teichmann, Wiltschut, Hamker (2012). Neural Comput., 24(5), 1271–96.
[2] Teichmann, Hamker (2015) MODVIS, St. Pete Beach, Florida, USA
[3] Teichmann, Shinn, Hamker (2013) Bernstein Conf., Tübingen, Germany
[4] Kermani Kolankeh, Teichmann, Hamker (2015) Front. Comput. Neurosci., 9:35

11.15 Proactive elements and environmental perception of Pedagogical Agents

Madlen Wuttke (`madlen.wuttke@phil.tu-chemnitz.de`)
Supervisor: Prof. Dr. Peter Ohler

Human-machine-interactions are heavily dependent on established technological modalities. The mouse and keyboard interface devices make up for the two mainly used input devices although they require a motoric learning process for a correct and timely usage. This is especially interesting when compared to evolutionary natural forms of communicative behavior in humans. Most aspects of face-to-face communication is transported verbally, but this form of communication is supported by a variety of additional information which is transported while speaking. Intonation delivers information about the emotional status and gives additional meaning to the voiced words while the visual channel delivers contextual information and allows the recipient to take gestures and the focus of attention of the counterpart into account, when decoding the received verbalized information. Therefore, the media-equation theory from Reeves and Nass [1] postulates an urge for social behavior of humans every time they try to communicate – even in cases of inanimate objects like a computer.

Consequently, within the context of the Crossworld project, an already established web-based-training tool about Adobe Dreamweaver of the institute of media research was improved by an enhanced pedagogical instance (EPI). The EPI enabled the system to check for environmental information via a microphone (to check for noise levels) and a HD webcam (to check for the gaze of the user). During an experimental validation, the subjects had to work through the web-based-training, use the demonstrated skills within the Dreamweaver Software and retention was tested via a multiple choice questionnaire.

Upcoming variations of the web based training will focus on the implementation of further proactive capabilities of the EPI by adding additional physiological sensors to the array of environmental information acquisition (e.g. eye-tracking, pupil dilation and cognitive load [2]).

---

[1] Reeves, B. & Nass, C., 1996. The Media Equation. How people treat computers, televisions, and new media like real people and places. New York: Cambridge University Press.

[2] Silva, L. M. (2009). The construct of cognitive processing and speed : test performance and information processing approaches. University of New Mexico.

12 GRK 1817: UbiCrypt - New Challenges for Cryptography in Ubiquitous Computing

Prof. Dr. Alexander May
Email: grako@hgi.rub.de
Ruhr University Bochum
Internet: http://www.ubicrypt.hgi.rub.de/

IT security has been studied in the open scientific community since the early 1980s. During the 1990s, research efforts have intensified and commercial products with security technologies have become increasingly important, e.g., authentication and voice encryption on mobile phones or SSL encryption of credit card transactions in web stores. The first decade of the 21st century has seen the success of smart phones, Web 2.0 and web services, all equipped with their own security features. The current solutions for securing the next generation of IT systems are not always sufficient.

The general theme of the Research Training Group (RTG) is the development of solutions for new security challenges in ubiquitous computing environments. The focus is on cryptographic components and protocols as well as support mechanisms which can be used universally, and which are often independent of the underlying platforms. In order to approach this complex topic in a systematic way, the research topics are structured in a three three-level model: the Crypto primitives level, the device level and the System level.

The Crypto Primitives Level deals with physically or mathematically based cryptographic functions, which form atomic building blocks for realizing security systems. At the Device Level, the goal is to study how to protect individual devices against attacks. Finally, at the System Level the goal is to study how these devices interact by means of cryptographic protocols and distributed applications.

More in detail, at the Crypto Primitives Level the RTG will deal with topics like lightweight ciphers, fully homomorphic encryption or cryptography resistant against physical attacks. At the Device level, topics include how to realize trustworthy platforms or cyber-physical systems. Finally, at the System level, the RTG studies how to achieve security across platforms or security models for inhomogeneous systems.

12.1 Privacy-preserving Learning

Francesco Aldà (`francesco.alda@rub.de`)
Supervisor: Prof. Dr. Hans U. Simon

The goal of *private data analysis* (also known as *statistical disclosure control*) is to enable rich and useful statistics on a database to be performed while simultaneously protecting the privacy of the individual records. The trade-off between privacy and usability has attracted much attention in many different fields, from statistics and theoretical computer science to security.

In their seminal work (2006), Dwork et al. introduced the notion of ε-*differential privacy*, which has become one of the most important paradigms for privacy-preserving statistical analyses. Among its several properties, this definition guarantees, in particular, that the presence or the absence of a record in a database does not affect the final output of the statistics significantly. Moreover, this notion has been shown to represent a resourceful tool in many other fields where privacy may be a concern, e.g. in *statistical learning* (Kasiviswanathan et al., 2008).

In this project, we investigate how well the objectives of statistical learning can be pursued subject to the constraint of achieving ε-differential privacy. Moreover, we aim at analysing the issues related to statistical disclosure control (under differential privacy) in terms of learning problems. The perspectives of these two areas are, indeed, closely related and, in some sense, dual to each other. In learning theory, one has a sample (a kind of database) and would like to infer information about an unknown target concept. In private data analysis, instead, one has only indirect access to a database via queries and wants to learn something about the unknown data in the database. Typically, one is not interested in the precise or approximate reconstruction of the database but wants to get some aggregated information only. One of the major goals of our research consists of establishing connections between these two fields, exploring the relevance of models and notions of learning theory in the field of private data analysis.

12.2 Tightness in Cryptography

Christoph Bader (`christoph.bader@rub.de`)
Supervisor: Prof. Dr. Jörg Schwenk

When a new cryptographic scheme is proposed, nowadays the construction comes along with a proof of security. Most commonly, the proof is relative to a complexity assumption which states that it is computationally hard to solve certain computational problem. That is, the proof describes an efficient algorithm, the *reduction*, that turns any successful attacker against the scheme (with respect to the considered security notion) into another efficient algorithm, the *inverter*, that breaks the computaional problem. Now, if no algorithm is known that efficiently solves the problem it is conjectured that an efficient attacker against the scheme cannot exist, since otherwise the inverter, given access to the attacker, solves the problem efficiently (i.e., *breaks* the complexity assumption). In other words, the reduction reduces breaking the complexity assumption to breaking the cryptographic scheme.

One can measure the quality of the reduction by considering its *loss* which is the ratio of the *work factor* (the expected running time) of the inverter and the work factor of the adversay against the scheme. Ideally, the inverter's work factor roughly equals the work factor of the adversary. In this case, the reduction is said to be *tight*. In general, a reduction's loss influences the size of the parameters that are used when a scheme is deployed in practice if these are selected to be theoretically sound: the smaller the loss, the smaller can the parameters be. Therefore a tight reduction is a desirable goal with practical applications. On the other hand, from a theoretical point of view, tight reductions are probably even more interesting, since they require rigorous design approaches and proof techniques that are fruitful for the community. Our research considers possibility and impossibility of tight reductions.

12.3 Ubiquitous Authentication

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

Recent improvements in the manufacturing of sensors, e.g., reduction of costs per unit or energy harvesting, enable so called *smart environments*. These include wearable devices like glasses or watches, which can measure the heart rate or monitor the movement, proximity, and even the sleep cycle of a person. Automated buildings, so called smart homes, try to reduce a household's energy consumption by sensing for sun light and switching off the heating and light bulbs if they are not necessary.

Today, it is require to authenticate, e.g., via a password, before one can use a service. As a lot of services move online, the number of required passwords are no longer manageable by a person. Thus, the already not very securely chosen passwords get reused on a daily basis. Stolen login credentials are leaked in huge quantities every year leading to serious problems for the affected users and websites.

New authentication systems are reinforced by accounting additional information during the login to derive a decision. Due to their constant sensing, smart homes allow us to build profiles that can be used for authentication and relive the user from the burden of actively remembering secrets. By combining different sensor data one can identify a person. Wearable devices deliver even more personal measurements and help to build a complete picture of the user's day. By profiling a user with its sensor data, we try to find new effortless authentication methods that can be used in a privacy preserving manner.

12.4 Selective Opening Secure Public Key Encryption

Felix Heuer (`felix.heuer@rub.de`)
Supervisor: Prof. Dr. 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.

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.

12.5 Reduction based Analysis of Real World Cryptographic Protocols

Matthias Horst (`matthias.horst@rub.de`)
Supervisor: Prof. Dr. Jörg Schwenk

Today a lot of information exchange in the internet is secured by cryptograhic systems. These systems use security protocols to define the exchange of messages between all participating parties. Because there is not only one protocol that is used everywhere, but there a lot of them, the question is which of these protocols are secure to use, and which are not. One possibility to show the security is to provide a mathematical proof that shows whether this protocol has security flaws that allow an attacker to break the protocol, or whether the protocol is secure. It is notable that a protocol can be insecure, even if all the used underlying crpytographic primitives are secure.

The problem with security proofs for protocols is, that it is mostly not possible to provide a proof for perfect security. This means even if we have this security proof, there might still be a way to break the protocol. But it is possible to provide reduction based proofs. These proofs show, that if an attacker is able to break the protocol, he is directly able to solve an assumption that should not be able to break. These assumptions are usually some mathematical problems that have been intensely studied for a long time, without anyone finding a solution. This means that with good assumptions, we still get a security proof, that we can rely on.

While it might be a good idea to design protocols with security in mind and only use in practice protocols that have a valid security proof, the reality shows us, that there a lot of protocols used in daily life that do not have a valid security proof. This can happen for various reasons. Sometimes the protocols first version were designed before the necessary means to build a security proof were even fully developed. And now the never version are just modifying the first version. This leads to the fact, that there are a lot of security protocols used in the real world that are in need of a security proof that is still missing. The research tries to add security proofs to protocols used in real daily life that are still missing them.

12.6 GPS Security

Kai Jansen (`kai.jansen-u16@rub.de`)
Supervisor: 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. In order to detach from the dependency on the US controlled GPS, additional Global Navigation Satellite Systems (GNSSs) are in development or already available, e.g., GLONASS (Russia), Bei-Dou (China), GALILEO (Europe).

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. In recent years, powerful spoofing attacks have been demonstrated by Humphreys et al. — Drone Hack (landing of an aerial drone) [2012] and Yacht Theft (changing the course on the high seas) [2013].

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.

12.7 Lattice-based cryptography

Elena Kirshanova (`elena.kirshanova@rub.de`)
Supervisor: 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 the problem 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.

12.8 Steganography and steganalysis for multimedia-based communication channels

Katharina Kohls (`katharina.kohls@rub.de`)
Supervisor: Prof. Dr. Christina Pöpper

Internet censorship limits publicly available information services as well as applies surveillance to private communication channels. This is enforced by techniques such as static blacklisting of text messages, blocking of URLs and IP addresses, or monitoring of phone and Voice-over-IP (VoIP) calls. Starting from this motivation *steganography* tends to provide privacy-preserving countermeasures by hiding information in communication channels. So called censorship circumvention systems provide a communication channel that enables for transmitting information that should remain unnoticed by the censor. Similar techniques can also be applied in different contexts, e.g., in digital rights management or tamper proofing of digital media.

The overall goal of steganography is to hide secret information within a carrier while preventing these changes from being detected. Therefore research in the field steganography focuses on the development and deployment of new techniques that provide secure hiding mechanisms for valuable information under different scenarios of attack.

In our project we began by focusing on steganography and steganalysis in the context of multimedia-based communication channels, in particular publicly available VoIP services such as provided by Skype. By applying the context of Internet censorship, this challenges the implementation of a preferably unobtrusive circumvention system that provides an acceptable bandwidth and realistic deployment scenario at the same time. Such characteristics can be achieved by directly adapting the conversation's voice signals through amplitude modulation.

With further research in the field of steganography we will focus on alternative carrier systems and contexts of deployment, e.g., tamper proofing, integrity checking, or watermarking of binary files.

12.9 Design and Analysis of Symmetric Primitives in Cryptology

Thorsten Kranz (`thorsten.kranz@rub.de`)
Supervisor: Dr. Gregor Leander

Symmetric cryptography is used in various scenarios in our everyday life. Famous examples 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 (SPNs). In this context, we analyze the characteristics of linear transformations and Substitution Boxes (S-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.

For example, when designing a block cipher, certain assumptions are made to precisely assess the security level with respect to linear cryptanalysis. However, often those assumption are wrong, for example, the assumption of independent round keys. This lack of knowledge concerning the security assessment leads to the integration of so-called security margins, that is, some extra rounds in the block cipher to make sure that we are "'on the safe side"'. A fundamental understanding might therefore improve the performance of symmetric primitives when we note that the security margin is too big or fully redundant. Furthermore, such an understanding clearly helps us assessing the security of symmetric primitives more confidently.

Another example of our current research is the decomposition of a SPN that is only given as a blackbox. 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.

12.10 Cryptography from Hard Learning Problems

Daniel Masny (`daniel.masny@rub.de`)
Supervisor: Prof. Dr. Eike Kiltz

In cryptography, primitives are desired to be as hard to break as solving hard learning problems. One famous example of a hard learning problem is the learning parity with noise (LPN) problem which is closely related to the problem of decoding random linear codes which is also known as the syndrome decoding problem. Solving syndrome decoding would have a significant impact on coding theory, but it remained unsolved since 1949 when Shannon implicitly showed its importance in his breakthrough work *A mathematical theory of communication*.

For most cryptographic primitives like pseudorandom functions, public key encryption (PKE) or digital signatures, hard problems are necessary to guarantee their security. While the hardness of a problem is required for the security of a scheme, it is not clear if the desired functionality of a cryptographic primitive could be obtained simultaneously. In particular it is an open question if more advanced cryptographic primitives could be designed which are as hard to break as solving LPN. Further constructions based on LPN are often not as efficient as schemes based on alternative assumptions. Since discrete logarithm and factoring could be solved using quantum computers, a wide range of cryptographic schemes do not provide security in a post quantum world. On the contrary, LPN is a reasonable candidate for post quantum security, because no quantum algorithm is known to solve LPN. Although the efficiency of LPN based schemes must be improved to give them practical relevance.

During the project, we investigated LPN based symmetric authentication and PKE. We managed to design a symmetric authentication scheme which is secure against Man in the Middle adversaries. Additionally we improved the efficiency of low noise LPN based chosen ciphertext secure PKE. Further, during an interdisciplinary project we investigated the potential of LPN in a setting where devices leak additional information. This is a serious problem in particular for rfid chips. We applied and optimized techniques from leakage resilient cryptography to LPN based authentication schemes. We implemented the resulting scheme on a avr micro-controller and evaluated its practicality.

12.11 Improved Algorithms for Hard Problems in Cryptography

Ilya Ozerov (`ilya.ozerov@rub.de`)
Supervisor: Prof. Dr. Alexander May

Almost all modern cryptographic schemes use variable parameters that control both the efficiency and security of the scheme. Choosing these parameters very low would result in a very efficient, but also insecure scheme. On the other hand, large parameters would imply a secure, but inefficient scheme. Therefore, finding a good trade-off between these two extremes is one of the crucial tasks in constructing practical systems.

Measuring the efficiency of a scheme is usually very easy, whereas measuring the security has always been a struggle. Hence, in the last years, researchers concentrated on a small number of hardness assumptions, which are problems that are assumed to be difficult to solve in practice. With the help of a reduction, they usually show that breaking their scheme would imply a solution to the corresponding hard problem, thus proving the security of the scheme. But it isn't enough to rely on the assumed hardness of a problem, the hardness has to be verified by presenting and analyzing the best algorithm for the problem.

In our work we present an algorithmic tool that is applicable to a large number of these hardness assumptions. In a big set of data, the algorithm finds data points that are unusually close in a certain metric. As an important application, we present the best known algorithm for decoding of random linear codes. This problem, also known as syndrome decoding, is a hardness assumption for the code-based McEliece cryptosystem and is closely related to the Learning Parity with Noise (LPN) problem.

12.12 Retrofitting security into complex software systems

Jannik Pewny (`jannik.pewny@rub.de`)
Supervisor: Prof. Dr. Thorsten Holz

Writing software is a complex and expensive task, even if you only take aspects of functionality, in contrast to security, into account. Thus, old software, so called *legacy software*, is unlikely to be replaced without very good reasons. Unlike such software, the field of software security has improved over the last decades, which means that legacy software by definiton cannot fulfill the state of the art with respect to security. However, even the fact that it will not be up to the task to defend against modern attacks, it is simply too expensive to be replaced. As a consequence, it becomes important to deal with the hardships of *retrofitting security* into systems, which may lack documentation or even source code. Retrofitting simply means to make security related changes to the system long after its rollout, which may include techniques which were developed decades after the system itself.

My thesis concerns with such hardships and provides related solutions from multiple angles. I started with work on *control-flow integrity*, which ensures that even modern attackers cannot make the program take unintended paths. The key idea at this point is to instrument the underlying program in such a way that any deviation from the normal control-flow is detected and forbidden. Many modern exploitation techniques, like return-oriented programming, are thwarted by this approach.

Next, I turned towards the root cause of many software vulnerabilities: Programmer's mistakes, often called bugs. Naturally, a vulnerability disappears, when the bug responsible for the vulnerability is fixed. To do that, however, it is necessary to *find bugs* in the first place. While abstract criteria specific to certain classes of bugs can be defined, these criteria may be hard to use in practice to actually find bugs. Thus, together with colleagues, I developed a technique based on a *fine-grained code similarity metric* to find pieces of code in a binary program, which are very similar to pieces of code with known bugs — and therefore, are likely to contain the same bug.

Later, we dropped the underlying technique of a tree-edit distance based symbolic metric in favor of a common intermediate represenation, which is fit for sampling. This allowed to abstract from many architecture specific syntactic details towards an actual semantic comparison. Ultimately, we were able to extend this project to work across different architectures. This is a rather important step, because software nowadays gets used on a multitude of different processors — both on modern smartphones or desktop systems, but also in heterogenous legacy systems.

12.13 Efficient Implementation of Lattice-Based Cryptography

Thomas Pöppelmann (`thomas.poeppelmann@rub.de`)
Supervisor: Prof. Dr.-Ing. Tim Güneysu

Digital signatures and public key encryption are used to protect almost any secure communication channel on the Internet or between embedded devices. Currently, protocol designers and engineers usually rely on schemes that are either based on the factoring assumption (RSA) or the hardness of the discrete logarithm problem (DSA/ECDSA). But in case of advances in classical cryptanalysis or progress on the development of quantum computers the hardness of these closely related problems might be seriously weakened. In order to prepare for such an event, research on alternatives is required that can provide long-term security. Additionally, even though RSA and ECC appear still secure given today's understanding of their mathematical structure and previously failed attempts to construct sufficiently powerful quantum computers, it makes sense to investigate new schemes early on. The reason is that it usually takes several decades before alternative schemes have been thoroughly tested, gained trust in the community, and have been standardized.

In his thesis I am working on the efficient implementation of such alternative schemes that can realize digital signatures and public key encryption. My research is focused on schemes which are based on the hardness of solving certain hard problems in a special class of lattices. And while an extensive theoretical background exists for lattice-based cryptography, not much is known about the efficiency of practical instantiations, especially on constrained and cost sensitive platforms. During the course of this thesis I have proposed techniques for high performance or resource efficient implementations of several schemes on embedded microcontrollers and reconfigurable hardware. My results show that lattice-based cryptography offers high performance and good efficiency on a wide range of devices. Key tools are the domain specific optimization of polynomial multiplication and discrete Gaussian sampling which are required building-blocks for almost all practical lattice-based schemes. Moreover, I also investigated options for hardware acceleration of homomorphic cryptography in a cloud environment. Homomorphic cryptography allows the computation on encrypted data and as a consequence, the entity performing the computation is not able to learn anything about the data it has been working with. However, in practice operations are very costly and acceleration using FPGAs is challenging due to large ciphertext and key sizes, as well as limited memory bandwidth of real world devices.

12.14 Leakage-Resilient Cryptographic Implementations

Tobias Schneider (`tobias.schneider-a7a@rub.de`)
Supervisor: Prof. Dr.-Ing Tim Güneysu

Recent years have seen a rise in the popularity of embedded devices. Their field of application reaches from everyday objects to medical science and is commonly denoted as the *Internet of Things*. As some of these devices are part of security-critical systems, cryptography is often applied to achieve confidentiality and authenticity. However, the deployed processing platforms are often heavily restricted which poses additional design challenges.

Physical security is one these major challenges that has to be taken into consideration in the design of such a secure system. Even though most modern cryptographic algorithms are believed to be secure from a theoretical point of view, their implementations can still be susceptible to physical attacks. One class of attacks uses so-called *side-channels*, e.g., the power consumption of the device, to extract information about the secret internal state of the computation. This information then can be used to break the security of the system, e.g., by recovering the secret key. Since traditional cryptography mostly assumes a black-box model, even implementations of proven secure algorithms are most likely vulnerable to some type of side-channel analysis (SCA) if no dedicated countermeasures are used.

The countermeasures are often dependent on the used technology and algorithm and, therefore, these factors have to be considered in the initial design. As different countermeasures possess different effectiveness and overheads, choosing the best solution for a given system is not a trivial task. An erroneous implementation of a countermeasure can lead to further vulnerabilities. Therefore, it is of uttermost importance to evaluate the performance and security of deployed side-channel countermeasures.

In my research, I work on improving techniques to detect and quantify side-channel leakage. With these methodologies it is possible to detect flaws in the implementation of countermeasures and to compare the efficiency of different schemes. Another part of my research covers the design of secure hardware circuits. In particular, my current focus lies on the implementation of ARX-based ciphers in hardware resilient to side-channel analysis.

12.15 Defensive and offensive aspects of applied software security

Felix Schuster (`felix.schuster@rub.de`)
Supervisor: Prof. Dr. Thorsten Holz

More than four decades after the assumed first documentation of a buffer overflow vulnerability, people are still struggling to develop and to deploy *secure software*. While old and well-studied problems like buffer overflows can still be found in abundance even in modern software, new types of software vulnerabilities regularly emerge alongside new technologies and new use cases: today's immensely popular web applications are plagued by the likes of the infamous *cross-site scripting* and *SQL injection* vulnerabilities; whereas the emerging kind of cloud applications faces completely new and highly challenging adversarial settings where the entire runtime environment may be attacker-controlled; all while the lower levels of the software stack—including for example operating systems or web browsers—largely remain susceptible to the traditional memory corruption vulnerabilities such as buffer overflows.

My thesis concerns with defensive and offensive aspects of software security. I researched and developed novel defensive mechanisms for different kinds of software in various deployment scenarios. Most notably here, together with researcher from Microsoft Research, we created the first practical end-to-end solution for the secure execution of distributed computations in the cloud [1]. Our system leverages COTS hardware security features and lightweight cryptographic protocols. It guarantees the integrity and secrecy of all the user's code and data under realistic assumptions and at modest costs.

Orthogonally, I also developed novel attacks against state of the art academic and commercial software defenses. I was able to show that different defensive systems that were widely believed to be "good enough" or even strong can in fact be bypassed in realistic scenarios. Such offensive results are important, because they reveal wrong assumptions and serve as a valuable guide for the design of future defenses.

---

[1] *VC3: Trustworthy Data Analytics in the Cloud* - `http://research.microsoft.com/apps/pubs/default.aspx?id=210786`

12.16 Security Aspects of FPGA-Designs and Embedded Software

Pawel Swierczynski (`pawel.swierczynski@rub.de`)
Supervisor: 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 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 and asymmetric cryptography can be undermined by an attacker who has to perform changes at a very low level. As a proof-of-concept, we have demonstrated 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. Besides to pinpointing to vulnerabilities, we address how to mitigate our presented attacks to raise the bar for an attacker.

12.17 Differential Privacy and Cryptography

Filipp Valovich (`filipp.valovich@rub.de`)
Supervisor: Prof. Dr. Hans U. Simon

In the framework of statistical data analysis we consider individual users storing their sensitive data records in statistical databases. Our concern is to find techniques protecting the privacy of these users against any kind of data analysts. At the same time we aim at allowing the data analyst to perform accurate analyses over the database. To handle these two conflicting goals simultaneously, the notion of *differential privacy* has become an important field of research in recent years. A mechanism is defined to preserve differential privacy when the presence or absence of a single user in the database inputted to the mechanism does not affect its output statistics by too much. In a *centralised setting*, such a mechanism is usually performed by a so-called *trusted curator* who collects the sensitive data of all users in the clear, perturbs it properly and makes the obtained noisy statistics available to the data analyst.

Differential privacy is a concept raised from the limitation of existing cryptographic methods to achieve the aforementioned goals. Accordingly, our research project aims at establishing connections between differential privacy and concepts from cryptography. In particular we are interested in *positive* results, i.e. our objective is to show how known (or own developed) cryptographic methods and ideas can provide positive impact to differential privacy. Concretely, we investigate solutions for the so-called *distributed setting*. In this setting we do not want to rely on a trusted curator. This, of course, complicates the goal of achieving privacy and accuracy at the same time. Therefore we study, how a proper perturbation process can be performed by the users on their own, such that the entire noise generated by this process is sufficient for preserving differential privacy. In order to enhance the accuracy of the obtained statistics, it is possible to introduce a cryptographic layer: using purpose-built cryptographically secure protocols between each single user on the one hand and the data analyst on the other hand, only the final statistics is revealed to the data analyst but not the individual user values. In this way, the perturbation process in the distributed setting can be split among all users, maintaining almost the same strong guarantees of differential privacy and accuracy as in the centralised setting.

In our research, we deal with the design and security analysis of proper protocols for this task and we investigate which kind of statistics can be accurately obtained using these protocols, while preserving differential privacy.

12.18 FPGA Security

Alexander Wild (`alexander.wild@rub.de`)
Supervisor: Prof. Dr. Tim Güneysu

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.

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.

13 GRK 1855: Discrete Optimization of Technical Systems under Uncertainty

Prof. Dr. Peter Buchholz
Email: peter.buchholz@cs.tu-dortmund.de
TU Dortmund
Internet: 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 in 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.

13.1 Primal Methods in Robust Discrete Optimization

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

In robust combinatorial optimization it is often assumed that the uncertainty only affects the objective function. This leads to the optimization problem

$$\min_{X \in \mathcal{X}} \max_{c \in \mathcal{U}} \ c(X),$$

where the certain set $\mathcal{X}$ contains all the feasible solutions and the uncertainty set $\mathcal{U}$ all the possible cost functions.

Our approach is to consider structural uncertainty. We mean thereby that the set of feasible solutions itself can change. This allows us to model the failure of resources. In combinatorial optimization, failure means that the corresponding subsets of nodes or edges are removed from the graph. Each set of possibly faulty resources defines a scenario of our robust optimization problem. The goal is to find a set of edges (or nodes) which contains a solution to the underlying problem no matter which scenario emerged. In general the robust solutions are not feasible to the underlying problem as they contain too many elements. Minimizing the total cost implies the inclusion of the cheapest additional elements needed in a robust solution. For details on this model we refer to
D. Adjiashvili, S. Stiller and R. Zenklusen. Bulk-Robust Combinatorial Optimization. Mathematical Programming A. Volume 149, Issue 1-2 , pp 361-390.

An illustrating example is the construction of an energy distribution network. In this case we are facing a robust version of the spanning tree problem. Our resources are the edges. In order to protect the distribution network against the failure of certain edges we have, in general, to include additional edges in the solution. Hence the solution is not a tree anymore because it contains cycles which are the price of robustness. But independent of the fact which resources fail, our network always contain a spanning tree and hence remains functional.

This question can be formulated as follows. Consider a graph $G = (V, E)$. The underlying optimization problem is denoted by $\mathcal{P}$. The set of resources A can be the node set V or the edge set E, depending on $\mathcal{P}$. The faulty resources are given by the scenario set $\Omega \subseteq 2^A$. The set of feasible solutions to the problem $\mathcal{P}$ on the graph G is denoted by $\mathcal{X}(G)$. The costs are represented by a function $c : 2^A \to \mathbb{R}$. Our robust optimization problem can be then stated as follows:

$$
\begin{aligned}
\min \quad & c(Y) \\
\text{s.t.} \quad & \forall F \in \Omega \ \exists X \subseteq Y \subseteq A : X \in \mathcal{X}(G - F).
\end{aligned}
\qquad (\mathcal{RP})
$$

As most problems in robust optimization the problem $\mathcal{RP}$ is likely to be $\mathcal{NP}$-hard in general even if $\mathcal{P}$ is polytime-solvable. The aim is to find tractable subclasses of $\mathcal{RP}$ and approximation algorithms for more general settings.

13.2 Stochastic Bilevel Programming

Matthias Claus (`matthias.claus@uni-due.de`)
Supervisor: 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.

13.3 Dynamic management of logistic facilities under uncertainty

Lars Eufinger (eufinger@itl.tu-dortmund.de)
Supervisor: 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.

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

Momchi Ivanov (`ivanov@statistik.tu-dortmund.de`)
Supervisor: Prof. Dr. Sonja Kuhnt

In many applications in industry it is turning into standard practice to study complex processes with the help of computer experiments. These computer simulations may have continuous inputs, or take mixed discrete/categorical-continuous variables as inputs.Simulations generally take a long time to run, making it impossible to directly optimize the computer code. Instead, the simulator is considered to be a black-box function and a cheaper analytical model is used to interpolate the simulation.

Model-based black-box optimization is a classical tool for computer experiments analysis. This work explores the capabilities of current black-box methods, many of which are based on the Kriging model, and also proposes new methods which improve the existing theory. This thesis considers two classes of experiments - simulations with continuous inputs and mixed-input simulations.

For continuous inputs, this work proposes a robust version of a powerful, Kriging-based procedure - the EGO algorithm. The novel method, called keiEGO, corrects some of the flaws of EGO, due to restrictive assumptions which EGO and the Kriging model make. KeiEGO uses an alternative metamodel to Kriging and implements a robust search criterion. It is shown that keiEGO works better than EGO in some cases, including a practical simulation study.

Furthermore in this work a parallelization procedure for continuous inputs is proposed - the ParOF algorithm, which uses powerful sensitivity analysis techniques. The ParOF method gathers information about the structure of the black-box function and is capable of using that information for parallel computations and dimensionality reduction. It is shown that this procedure works well on a real computer experiment example.

Although the mixed case is of interest for various applications, there are only a handful of model-based optimization procedures in existence, which are 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 classical 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 the Kriging model 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 furthermore shown, that the procedure is able to tackle mixed problems fairly well. In addition, with the help of the modified Kriging kernel, the adaptation of the already mentioned ParOF parallelization algorithm to mixed-input problems is made possible.

13.5 Min-max-min Robustness For Combinatorial Optimization Problems

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

Data uncertainty is inherent in many optimization problems. Measurement or rounding errors can lead to uncertainty in the parameters of an optimization model, but also external influences such as traffic or changing regulations may lead to unknown costs. In recent decades, both robust and stochastic optimization approaches have been developed to address such uncertainties.

In my thesis, I consider combinatorial optimization problems of the form

$$\min_{x \in X} \quad c^\top x, \tag{13.1}$$

where $X \subseteq \{0,1\}^n$ contains the incidence vectors of all feasible solutions of the given combinatorial problem. All probable scenarios, i.e., all cost vectors to be considered, are contained in an uncertainty set $U \subseteq \mathbb{R}^n$. In the literature, different classes of uncertainty sets are discussed, mainly discrete, ellipsoidal, polytopal or interval uncertainty.

The idea of robust optimization is to calculate a solution which is feasible in every possible scenario and optimal in the worst case. This leads to the so called *min-max robust* approach, addressing the problem

$$\min_{x \in X} \max_{c \in U} \quad c^\top x. \tag{13.2}$$

The resulting class of problems has been studied intensively in the literature. Apart from creating hard problems in general, the main drawback of the min-max robust approach is the so-called *price of robustness*: the robust optimal value can differ substantially from the actual optimal value for a specific scenario. In my thesis, I propose and analyse a novel approach to alleviate this drawback. The objective is to calculate k different solutions which minimize the objective value in the worst-case scenario if we consider the best solution of all k solutions in every scenario. Formally, this leads to the problem

$$\min_{x^{(1)},\ldots,x^{(k)} \in X} \max_{c \in U} \min_{i=1,\ldots,k} c^\top x^{(i)} \tag{13.3}$$

where $U \subseteq \mathbb{R}^n$ and $X \subseteq \{0,1\}^n$ as before and $k \in \mathbb{N}$. The idea behind this approach is to calculate a set of solutions once in a (potentially expensive) preprocessing phase and from then on choose the best of the calculated solutions each time a scenario occurs.

In my thesis I analyze the latter approach for different combinatorial problems and uncertainty classes. I will present theoretical algorithms to solve problem (13.3) and I will prove complexity results for these algorithms. Additionally I will present computational results to compare Problem (13.3) to Problem (13.2).

13.6 Linear Programming Formulations for Stochastic Routing Problems

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

In a first phase, we considered 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) 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 equivalent to solving CSP instances.

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

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

My research focuses on interface and interaction design in the context of uncertain information and is part of the psychological research field of the graduate school. In the current studies I'm trying to uncover the representations users are developing about technical systems they are using to process their tasks. In a broader sense this representations are also called mental models and can be defined as long-term knowledge structures, which represents a user's understanding of situation-specific system functioning. In addition to subjective approaches, we assess eye movement behavior during the interaction with computer interfaces as an objective measurement. In order to investigate the development of mental models we established a spatial search task. In this task participants have to predict the spatial appearance of stimuli while they learn an underlying probability concept. In general, we expect that the more precise the participants' mental model of the task, the better the performance. Results of the spatial search task experiment show that eye movement patterns change over time with increasing expertise: fixation durations increase, whereas the amount of fixations as well as the amount of gaze shifts decrease. Thus, eye movement patterns may inform about the learning progress of spatial concepts under uncertainty. Furthermore, eye movement patterns might be an appropriate measure of the amount of task uncertainty. At the beginning of the experiment, task uncertainty is high and participants show extensive visual search behavior, whereas at the end of the task visual search behavior is more focused presumably due to the reduced task uncertainty. In addition, our findings suggest that the efficiency in developing mental representations also depends on the characteristics of the user interface, viz. learning performance depends on the noise of the visual background. Such findings can be explained by changes in acquisition processes and are consistent with actual learning and memory models. In future studies, we are going to investigate the dynamics of learning and the way eye movement patterns change when probability concepts alter over time. Furthermore, we plan to examine how to support the development of appropriate mental models by social learning. Finally, I try to build a bridge between theoretical and applied research. In a cooperation project with the Robotics Research Institute we developed a new questionnaire (QUHCC:Questionnaire for User Habits of Compute Cluster) to investigate user behavior and satisfaction in High Performance Computing. We use data resulting from the QUHCC to model users and to run scheduler simulations. In a next step, I plan to extent this questionnaire for assessing mental models developed by users of compute clusters.

13.8 Markov decision processes with uncertain parameters

Dimitri Scheftelowitsch (`dimitri.scheftelowitschtu-dortmund.de`)
Supervisor: Prof. Dr. Peter Buchholz

This PhD project deals with uncertainty in Markov decision processes. Its main motivation lies in the inherent hardness of Markov modeling and possible problems that cannot be captured by the standard MDP paradigm.

One major topic in this project concerns with introducing a set of possible Markov decision processes, as in [1], 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 [2]. Furthermore, multi-objective approaches to parameter uncertainty have been explored, and it was possible to create algorithms for the arising multi-objective problems.

Another topic that has been explored 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 theoretically possible to view this problem as a special case of partially observable Markov decision processes, the known lower bounds for solving POMDPs are large; thus, it is intuitive to consider a special case in the hope to shed some of the inherent hardness of the original problem. We developed a framework that captures transition time uncertainty in Markov decision processes and solved several problems within this framework.[1]

---

[1] [1] Robert Givan, Sonia M. Leach, and Thomas L. Dean. Bounded-parameter Markov decision processes. *Artif. Intell.*, 122(1-2):71–109, 2000.

[2] Dimitri Scheftelowitsch. The complexity of uncertainty in Markov decision processes. Accepted for *SIAM CT15*, 2015.

13.9 User Modeling in High Performance Computing

Stephan Schlagkamp (`stephan.schlagkamp@udo.edu`)
Supervisor: Prof. Dr. Schwiegelshohn

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.

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

Thomas Siwczyk (`thomas.siwczyk@bci.tu-dortmund.de`)
Supervisor: 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.

14 GRK 1907: RoSI - Role-based Software Infrastructures for Continuous-context-sensitive Systems

Prof. Dr.-Ing. Wolfgang Lehner
Email: wolfgang.lehner@tu-dresden.de
Technische Universität Dresden
Internet: 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.

14.1 Formal Semantics for Models with Meta-Predicates

Stephan Böhme (`stephan.boehme@tu-dresden.de`)
Supervisor: 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 DLs[2] 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, it is also possible to play a rôle for a certain time. Until now that dynamic aspect of roles is neglected, since the current framework does not feature any notion of time. Hence, 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.

One step towards a usable system will be the investigation and development of algorithms for deciding standard reasoning tasks. This will result in a proto-typical implementation.

---

[1] Szymon Klarman and Víctor Gutiérrez-Basulto. Two-dimensional description logics for context-based semantic interoperability. In *Proceedings of AAAI-11*. AAAI Press, 2011.

[2] Stephan Böhme and Marcel Lippman. Decidable Contextualized DLs with Rigid Roles. In *Proceedings of DL-15. CEUR-WS.org*, 2015.

[3] Franz Baader, Silvio Ghilardi and Carsten Lutz. LTL over description logic axioms. *ACM Trans. Comput. Log.*, 13(3):21, 2012.

14.2 Context-based Reasoning in Ontologies

İsmail İlkan Ceylan (`ceylan@tcs.inf.tu-dresden.de`)
Supervisor: 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] Ceylan, İ.İ., Peñaloza, R.: The Bayesian Description Logic BEL. In *Proc. of IJCAR. Springer Verlag*, 2014

[2] Ceylan, İ.İ., Peñaloza, R.: Tight Complexity Bounds for Reasoning in the Description Logic BEL. In *Proc. of JELIA. Springer Verlag*, 2014

[3] Ceylan, İ.İ., Peñaloza, R.: Query Answering in Bayesian Description Logics. In *Proc. of DL, To appear*, 2015

[4] Ceylan, İ.İ., Peñaloza, R.: Dynamic Bayesian Description Logics. In *Proc. of DL, To appear*, 2015

[5] Ceylan, İ.İ., Lukasiewicz, T., Peñaloza, R.:Answering EL Queries in the Presence of Preferences. In *Proc. of DL, To appear*, 2015

14.3 Formal Quantitative Analysis of Role-based Systems

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

Role-based modeling is a promising approach to cope with the context-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.

14.4 Database Versioning

Kai Herrmann (`Kai.Herrmann@tu-dresden.de`)
Supervisor: 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[1]. 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[2]. 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*, 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*[3] database schema[4]. 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] K. Beck et al., Manifesto for Agile Software Development, 2001.

[2] C. Curino, H. J. Moon, A. Deutsch, and C. Zaniolo, Automating the database schema evolution process, VLDB Journal, vol. 22, no. 1, 2013.

[3] T. Kühn, M. Leuthäuser, S. Götz, C. Seidl, and U. Aßmann, A Metamodel Family for Role-Based Modeling and Programming Languages, SLE LNCS, vol 8706, 2014

[4] T. Jäkel, T. Kühn, H. Voigt, and W. Lehner: RSQL - A Query Language for Dynamic Data Types. IDEAS, 2014,

14.5 Role-based Execution of ubiquitous, interactive Processes

Steffen Huber (`steffen.huber@tu-dresden.de`)
Supervisor: Prof. Dr.-Ing. Thomas Schlegel

Ubiquitous Systems (UbiSys) are highly runtime dynamic and context-sen-sitive systems, integrating a large number of heterogeneous components as well as users. Sensors, actuators, WebServices and software components create a closed loop between sensing the physical world, reasoning in the cyber world and subsequently acting on the physical world. Common application scenarios for UbiSys are smart environments like smart homes and the factory of the future, where ubiquitous system components collaborate in order to reach user-specified goals. Processes and workflows represent the most prominent means for formalising such goals and repeating tasks. However, the dynamic structure and context-sensitivity of ubiquitous systems represent major challenges for process modelling and execution, as a large variety of heterogeneous resources and subsystems as well as sources of information and context factors have to be integrated. In addition, the dynamic removal of process resources has to be supported at runtime. These factors represent serious obstacles for the successful employment of ubiquitous systems for process execution nowadays and in future. Existing approaches apply property-based or goal-oriented under-specification of dynamic processes not considering context-sensitive behaviour. Our research aims at a goal-oriented process execution approach for ubiquitous systems that combines goal-based process model specification at design time with role-based resource allocation at runtime. This approach increases flexibility and runtime-adaptivity of processes as required by ubiquitous systems. It allows for per activity process model adaptation according to available resource roles. The application of roles for resource abstraction and allocation enables a context-sensitive selection of component compositions. Goals simplify the process specification and yield more flexible activities and processes.

14.6 Role-based Database Model and Architecture

Tobias Jäkel (`tobias.jaekel@tu-dresden.de`)
Supervisor: 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, W. Lehner: RSQL - A Query Language for Dynamic Data Types. Proceedings of the 18th International Database Engineering & Applications Symposium (IDEAS '14), 2014, Porto, Portugal

[2] T. Jäkel, T. Kühn, S. Hinkel, H. Voigt, W. Lehner: Relationships for Dynamic Data Types in RSQL. Datenbanksysteme für Business, Technologie und Web (BTW), 2015, Hamburg, Germany

14.7 Semantics of Role Composition

Thomas Kühn (`thomas.kuehn3@tu-dresden.de`)
Supervisor: 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.[2,3] More importantly, because current software systems are characterized by increased complexity and context-dependence,[4] 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.[5] 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.[6] 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[2,3] and no approach fully incorporates both the context-dependent and the relational nature of roles.[3] In my thesis, I will devise a formal model for a *family of role-based modeling languages*[3] to capture the various notions of roles. In particular, the semantics of role composition, will enable the generation of this *language family* for Role-based Software Infrastructures (RoSI).

---

[1] Bachman, Charles W., and Manilal Daya. 1977. "The Role Concept in Data Models." In *Proceedings of the Third International Conference on Very Large Data Bases*, 464–76. Tokyo, Japan.

[2] Steimann, Friedrich. 2000. "On the Representation of Roles in Object-Oriented and Conceptual Modelling." In *Data Knowl. Eng* 35 (1): 83–106.

[3] Kühn, Thomas, Max Leuthäuser, Sebastian Götz, Christoph Seidl, and Uwe Aßmann. 2014. "A Metamodel Family for Role-Based Modeling and Programming Languages." In *Software Language Engineering* 8706:141–60. Lecture Notes in Computer Science. Springer International Publishing.

[4] Murer, Stephan, Carl Worms, and Frank J. Furrer. 2008. "Managed Evolution." In *Informatik-Spektrum* 31 (6). Springer: 537–47.

[5] Reenskaug, Trygve, and James O. Coplien. 2011. "The DCI Architecture: A New Vision of Object-Oriented Programming." In *artima Developer*.

[6] Herrmann, Stephan. 2007. "A Precise Model for Contextual Roles: The Programming Language ObjectTeams/Java." In *Applied Ontology* 2 (2). IOS Press: 181–207.

14.8 Towards Role Dispatch - Exploring Configurable 4-dimensional Role Dispatch

Max Leuthäuser (`max.leuthaeuser@tu-dresden.de`)
Supervisor: 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.

14.9 Role Adaptation Through Intention Recognition

Jan Reubold (`jan.reubold@tu-dresden.de`)
Supervisor: 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 these 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 extend IMMC is capable of learning intentions from data.

14.10 Towards a Highly Flexible Runtime Framework based on Role Modeling

Nguonly Taing (`nguonly.taing@tu-dresden.de`)
Supervisor: Prof. Dr. rer. nat. habil. Dr. h. c. Alexander Schill

A mission critical software system may not tolerate the down time for a small change or a bug fix in the system. Though not been proven in term of implementation, *Role* modeling is conceptually regarded as a mean to model the complex and dynamic software system as it allows object to capture user context dependent and adapt its behavioral change at the runtime.[1]

To our best knowledge, there is no research attempts to model role for bugs fix or unanticipated change while system is running. This paper proposes a software modeling based on role to achieve the two aforementioned properties by taking advantage of the advanced features of programming languages. Based on data type, reflection and meta programming features, five different role models with different level of flexibilities are introduced.

The first model is very similar to existing role model[2] that uses static data type for role type and requires common interfaces for different concrete roles. There is no binding mechanism discussed in the previous works; therefore we use dependency injection for role binding and adaptation for triggering the role change. There is no interface for the second model because dynamic data type is used. Since role is modeled as a separated type, the core object can use dynamic type to bind and unbind to any role type. This model may have a greater flexibility compare to previous one but it comes with performance penalty when invoke methods through dynamic type as it requires method lookup process at runtime.

The third and fourth enhance to the first and second model respectively. They rely on reflection technique to add new roles for unanticipated change and bug fix. Reflective roles can be compiled and attached to the system during runtime. The adaptation will trigger the core object to play the reflective role through configuration. These models poorly perform as method invocations through reflection are quite slow.

Similar to the fourth, the fifth model exploits unique feature of meta-programming that allows program to alter itself during execution. This is the ultimate flexibility that we can achieve as a core object can bind and unbind existing or new roles through code alteration. However, not all programming languages support this meta modeling feature.

There is a tradeoff between performance and flexibility in selecting a model among those five. The choice depends on the target system requirement.

---

[1] M. Fowler, "Dealing with Roles," Proceedings of PLoP. Vol. 97. 1997.

[2] D. Baumer, D. Riehle, W. Siberski and M. Wulf, "The Role Object Pattern," Washington University Dept. of Computer Science. 1998.

14.11 Runtime Adaptation of Role-based Software Systems

Martin Weißbach (`martin.weissbach1@tu-dresden.de`)
Supervisor: Prof. Dr. rer. nat. habil. Dr. h. c. Alexander Schill

Mobile devices not only have become more computational powerful and smaller of size, but are also equipped with a multitude of different sensors, e.g. GPS, gyroscope, ambient light etc., which are accessible by applications run on the device. In order to enhance the user experience and to save scarce resources, developers of applications for mobile and pervasive environments can utilize the available sensor information to enable runtime adaptation of the application to respond to changing sensor values. As a consequence context-aware self-adaptive systems have emerged that provide frameworks to ease development of such adaptable applications.

Resulting frameworks from the work on self-adaptive software systems provide runtime variation mechanisms mostly only on the level of components. Fine-grained adaptations are possible only via the modification of publicly available parameters of the components. Variations on the runtime object or programming language level of an application can be realized with different approaches, e.g. context-oriented or dynamic aspect-oriented programming. Yet there is no approach existing that incorporates runtime adaptations on both layers to the best of our knowledge.

We utilize the concept of *Roles* to present a framework that allows to control role-based runtime adaptation operations of a software system. To allow runtime adaptation of a given application we will develop a reference architecture for the adaptation control of a self-adaptive system. A revised component model that introduces the context-features of roles to the component will be a prime concern of our research. This will include mechanisms that allow fine-grained role-based adaptations on the level of runtime objects of a component. Concepts and mechanisms to modify a component's runtime objects are assumed to be already present. On both layers, we will thoroughly investigate operations to control the adaptation process with the aim to present a set of meta-operations that can be mapped to either layer of context-based adaptation.

To evaluate the utility of our role-based adaptation approach we will develop a prototypical implementation of our proposed framework and perform performance evaluations and simulate the system's behavior under differently swift changing environments. The overhead and duration of adaptations on the component level of our approach will be measured against existing self-adaptive systems or existing runtime object approaches, e.g. context-oriented programming, when fine-grained runtime object level adaptations are being performed.

14.12 Modeling of Role-based Adaptive Software Systems

Markus Wutzler (markus.wutzler@tu-dresden.de)
Supervisor: Prof. Dr. rer. nat. habil. Dr. h. c. Alexander Schill

Mobile devices are very heterogenous regarding hardware specifications (e.g. sensors), operating systems and programming language support. These parameters are dynamic at design time but static at runtime. Additionally applications on such devices are challenged with changing environments which are dynamic at runtime. Considering these parameters as context features mobile and ubiquitous applications need to be context-aware and dynamically adaptable at runtime. In practice, situations that should trigger a system's adaptation require the monitoring of a large set of context features. The appropriate specification of such situations and the design and implementation of systems that adapt according to detected situations is challenging for developers.

Current modeling approaches for adaptive software systems either don't consider context at all or require complex context descriptions. According to Bachmann[1], the concept of roles allows for capturing context-dependent and collaborative behavior. So far, existing role models allow developers to model a set of valid but static system configurations using roles and compartments. The concept of role modeling for adaptive systems has not yet received much attention as well. An issue of existing role models is a lack of environmental context like sensor or system information (e.g. network availability or energy consumption).

We assume that incorporating context models into role models reduces the complexity of context descriptions. An incorporated model of roles and context enables us to describe system configurations in their valid situation already at design time and to derive adaptation instructions and monitoring information for a runtime environment.

In a first step, we will investigate appropriate models to describe non-functional properties, quality of service, and context in general. After that a mapping needs to be defined that correlates static system configuration in their corresponding situations. We expect that we can incorporate context information into roles so that a role model specifies when or not a role is active. This allows for calculation of all valid configurations in their valid contextual scope and finally we can provide a transformation to a runtime processable description of monitored values, adaptation strategies, and application code. To evaluate we will prototypically implement the system and conduct a developer study to compare our approach with existing ones.

---

[1] C. W. Bachman, "The programmer as navigator," Communications of the ACM, vol. 16, no. 11, pp. 653–658, Nov. 1973.

15 GRK 1931: SocialCars - Cooperative, (de-)centralized traffic management

Prof. Dr.-Ing. Bernhard Friedrich
Email: friedrich@tu-braunschweig.de
Technische Universität Braunschweig
Internet: http://www.socialcars.org

The overall objective of the SocialCars Research Training Group is to research new methods and applications of decentralized, cooperative traffic management, that are enabled by new technological trends and developments such as Car-to-X communication.

SocialCars focuses on the integration of the individual objectives of traffic participants into a commonly agreed traffic planning policy. This integration will be achieved by cooperative interactions between the traffic management and the individuals. In order to comprehensively study this interplay while considering both the requirements of traffic participants and the constraints of the urban environment, we propose six fields of research, in which we investigate novel and interdisciplinary research questions.

In these fields of research, we study problems related to behavioral aspects of traffic participants, societal objectives, technical and algorithmic foundations of communication, interaction, and dynamic geo-information, as well as models and methods of cooperative, (de)centralized traffic management. We research solutions to these problems that will enable us to realistically describe dynamic cooperative traffic systems, and to evolve and optimize such systems in accordance with societal objectives.

15.1 Multiagent-based simulation of co-operative traffic maneuvers

Malte Aschermann (`masc@tu-clausthal.de`)
Supervisor: Prof. Dr. Jörg P. Müller

Due to the increasing individual mobility of traffic participants, rising resource consumption and a growing risk of accidents can be expected in the future [5]. Ongoing research in this field tries to reduce the risk of accidents by developing driver assisting technologies and infrastructure elements (C2X communication). The goal of these technologies is to raise the situation awareness of drivers and recommend optimized (tactical) maneuvers. Enabled by an underlying C2X infrastructure, cooperative maneuvers might help to improve the overall traffic flow and saturation of available road segments. This raises the question whether cooperation between vehicles can have a positive effect on traffic efficiency (compared to non-cooperative case). Additionally we investigate whether cooperative driving maneuvers can have a positive effect on traffic safety and if these positive effects which can be observed (and the degree to) depends on penetration rate of vehicles capable of cooperative maneuvering.

As optimizing tactical maneuvers ranges from individuals and groups up to higher-level traffic management, it is sensible to combine these aspects in a joint architecture. Furthermore it is important for plans, agreed upon on a cooperating level, to be understood and executed on a local, driver level. Therefore a high-level abstraction and low-level refinement of plans is necessary.

The basic concept of a plan abstraction hierarchy was introduced by [3]. [1] combines these high-level task networks with action-based planning. [2] proposes an algorithm for finding optimal high-level plans in hierarchical plan structures. [4] provides a multiagent architecture to connect institutionalized traffic management with group-wise decision making and individual, anticipatory behavior.

In this thesis a three-layer approach will be proposed to tackle the questions raised above. Cooperative maneuvers will be managed in an architecture, similar to [4]. It will contain layers for institutionalised traffic management, abstract cooperative and norm-based maneuver planning and individual vehicle planning.

The focus will be on the micro and meso layers, designing an architecture to allow individual vehicles to execute joint maneuvers and provide an abstraction for distributing a hierarchical plan structure among them. For an evaluation of the research questions, various scenarios will be investigated, each with different penetration rates of coordination aware vehicles. The results from a multiagent-based traffic simulation will be compared to answer the above questions.

[1] Kambhampati et al., Hybrid Planning for Partially Hierarchical Domains, AAAI-98
[2] Marthi et al., Angelic hierarchical planning: optimal and online algorithms, ICAPS-08
[3] Sacerdoti, Planning in a hierarchy of abstraction spaces, AIJ, 5(2), 115-135, 1974
[4] Sanderson, D.; Busquets, D.; Pitt, J., A Micro-Meso-Macro Approach to Intelligent Transportation Systems, Self-Adaptive and Self-Organizing Systems Workshops (SASOW), 2012 IEEE Sixth International Conference on , vol., no., pp.77,82, 10-14 Sept. 2012
[5] Stiller, C.; et al. DFG SPP 1835 Kooperativ interagierende Automobile

15.2 Automatic generation of dynamic parking maps based on crowd-sensing

Fabian Bock (`fabian.bock@ikg.uni-hannover.de`)
Supervisor: Prof. Dr.-Ing. Monika Sester

More and more modern vehicles are equipped with multiple sensors which perceive their surroundings. These sensors can be used to detect parked vehicles on the street. Combining the sensor data contribution of many vehicles, the information of parked vehicles at different times for the full city area can be obtained.

This project focuses on the generation of parking maps from this data using machine learning techniques. The spatio-temporal distribution of parked vehicle detection allows to determine legal parking spaces. Challenges are the inaccuracy of the sensors as well as the parking behavior of drivers who not always adhere to the law. The identification of spatio-temporal patterns shall facilitate the generation of a robust parking map.

In addition to this static information of legal parking spaces, methods shall be developed to extend the parking map by dynamic content. The current availability of parking spots can be obtained from comparison of vehicle detection and legal parking map. To increase robustness, patterns in space and time shall be identified and combined with current sensor information.

15.3 Determination of Meeting Points in Ride-Sharing Scenarios

Paul Czioska (`paul.czioska@ikg.uni-hannover.de`)
Supervisor: Prof. Dr.-Ing. Monika Sester

Many urban areas suffer from traffic congestion and air pollution, which is a growing problem that arises from individual motor car traffic, alongside with many other negative side-effects like road traffic injuries, carbon dioxide emissions and road traffic noise. A goal is therefore to reduce the number of cars driving though urban areas. Private car occupancy rates (number of travellers per vehicle trip) are meanwhile still very low. An increase of car occupancy rates could hence play a major role in releasing the cities from clogged streets. An effective way to use empty seat capacities is the principle of ride-sharing, which can be described as a system that brings together travellers with similar itineraries and time schedules. In addition to the reduction of cars, it offers the possibility to share all travel costs (including car maintenance costs) among several users. There exist already various commercial systems which realize such a ride sharing (Flinc, Uber or Matchrider to name only a few).

In most cases, the driver with the vehicle will not start at the same place as the ride passenger. This assumption reveals the need for a meeting point. A trivial solution is that the host picks up the client at the clients start position, e.g. in front of his home. In order to optimize travel times, this solution is often not the best possible option when the start time of the travel is the same, since the client could use the time when the host is on the way to walk or bike a certain distance so that they can meet in between. It reduces waiting time of the rider and driving time and distance of the driver.

This concept can also be extended to flexible public transportation systems that operate demand-responsive. Spatially flexible stopping places could offer the possibility to find best fitting meeting points for a unique route, so that the travel time or the distance for the transportation vehicle and the passengers can be reduced. When considering the case of multiple vehicles, cooperative approaches are necessary to reach a good efficiency. In addition, traffic management can be taken into account, so that in case of congestion the location of the stopping position can be changed. Furthermore it could be conceivable to prefer landmarks such as churches, fountains or parking places as meeting points to ensure a safe navigation and boarding.

15.4 Collective Decision-Making Mechanisms in Urban Traffic

Sophie Dennisen (sophie.dennisen@tu-clausthal.de)
Supervisor: Prof. Dr. Jörg P. Müller

This project aims at exploring possible applications of methods from Computational Social Choice for traffic management. Computational Social Choice is a field of study at the interface of Social Choice Theory and Computer Science. On the one hand, methods from Computer Science such as complexity analysis are applied to constructs from Social Choice Theory such as voting systems; on the other hand, concepts from Social Choice Theory are applied to Computer Science.

Research in Social Choice investigates collective decision-making mechanisms, i.e. methods aiming at creating a common decision for a group with differing preferences/decisions which takes all individual preferences/decisions into account.

Previously considered applications of collective decision-making mechanisms in urban traffic will be taken into account when searching for further possible applications. The first application to be investigated is the formation and decision making of tour groups in the sense of share-taxi passenger groups, where the decision making is based on the individual preferences for points of interest (POIs) and each tour group agrees on a set of POIs to visit.

It is planned to conduct the evaluation of the methods via agent-based simulation, where human and automated actors are modelled by means of a multi-agent system. Different collective decision-making mechanisms, particularly voting systems, will be compared - on the one hand, simulatively evaluating satisfaction of the group members, travel time, waiting time, air pollution and noise pollution - and on the other hand, evaluating theoretical properties.

15.5 Geo-Routing in Urban Car-2-X Communication Networks

Mehdi Tavakoli Garrosi (`mehdi.tavakoli.garrosi@ikt.uni-hannover.de`)
Supervisor: Prof. Dr.-Ing. Markus Fidler

In order to develop the Intelligent Transport Systems (ITS) and to realize a cooperative (de)centralized traffic management, the main element is the cooperation between the environment and traffic participants, also between traffic participants themselves i.e. efficient vehicle-to-vehicle and road-to-vehicle communications. To do so, On-Board Units (OBU) should be installed on the vehicles, and Road Side Units (RSU) should be installed on the road-networks. Such a system provides services related to traffic management, road-safety applications, and comfort applications including: infomobility e.g. helping to find the next gas station, mobile e-commerce e.g. sending advertisements, and infotainment and interactive services e.g. providing internet access.

Vehicular Ad-hoc Networks (VANET) are networks consisting of vehicles which dynamically set up an ad-hoc network without the aid of any infrastructure. These vehicles try to send messages using unicast, multicast, geocast and broadcast for different purposes via multi-hop vehicle communications. The vehicles between the source and destination receive the message and forward it through the network based on the routing protocol. Therefore, one of the key factors to successfully establish such a VANET is the design and development of a suitable routing protocol. This routing protocol should fulfill the Quality-of-Service (QoS) requirements e.g. low end-to-end latency, high packet delivery ratio and low routing overhead.

VANETs are Mobile Ad-hoc Networks (MANET) which employ vehicles as mobile nodes. Therefore some characteristics make them different from MANETs. In VANETs the vehicles move fast and because of this, the topology of the network changes rapidly. As a result, network disconnections happen frequently like in case of low vehicle congestion. Also, nodes are constrained by the layout of roads, so are the transmissions of packets.

Data dissemination and routing in MANETs have been extensively addressed but because of the unique characteristics of VANETs, and the diversity in the promising applications, they offer newer research challenges.

15.6 Speed choice on urban roads - situational and personality factors

Anne Goralzik (`a.goralzik@tu-braunschweig.de`)
Supervisor: Prof. Dr. Mark Vollrath

How individual drivers choose and maintain their speed in the presence of other road users is a key factor in cooperative urban road traffic management. Speed choice as core aspect of driver behaviour is mainly determined by automatic responses to specific environmental stimuli (e.g. road width, curvature), personality traits (e.g. sensation seeking), and situational factors (e.g. time pressure). However, it is unclear to what extent information from an intelligent cooperative traffic system, e.g. on current traffic hazards or environmental aspects, would be considered by drivers and how this additional information would be integrated with the more automatically processed information.

Driving simulation studies are conducted to examine these factors as well as the interaction between them by systematically varying and combining relevant driving scenarios. This way, a model of speed choice can be developed that is relevant to both the modelling of distributed intelligent and cooperative systems and the cooperative traffic management. Cooperative management applications may use the results of this dissertation to develop information displays that are most effective in influencing driving speed in the desired manner. By predicting driver behaviour, the model may also serve as a transport planning tool.

15.7 Impact of Traffic Controll Management on Urban Routing

Felix Köster (`f.koester@tu-braunschweig.de`)
Supervisor: Prof. Dr. Dirk C. Mattfeld

Urbanization does not only lead to an increased individual traffic volume, but also to increased freight traffic in cities. Globalization results in a worldwide transportation of goods and is another factor for the increasing number of transports in cities. This development is further reinforced by the continuous growth of e-commerce. Online purchases of goods add an extra transport layer in comparison to non-online shop purchases. As a results of the depicted trends, demand of transports in cities is constantly growing. These transports are generally known as last mile deliveries. To fulfill these transports, courier express and parcel services schedule vehicles in an urban environment of city logistic. CEP distribute products from manufactures to consumers, who expect fast and reliable service. An efficient transportation planning in cities is challenging. CEP have to plan considering city logistic uncertainties. In particular, travel times are varying regarding traffic volume, following daytime pattern. At the same time travel times are changed by uncertain events like sudden congestion or accidents. CEP must consider varying travel times in tour planning and, if necessary, adjust scheduled tours accordingly.

Further, city administrators have a major impact on travel times. Objective of city traffic control managements (TM) is to maintain efficient city traffic by controlling traffic flows in city areas. Therefore, TM draws on a number of possible actions. These actions are, for example, changes traffic control lights, lane control and speed limits. Usually, TM combines sets of actions to so called traffic strategies, each traffic strategy suitable for a specific traffic flow pattern. As a result, travel times between city locations situate not only by the occurring traffic volume but also by the traffic strategy applied by TM. Even though the strategy applied by the TM significantly impacts travel times, the strategies are generally not communicated. This research looks into the possibility of improving CEP routing efficiency, if information can be acquired from a cooperative traffic management and included in the tour planning by the CEP. We consider a routing problem, where a vehicle has to serve a set of customers. Travel times are time-dependent, stochastic and depend on the applied traffic strategy. Objective is to minimize the overall travel times. We apply approaches differing in the degree of information provided by TM. Results show, that considering TM-decisions in routing allow an increase in solution quality.

15.8 Design of adaptive V2V-Protocols for traffic performance improvement

Torsten Lorenzen (`torsten.lorenzen@ikt.uni-hannover.de`)
Supervisor: Prof. Dr.-Ing. Markus Fidler

Communication in Vehicular Ad-Hoc Networks (VANETs) is expected to improve road safety and traffic efficiency through the development of next generation road traffic applications. By recently signing the Memorandum of Understanding (MoU), European vehicle manufacturers have signalized their intention to bridge the gap from research to market by the deployment and integration of communication systems into cars from 2015 on. Vehicle-to-Vehicle (V2V) communication operating in the 5.9 *GHz* frequency band pave the way for efficient and innovative road traffic applications which primarily help drivers in critical situations but could also improve traffic efficiency by providing real time information about road traffic conditions.

Cooperative V2V applications rely on the single-hop broadcast of status information shared among vehicles on a single channel. However, in high network load conditions caused by high vehicle densities and a fixed periodic message generation rate, the channel will suffer from severe channel congestion which subsequently leads to a deterioration of the communication performance reflected by packet collisions. The key challenge of V2V is to ensure the reliability of the communication in such a way that a cooperative awareness between nodes in direct neighbourhood can be achieved, especially at urban intersection which is characterized by the complex and rapid changing topology of vehicular networks due to varying node densities. Even if in the early stage of V2V deployment, only a low penetration rate - which a ratio of number of equipped vehicles with a communication system - could be achieved, traffic density can be expected to growth substantially in urban environments during peak hours. Moreover, road traffic congestion would negatively affect the network load caused by the increased number of nodes contenting the communication channel. Hence, congestion control methods are required to limit and control the load on the channel even in harsh radio propagation conditions so that each node would be able to detect and possibly communicate with surrounding vehicles and road side units present in its local neighbourhood.

To achieve this, dynamic and adaptive approaches are needed to ensure reliable environment independent communication. Especially for urban areas there are mechanisms which could improve communication performance and therefore traffic performance as a result of traffic efficiency applications. Even though many studies have been published in the past, there is still much place for improvement.

15.9 Approaches to support tactical Service Network Design of Bike Sharing Systems

Bruno Neumann Saavedra (`b.neumann-saavedra@tu-bs.de`)
Supervisor: Prof. Dr. Dirk C. Mattfeld

Bike Sharing Systems (BSS) are a promising approach to tackle critical problems of today's urban mobility. However, the acceptance of BSS depends on the service level of the system, i.e., the successful provision of bikes for rentals and free bike racks for returns. Due to spatio-temporal demand variation, one-way trips and limited capacity of stations, rentals or returns may not be possible for every customer. Therefore, suitable bike fill levels for every station have to be determined, in order to ensure service reliability.

Within the scope of the tactical planning level, target fill levels have to be determined for each station through the course of the day. Within the scope of the operational planning level, the BSS provider relocates bikes among stations based on the target fill levels. Fill levels and relocation operations are interdependent since relocations are required to compensate for inadequate fill levels. Neglecting relocation operations in the tactical planning level may lead to suboptimal target fill level decisions. Therefore, anticipation of operational decisions in the tactical planning level is crucial for the viability of BSS.

Tactical Service Network Design (SND) yields regular services to transship goods between suppliers and demanders in order to achieve a suitable trade-off between the customer service level and the systems operation costs. The notion of SND is adapted for the BSS context (SND-BSS) to determine target fill levels and a suitable anticipation of operational decisions. The SND-BSS is formulated as a network flow programming, in which bikes are moved among the stations due to either bike demand or relocations.

The SND-BSS approach provides time-dependent target fill levels for every station. It is ensured that the relocation operations by means of ST are cost-efficient and a strong anticipation of operational decisions.

15.10 Decision making in navigation tasks - influencing factors and ways to change them

Madlen Ringhand (`m.ringhand@tu-braunschweig.de`)
Supervisor: Prof. Dr. Mark Vollrath

The effectiveness of traffic management depends on how drivers follow central traffic information, i.e. change the route in a desired way. In order to do so, an understanding is needed, concerning the type of information used by drivers for their route choice: the decision criterions that play a role, as well as the way different evaluations are integrated. This essentially involves cognitive decision-making-processes.

Based on driving simulation studies it will be examined how driver evaluate different information and integrate them to one decision. The corresponding characteristics of routes are varied and combined to experience this in the simulated driving, as well as determine the relational meaning of the influencing factors. Thereby shall, in particular, be examined the extent to which decisions and strategies of cooperative traffic management can be communicated and integrated into the driver's decisions. Both, centralized (e.g. evenly distribution of traffic throughout the city) and decentralized (e.g. optimization in the area of an intersection), are considered aspects.

The results of this study will contribute to the strategies of traffic management. One the one hand, traffic management can selectively impart the relevant information, on the other hand it can take into account how drivers will behave according to the recommendations. Furthermore the results will also contribute to the modeling in context of multi-agent systems.

15.11 Left turn prohibited problem combining signal control and traffic assignment model

Qinrui Tang (`q.tang@tu-braunschweig.de`)
Supervisor: Prof. Dr.-Ing. Bernhard Friedrich

Direct left turn at intersections increases delays and causes more accidents in certain conditions. Permissive-only left turn may cause safety problem because drivers have to find a suitable gap to go through the opposite go-straight flow. Vehicles in protected-only left turn lane may block the vehicles in go-straight lane, which results in larger overall delays.

The research aims to analyze which left turns should be prohibited in a city network due to safety and efficiency. The respective optimization will therefore minimize both travel times and the number of left turns in the road network. In order to obtain the criteria of the objective function a traffic demand and a traffic flow model need to be integrated in an optimization algorithm. The optimization will take into account the requirements of signal control programs for all traffic modes, such as realistic minimum green, maximum red and safe intergreen times. The results will provide suggestions for urban traffic management.

16 HPI Research School on Service-oriented Systems Engineering

Prof. Dr. Andreas Polze, Prof. Dr. Robert Hirschfeld
Email: {first.last}@hpi.uni-potsdam.de
Hasso Plattner Institute at the University of Potsdam
Internet: http://kolleg.hpi.uni-potsdam.de

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 and Computer Vision as Service (Prof. Dr. Patrick Baudisch), Service-oriented Geovisualization Systems (Prof. Dr. Jürgen Döllner), Algorithm Engineering for Service-oriented Computing (Prof. Dr. Tobias Friedrich), Modeling and Verification of Self-adaptive Service-oriented Systems (Prof. Dr. Holger Giese), Tools and Methods for Software Engineering in Service-oriented Systems (Prof. Dr. Robert Hirschfeld), Security Engineering of Service-based IT-Systems (Prof. Dr. Christoph Meinel), Service-oriented Information Integration (Prof. Dr. Felix Naumann), Evolutionary Transition of Enterprise Applications to Service-Orientation (Prof. Dr. h.c. Hasso Plattner), Operating System Abstractions for Service-oriented Computing (Prof. Dr. Andreas Polze), Services Specification, Composition, and Enactment (Prof. Dr. Mathias Weske), and Quantitative Evaluation and Optimization of Service-oriented Systems (Prof. Dr. Werner Zorn).

16.1 Simulation User Behavior on A Security Testbed Using User Behavior States Graph

Aragats Amirkhanyan (`aragats.amirkhanyan@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Christoph Meinel

For testing new methods of network security or new algorithms of security analytics, we need the experimental environments as well as the testing data, which are much as possible similar to the real-world data. Real data is always the best basis for testing new methods or algorithms. However, it is always impossible to get the real data, especially for doing the research in the area of IT security. The lack of data is a result of the fact that mostly the huge amount of data belongs to industrial companies, but they are usually not able to share them because of security and privacy reasons. The reasons could be manifold. One of them is the security issue, because the security-related infrastructures, which generate the security data, for example firewalls, gateways and etc., are usually the critical parts for the entire infrastructure. Therefore, it could be dangerous to change the configuration or install other tools to collect data. Also, there is the privacy issue to access the data. The data, such as Active Directory logs, often contain personal information and, therefore, such kind of data must be anonymized before exporting for analysis. Therefore, the scientific world is always trying to find the best approaches and recommendations for creating and simulating testbeds, because the issue of automation of the testbed creation is a crucial goal to accelerate research progress.

There are several ways to generate data. One of them is to generate synthetic data. This method implies that you know about the structure of data, the correlation between data and you roughly know what the result of analysis you will get based on the generated data. But synthetic data have suffered from the criticism, because they are unrealistic due to the typical approach of using random data that looks like real data, but lacks the characteristics and substance of real data. In new approach I try to overcome this disadvantage by using the method of simulating real user behavior to produce needed data. The desire to simulate real user behavior gives us new challenges: how to describe the user behavior scenario and how to describe all possible user behavior states and actions.

In the scope of the topic, I present a new approach of describing user behavior for simulation tools. This approach meets requirements of simplicity and extensibility. And it could be used for describing user behavior scenarios to simulate them on Windows-family virtual machines. The proposed approached is applied to our developed simulation tool that we use for solving a problem of the lack of data for research in network security and security analytics areas by generating log dataset.

16.2 Finding and Extracting Implicit Decision Rules in Process Models

Ekaterina Bazhenova (`ekaterina.bazhenova@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Mathias Weske

To stay competetive in an ever changing market environment today, modern enterprises have to manage their business process in an effective way. Modeling languages as BPMN [1] are well suited for process experts as well as - thanks to tool support - end users. Process models allow documentation of business operations, enactment of business processes following the given execution semantics, and process analysis towards correctness, improvement, compliance, etc. In the course of process execution, multiple decisions are taken that influence the mentioned areas. Analysis of industry processes reveals that such decisions include the assignment of actual resources to activities answering the question who shall execute a specific activity or evaluating a given set of data to calculate a decision indicating which path shall be followed at decision points. Especially, in the insurance and banking domains, regulatory compliance highly influences process execution by specifying which guidelines must be followed.

Following the "separation of concerns" paradigm, this allows to keep the decision logic in a dedicated decision model and the process logic in a dedicated process model. To take advantage from existing information, in our recent work we introduced an approach to automatically detect decision logic in business process models and to generate decision models and corresponding decision tables from process models' decision logic. These decision models conform to both BPMN standard for process modeling, and the recently published Decision Model and Notation (DMN) [2] standard for decision modeling.

Our research work was focused on finding and extracting the decision logic from process models. In patricular, that included (i) identification of decision logic in process models, (ii) derivation of a corresponding DMN model and adaptation of the original process model by replacing the decision logic accordingly, and (iii) final configuration of this result during post-processing. This approach enables business organizations to migrate already existing BPMN models.

---

[1] OMG: Business Process Model and Notation (BPMN), Version 2.0 (January 2011), `http://www.omg.org/spec/BPMN/2.0/`

[2] OMG: Decision Model and Notation (DMN), Version 1.0 (February 2014), `http://www.omg.org/spec/DMN/1.0/Beta1`

16.3 Software Evolution Within Enterprise Software Ecosystems

Thomas Brand (`thomas.brand@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Holger Giese

Enterprise application software needs to be adapted in order to fit to changing requirements and to maintain or increase its relevance to the users. In addition software manufacturers also need to consider the health of their software ecosystem, comprising for example extension developers, software vendors and customizing consultants as well as hosting providers. Little research is done about proprietary software ecosystems like the one of SAP.

Within the ecosystem product managers and requirement engineers of software manufacturers like SAP are responsible for:

- Gathering, generalizing and prioritizing customer requirements.

- Discover potential for simplification, optimization and innovation.

- Describe best practices on how to use the software for different customer groups.

- Attract software ecosystem partners, for example by providing aggregated information like key performance indicator benchmarks.

Important information sources for product managers today include direct customer contact and feedback provided by third parties from within the software ecosystem, such as customizing consultants. Those sources have the following characteristics, which can be disadvantageous:

- The feedback is a subjective assessment by people, who might have other objectives and backgrounds than the software manufacturer.

- Due to the costs and efforts to collect feedback manually, only the feedback of a small fraction of customers can be considered.

- Also due to low sampling rates it is harder to discover trends compared to continuous automated long-term monitoring.

During my research I would like to understand, which feedback information could be gathered and how it could be presented so that product managers can use it for decision making in the requirements and deployment process. Of special interest is, to which extend the feedback loop that is focusing on business functionality within the evolution process can be automated considering current technologies and upcoming cloud deployment options and how the required components differ from the one of the architectural blueprint for autonomic computing.

16.4 Service-Oriented Integration, Processing, and Provision of Massive 3D Point Clouds

Sören Discher (`soeren.discher@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Jürgen Döllner

In-situ and remote sensing technology (e.g., laser scanning and photogrammetric approaches) allow for an efficient and automatic creation of so-called 3D point clouds, i.e., point-based digital representations of spatial environments such as cities and landscapes. Applications and systems for the processing and visualization of such 3D point clouds are faced by a massive amount of data due to an increasing availability (e.g., for whole countries), density (e.g., 400 points per m2), and capturing frequency (e.g., once a year). As a remedy, the traditional workflow of geoinformation systems -i.e. using 3D point clouds to derive 3D meshes as an intermediate step- is becoming increasingly inefficient, especially when parts of the data have to be updated continuously. Thus, to make efficient use of the full resolution and potential of dense, spatial overlapping, and multitemporal 3D point clouds, the point data should be processed and visualized directly. My research focus is on concepts for a service-oriented infrastructure for 3D point clouds that provides the following features:

- Efficient storage and management of heterogeneous 3D point clouds (e.g., airborne, mobile, or terrestrial) that may be specified in different formats or georeference systems enabling an efficient access to the data.

- Distributed, scalable, adaptive, and selective execution of common processing and analysis tasks (e.g., validation of building cadastre data) directly on the point data.

- Efficient provision and scalable 3D rendering of massive 3D point clouds to allow for an interactive exploration of a captured area without having to derive mesh-based 3D models.

In recent work, I was concerned with the scalable rendering of arbitrarily large 3D point clouds on a broad range of hardware devices, ranging from high-end desktop computers to low-end mobile devices (e.g., smartphones or tablets). This can be achieved by combining out-of-core or external memory algorithms with client-server-based rendering approaches. Further research has to be put into novel compression and decompression algorithms for a more efficient transfer of point data via network.

16.5 Graph Transformation Systems and Verification with k-Inductive Invariants

Johannes Dyck (`johannes.dyck@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Holger Giese

Invariant checking is a static analysis technique related to model checking. Based on a formalization of a system's behaviour, it is possible to show or disprove the validity of certain properties of the system. An existing technique[1] is focused on the special kind of *inductive invariants*. An inductive invariant is a property whose validity is not violated by a change of the system's state, shifting the corresponding analysis from the states to the nature of the system's transitions between states. Inductive invariants do not take initial states into account, making reachability checks for states obsolete. Furthermore, a change to the system's initial state does not compromise the validity of properties proven to be inductive invariants. As a means of specifying properties and system behavior, the abstract and expressive concepts of graphs and graph transformations are employed.

However, properties shown to not be inductive invariants do not automatically imply an unsafe system, as, for example, counterexamples to the properties may not consist of actually reachable states, i.e. states in the system's state space. Consequently, a more detailed analysis is often desirable to discard false negatives.

Instead of applying the time-consuming and possibly non-terminating approach of state space generation, we propose the notion of *k-inductive invariants*, relating to the concept of k-induction[2]. The idea is to analyse not only a single transition between states and its capability to violate a property, but to take a path of transitions into account, which provides additional context and may result in new information sufficient to discard counterexamples under investigation. It also offers the possibility to find earlier errors, revealing that counterexamples are not reachable from an error-free state.

Important results include the use of symbolic representation and constraint reasoning to address complexity challenges arising from increased expressive power of the specification language and the inherently exponential nature of k-induction. Recently, the base technique of inductive invariant checking has been applied to the verification of model transformations.

---

[1] Becker, B., Beyer, D., Giese, H., Klein, F., Schilling, D.: Symbolic Invariant Verification for Systems with Dynamic Structural Adaptation. In: Proc. of the 28th International Conference on Software Engineering (ICSE), Shanghai, China, ACM Press (2006)

[2] Sheeran, M., Singh, S., Stålmarck, G.: Checking Safety Properties Using Induction and a SAT-Solver. In Hunt, W., Johnson, S., eds.: Formal Methods in Computer-Aided Design. Volume 1954 of Lecture Notes in Computer Science. Springer Berlin/Heidelberg (2000) 127-144

16.6 Solving Constraints on Object Behavior

Tim Felgentreff (`tim.felgentreff@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Robert Hirschfeld

Constraints provide a useful technique for ensuring that desired properties hold in an application while avoiding scattered, imperative code that ensures these properties explicitly. As a result, they have been used in a wide range of applications, including graphical layouting, physical simulations, load balancing, and interactive puzzles. In these domains, it is often easier to state *what* the rules are than *how* to achieve them. Another advantage constraints offer over an imperative programming style is that constraint solving has a clean semantics when it comes to trading off multiple and possibly competing constraints with varying degrees of preference.

Despite their advantages, constraints have failed to become a commonly used tool in in the context of object-oriented programming. Even where constraints may be applied directly, purely imperative programming is still the norm. We believe this is in part due to performance considerations, the lack of integration with existing, imperative code, as well as inexperience of the programmers with the features and limits of constraint solvers. There have been attempts to provide constraints as part of general purpose object-oriented programming languages. These either propose new programming mechanisms that combine abstractions for constraints and object-oriented programming, or they incorporate constraints into object-oriented programs as library. The former has the disadvantage of having to learn a new programming language with new abstraction mechanisms, while the latter leaves it up to the programmer to translate the relations between objects into constraints for the solver and back at appropriate times in the program.

In our work we present Babelsberg, a design to integrate constraint solving with existing object-oriented languages, while re-using the object-oriented abstractions, including allowing constraints on the results of polymorphic message sends. Babelsberg is an instance of *object-constraint programming*, for which we also provide a formal semantics that incrementally adds constraints to an object-oriented host language with dynamic typing, object encapsulation, object identity, and message sends. In our design and semantics, we clarify many corner cases around the interaction of constraints with object structure that could lead to surprising or undesirable solutions. Finally, to show that our design is practical, we have implemented prototypes in different languages that demonstrate how multiple solvers can cooperate to solve an interesting set of problems, how our design can be integrated with a just-in-time compiler to provide adequate performance, and how the constraints can be integrated with syntactically with different host languages according to meet the expectations of developers in those languages.

16.7 Requirements for Analysis of Multi-Temporal 3D Point Clouds

Dietmar Funck (`dietmar.funck@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Jürgen Döllner

3D point clouds are a 3D model of surface structures and objects, described as a discrete set of points. There are different remote sensing technologies available for the creation of 3D point clouds (e.g., laser scanning or image matching), which can be mounted on different platforms (e.g., airplane or car). Independent from the used remote sensing technology and platform a 3D point cloud is a snapshot of the captured environment including static structures (e.g., buildings, terrain) as well as dynamic objects (e.g., pedestrians, vehicles). In recent years the increased availability, density and capturing frequency lead to massive 3D point clouds. The main purpose of the increased capturing frequency is to provide up-to-date 3D point cloud data for a variety of applications such as deriving of building models, tree cadastres, urban analytics and simulation. Having 3D point clouds from different points in time for the same area results in multi-temporal 3D point clouds. An advantage of multi-temporal 3D point clouds is the redundant surface information that allows to detect static structures and dynamic objects. To analyse multi-temporal 3D point clouds the following primary requirements have to be met:

1. Proper registration of 3D point clouds from different points in time.

2. Calculation of point normals to estimate the represented surface.

3. Algorithms have to be robust regarding noise, outliers and varying point densities.

4. Out-of-core concepts for handling massive 3D point clouds.

Analysis of multi-temporal 3D point clouds offers new opportunities to manage, process and analyse 3D point clouds as required by a growing number of applications and systems. Integrating the analysis of multi-temporal 3D point clouds in a service-oriented computing environment would ease the access to the required modern processing hardware.

16.8 Utility-Driven Modularized MAPE-K Loop Architectures for Self-Adaptive Systems

Sona Ghahremani (`sona.ghahremani@hpi.uni-postdam.de`)
Supervisor: Prof. Dr. Holger Giese

As a consequence of either the changes that are made in the software and environment or the failure of the developer to modify the software to meet the changes, the software will age. Software aging leads to inability to keep up, decrease in reliability and reduced performance. In order to reduce the effects of aging, software needs to evolve and adapt to new circumstances and environmental changes. A self-adaptive software is capable of evolving and modifying itself at runtime to obtain a specific level of quality of service and achieve certain functional goals.

A MAPE-K loop, is an efficient way to employ a control loop in the adaptation engine. Being a growing and multi-concern system requires handling many runtime issues which means the adaptation engine must be modularized and include several feedback loops each responsible for one issue at a time to be able to keep up with the speed of environment changes and software demands.

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.

16.9 Visualizing Structure and Runtime Behaviour of Multi-threaded Software Systems

Sebastian Hahn (`sebastian.hahn@hpi.uni-potsdam.de`)

Supervisor: Prof. Dr. Jürgen Döllner

Program understanding is a crucial but tedious and timeconsuming task within the software development and maintenance process that becomes even more complex with the use of multi-threading. Visual software analytics tools can help to gain insight into the non-trivial processes of such systems. However, most of these tools create depictions that either focus on the runtime behavior or the static structure, not taking into account that for various comprehension tasks the combination of both information bases are required.

Although, previous research in combining static structure of a system with its runtime information for sequential working applications was conducted, there are no suitable approaches for the visualization of systems with concurrent runtime behavior. In this work, we present a visualization technique and prototypical tool that allows for the analysis of multi-threaded systems using a combination of both, the organizational structure as well as concurrent runtime-behavior information of a system.

16.10 Software Dependability Evaluation

Lena Herscheid (`lena.herscheid@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Andreas Polze

Software is becoming more ubiquitous and therefore plays an increasingly prevalent role in dependability research. Fault and error models need to be tailored and adapted for software systems. The understanding of complex propagation chains is essential for increasing and comparing the dependability of real world software systems. This research focusses on evaluating software dependability both from a theoretical, and a practical perspective.

Fault injection is a useful tool for practical experimentation. It can be used to test the fault tolerance features by artificially inserting faulty behaviour and error states into the 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, the questions of when and where to inject faults need to be answered.

Therefore, the theoretical focus of this research is to better understand and formalize the details of fault activation and error propagation in software. The state conditions which trigger the activation of dormant software faults, and thus lead to error states are not usually part of software fault models – they still form an elusive aspect. To this end, *fault activation and error behavior patterns* can describe exactly which state changes in the investigated and environment system cause a fault to become activated, and eventually lead to an error state. A deeper understanding of such patterns can be used to provide realistic fault injection targets. Further, automatic approaches to detecting and preventing fault activation during runtime can be explored.

16.11 Skin Drag Displays

Alexandra Ion (`alexandra.ion@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Patrick Baudisch

Wearable devices, such as smart watches, provide an instant notification service as they connect to online services and social networks and inform the user about current events. Tactile devices that are in continuous physical contact with the wearer's skin allow sending simple messages to the user without the need to visually examine the device. Devices based on a single vibrotactile actuator[1], for example, allow pulsing "Morse-like" messages.

We propose a new type of tactile displays that drag a physical tactor across the skin in 2D. We call this *skin drag*. We demonstrate how this allows us to communicate geometric shapes or alphabetical characters to users. The main benefit of our approach is that it simultaneously produces two types of stimuli, i.e., (1) it moves a tactile stimulus across a larger skin area and (2) it stretches the user's skin. Skin drag thereby combines the essential stimuli produced by vibrotactile arrays, which allows drawing simple shapes by fading from one vibration motor to the next[2], and skin stretch, which pushes and stretches the user's skin with a physical contactor to communicate directional cues[3].

In our study, skin drag allowed participants to recognize tactile shapes significantly better than a vibrotactile array of comparable size. We present two arm-worn prototype devices that implement our concept.

The devices run self-contained. In order to play back geometric shapes, we send data from a mobile device wirelessly via the RN42 Bluetooth module. A microcontroller board controls the two motors inside the device and two li-ion batteries power the device. The microcontroller interpolates between the control points of a shape and controls the motors using a PID control loop and position feedback encoders to form the shape.

[1] Brewster, S. and Brown, L.M. Tactons: structured tactile messages for non-visual information display. Proc. AUIC'04, 15–23.

[2] Israr, A. and Poupyrev, I. Tactile Brush: Drawing on Skin with a Tactile Grid Display. Proc. CHI'11, 2019–2028.

[3] Caswell, N.A., Yardley, R.T., Montandon, M.N., and Provancher, W.R. Design of a forearm-mounted directional skin stretch device. Proc. HAPTICS'12, 365–370.

16.12 Comparing and Describing Datasets on the Web of Data

Anja Jentzsch (`Anja.Jentzsch@hpi.uni-potsdam.de`)
Supervisor: 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[1]. This trend, together with the inherent heterogeneity of Linked Datasets and their schemata, makes it increasingly time-consuming to find and understand datasets that are relevant for integration. 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, e.g., the relational model, 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, ontology information for a Linked Dataset is not always available or may be incomplete. Algorithms and tools are needed that profile the dataset to retrieve relevant and interesting metadata analyzing the entire dataset.

There are many commercial tools, such as IBM's Information Analyzer, Microsoft's SQL Server Integration Services (SSIS), or others for profiling relational datasets. However these tool were designed to profile relational data. Linked Data has a very different nature and calls for specific profiling and mining techniques.

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 (`datahub.io`), these registries usually are manually curated. Furthermore, existing means and standards for describing datasets are often limited in their depth of information. VoID and Semantic Sitemaps cover basic details of a dataset, but do not cover detailed information on the dataset's content, such as their main classes or number of entities.

In order to compare data sets their content and structure must be defined and described. In order to calculate the similarity of two Linked Datasets a suitable hierarchy of metrics and a weighting of these metrics according to user-defined criteria will be developed.

---

[1]The Linked Open Data Cloud nicely visualizes this trend: `http://lod-cloud.net`

16.13 Level-Ups: Motorized Stilts that Simulate Stair Steps in Virtual Reality

Robert Kovacs (`robert.kovacs@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Patrick Baudisch

Ever since its conception in the 1960's, head-mounted virtual reality systems have been primarily concerned with the user's visual senses[1] and optionally spatial audio[2]. As the next step towards realism and immersion, however, many researchers argue that such systems should also provide a physical/haptic experience[3].

In my research, I thus aim at investigating how to add physical feedback to virtual environments to make them more immersive—moving it closer to the perception of actual reality. As an exploratory proof-of-concept prototype, I built "Level-Ups" which are computer-controlled stilts that allow virtual reality users to experience walking up and down actual physical steps. Each Level-Up unit is a self-contained device worn like a boot. Its main functional element is a vertical actuation mechanism mounted to the bottom of the boot that extends vertically. Each unit also contains pressure sensors that determine the right moment for actuation, a micro controller running a PID control loop, and a Bluetooth modem that connects each device to the server running the virtual reality experience.

Level-Ups are part of an integrated system. The user is wearing a head-mounted display (Oculus Rift) and is tracked using an optical motion capture system (OptiTrack). The data from the motion capture software (Arena) is streamed via a UDP connection to a VR server that forwards the data to the clients that are registered with the system. Each client runs on its own processing unit (e.g. MacBook Pro) that the user carries in his/her backpack. To be able to actuate Level-Ups in time, we wrote a simple prediction algorithm that determines where in the virtual world the user is most likely to step next; the software then determines the height of the terrain at this predicted location and sends this height information to the respective Level-Up unit. Our system then starts actuating the device with a delay less than 100 ms. Using this system, we run a user study, in which participants rated the realism of their experience on average 6.0 out of 7.0 when wearing Level-Ups compared to 3.5 without.

---

[1] Sutherland, I.E. A Head-Mounted Three Dimensional Display. In Proc. AFIPS'68, 757/764.

[2] Begault, D.R. 3-D Sound for Virtual Reality and Multi-media. AP Professional, 1994.

[3] Cheng, L.P., Lühne, P., Lopes, P., et al. Haptic Turk: a Motion Platform Based on People. In Proc. CHI'14, 3463–3472.

16.14 Theory of Ant Colony Optimization Algorithms on Stochastic and Dynamic Problems

Martin Krejca (`martin@krejca.de`)
Supervisor: 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 for exploiting 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, such as *ant colony optimization*[1] algorithms, are frequently the only way to achieve decent optimization. These algorithms can be engineered, employing benchmark tests and theoretical insight, to quickly derive algorithms which can be employed in practice to get good results in areas that previously required optimization by hand.

The main goal of our research is to further the understanding of ant colony optimization algorithms, using formal arguments, especially in settings involving stochastic environments (meaning the optimization landscape is perturbed by some random noise) and dynamic ones (where the landscape changes over time), since traditional optimization techniques in these settings are scarce, but the settings themselves are more realistic than deterministic environments.

For theoretical research, one mostly looks at pseudo-Boolean and combinatorial domains, optimizing problems or problem classes that show how generic optimization algorithms can handle certain aspects of the landscape to optimize.

We want to derive asymptotic run time bounds for a number of different formal problems in the aforementioned domains. The idea is that ant colony optimization algorithms were successfully employed in practice for such settings and also give very robust solutions (e.g., changing the landscape a bit does not affect the process of finding a new solution that much either).

We hope that a further theoretical understanding helps in making better use of ant colony optimization algorithms in real life applications.

---

[1] M. Dorigo and T. Stützle. *Ant Colony Optimization*. MIT Press, 2004.

16.15 Proprioceptive Interaction: Interfaces That Read and Write to the Human Body Using Electrical Muscle Stimulation

Pedro Lopes (`pedro.lopes@hpi.uni-postdam.de`)
Supervisor: Prof. Dr. Patrick Baudisch

The Internet of Things (IoT) allows objects and users to communicate via a distributed ad-hoc sensor/actuator networks. This allows objects to adapt dynamically to users intentions, such as a RFID-enabled door that unlocks only when an authorized user is present. However, the IoT as of today is limited to only simple sensor networks because installing complex mechanical actuators in every single object around us is costly and does not scale to every household object we own (e.g., hundreds of objects per user).

Thus, we propose allowing objects to dynamically change their behavior by, instead of adding mechanical actuators to every object, instrumenting the user instead. With our concept, which we call Affordance++, we extend the affordance of objects by allowing them to communicate dynamic use, such as (1) motion (e.g., spray can shakes when touched), (2) multi-step processes (e.g., spray can sprays only after shaking), and (3) behaviors that change over time (e.g., empty spray can does not allow spraying anymore). Rather than enhancing objects directly, however, we implement this concept by enhancing the user using Proprioceptive Interaction, which is a human-computer interaction modality we developed in our research.

Our proprioceptive interaction modality allows users to interact and perceive the world by the sense of proprioception, i.e., how their body is posed. This is achieved by stimulating the user's arms using electrical muscle stimulation. Using this modality, our Affordance++ prototype allows objects not only to make the user actuate them, but also perform required movements while merely approaching the object, such as not to touch objects that do not "want" to be touched.

Our proof-of-concept prototype is implemented as a bracelet equipped with Wi-Fi for communications, RFID for object tracking and a ATMEGA328 for controlling the medically-compliant electrical muscle stimulator. The user-object relationships (i.e., which gesture to trigger for each user's action) are stored in a database accessible by the bracelet. Once the user grabs an object: (1) the bracelet identifies it via RFID, (2) requests the user profile from remote database, and, (3) retrieves the stimulation pattern for the adequate action, for instance: shaking the spray can before using it.

Lastly, in our user study, we demonstrated that affordance++ helped participants to successfully operate devices of poor natural affordance, such as a multi-functional slicer tool or a magnetic nail sweeper, and to stay away from cups filled with hot liquids.

16.16 From Choreography Diagrams to RESTful Interactions

Sankalita Mandal (`sankalita.mandal@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Mathias Weske

As the number and the complexity of interactions between multiple business partners grow, it becomes important to describe them using precise models and notations which can be refined to a level of detail suitable for their implementation. Today, business process management is a key approach to organize work, and many companies represent their operations in business process models. Recently, choreography diagrams have been introduced to represent interactions between business processes, run by different partners. While there is considerable work on using process models during process implementation, there is little work to use choreography models to implement interactions between business processes.

As more and more services adopt the representational state transfer (REST) architectural style [1] to expose their internal business processes on the Web [2], we identify the opportunity to define and represent interactions among business processes at a suitable level of abstraction with choreography diagrams, specified in the Business Process Model and Notation (BPMN) standard [3]. We introduce a novel approach to enhance choreography diagrams with annotations that facilitate capturing all the details that are necessary to give an efficient implementation of the HTTP-based information exchanges among two or more interacting partners. Using enhanced choreography diagrams allows us to develop REST-based interactions among business partners in an efficient manner. We complement the RESTful choreography diagram with an object life cycle model, also annotated with REST interaction information.

[1] Fielding, R.T.: Architectural Styles and the Design of Network-based Software Architectures. PhD thesis (2000) AAI9980887

[2] Pautasso, C., Wilde, E.: Push-enabling restful business processes. In: Proc. of the 9th International Conference on Service Oriented Computing (ICSOC 2011)

[3] OMG: Business Process Model and Notation (BPMN), Version 2.0. http://www.omg.org/spec/BPMN/2.0/ (January 2011)

16.17 Optimizing Dynamic Languages for Analytical Workloads

Toni Mattis (`toni.mattis@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Robert Hirschfeld

Dynamic, object-oriented programming languages are well suited for implementing online services, as they support writing the domain logic in a concise and maintainable way. Unfortunately, they are relatively inefficient when required to analyze large data volumes, such as medical records, sales events, and sensor data, in order to support decision making or uncover new insights.

In contrast to dynamic languages, modern in-memory databases have successfully addressed the performance challenges inherent to analytical workloads and large data volumes.[1] Research has shown that analytical algorithms often traverse large amounts of records but only read a few attributes per record. This observation has motivated a column-oriented memory layout that keeps values of the same attribute in a sequential chunk of memory. Traversing a few columns is significantly faster than traversing full records and allows for better compression, CPU cache utilization and hardware-level prefetching.

However, for gaining performance, it is not always desirable to use a full-fledged database along with the service, as this splits domain logic between application and database, and introduces a system boundary, at which tool support and runtime optimizations on either side are lost when data or control flow crosses this boundary.

Therefore, we explored possibilities to transfer recent developments from the database domain to a dynamic, object-oriented execution environment, especially the column-oriented memory organization and relational optimizations, and merge them with recent advances in JIT compiler technology.

Our research prototype is based on PyPy, a Python implementation equipped with a meta-tracing JIT compiler.[2] Using a JIT-aware, column-oriented memory organization for objects, we achieved up to three times faster execution of a wide range of analytical algorithms compared to standard PyPy, and a similar performance as commercial in-memory databases.

[1] Hasso Plattner: "In-Memory Data Management: Technology and Applications", 2nd ed., Springer, 2012

[2] Carl Friedrich Bolz, Antonio Cuni, Maciej Fijalkowski and Armin Rigo: "Tracing the meta-level: PyPy's tracing JIT compiler", Proceedings of the 4th workshop on the Implementation, Compilation, Optimization of Object-Oriented Languages and Programming Systems, ACM, 2009

16.18 Fast Generic Virtual Machine Optimizations for Language Experimentation

Tobias Pape (`tobias.pape@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Robert Hirschfeld

Experimenting with programming languages is typically bound to complex implementation processes and low-level programming, since a large number of programming languages are written in lower-level languages such as C or C++ mainly for reasons of performance, especially for dynamic languages that run on a virtual machine (VM). Yet, programming language experimentation calls for highly expressive languages, low turnaround times from code to running program, and fast-enough performance to gain useful insights from experiments. Implementing a programming language experiment *within* the language the experiment is designed for (that is, meta-circularly) can provide both expressiveness and low turnaround times. Literature suggests that during the early experimentation phase, the dynamic and high-level nature of the implementation languages has provided a suitable and malleable environment to gain insights for the then not well understood ideas. A similar experience provided the application of design by contract (DbC) to the Racket language, a Scheme dialect. However, in both instances the performance when using the newly provided feature is substantially worse compared to not using the feature at all. This hampers the adoption and 'real-life' evaluation of the new features.

The common way to address performance issues of language features like this is to adapt the runtime environment, as its typically more low-level nature allows special-casing the language feature and subsequently providing better performance. As a result, experimentation is hardly possible and future maintenance impaired from the beginning. One approach we investigated to address this situation are generic VM optimizations.

Providing higher performance for generic data structures and faster execution for generic behavior should lower the impact of language experiments and should ease their transition from experiment to language feature. A successful example is *Pycket*, an implementation of the Racket language. The careful optimization of certain basic structures of the Racket language reduced the overhead of the DbC implementation to ca. 5 %–15 %—much lower than Racket's of typically more than 100 %. Likewise, with *adaptive data structure optimization* we can show that the overhead of more delegation-based data structures, such as trees and lists, can be reduced so much that other data structured such as vectors can be avoided, which traditionally had to be chosen to provide feasible performance. That way, experiments in pure delegation based systems can be hoisted from pure VM implementations to language-level meta-circular implementations.

16.19 Highly-Available Applications with Non-HA Infrastructure

Daniel Richter (`daniel.richter@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Andreas Polze

Today's applications and IT systems become more and more complex – they rely on different third-party libraries and frameworks, communicate with remote services, and often are distributed. But assembling a large number of components leads to the effect that software developers cannot give any promises about the reliability and availability of an IT system or its subcomponents any more; hence, tools and methods are needed to either evaluate the robustness of a software system – or to deal with unexpected faults.

To evaluate the correctness of fault-tolerance mechanisms, we investigated experimental evaluation of software systems and IT-environments by injecting faults so the consequences of errors can be evaluated. Our focus was on fault injection for distributed systems and cloud environments. In an ongoing industry cooperation we work on a project that evaluates a reference architecture for JEE-like applications with real-world applications as example in terms of performance (the ability to operate within a given specification e.g. under heavy load or with complete or partial crashes of sub-components) and consistency (scenarios with distributed databases and different data access implementations such as relational databases vs. NoSQL).

One focus of our recent research activity was on embedded real-time systems enhanced by remote (non real-time) backbone services accessed via the mobile Internet – whereas wide-distance communication channels cannot guarantee compliance with any real-time constraints. Using approaches such as analytic redundancy, our architecture employs the concept of cascaded processing stages each with own safety controllers and allows for decoupling of hard real-time processing on embedded control units and soft real-time data acquisition on the outer layers.

In today's software systems, the solution for fault tolerance and availability usually is to use (only) spatial redundancy. Therefore, we want to focus on different types of analytic redundancy and computing with uncertainty in mixed-criticality systems. On the one hand, we want to evaluate the possibilities of acceptability-oriented programming, where some differences from the correct result are tolerate, is applicable in this scenario – with an extended error model. On the other hand, we want to have a look at differential and multi-version programming and review where variant-rich software components and variability-aware testing.

16.20 Distributed Algorithms on Scale-Free Networks

Ralf Rothenberger (`ralf.rothenberger@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Tobias Friedrich

Large Peer-to-peer (P2P) systems like BitTorrent, RetroShare or Skype are decentralized and unstructured. The fact that peers are connecting and disconnecting from the network has implications about the nature of the overlay topology. In practice, because peers tend to discover highly available and high-outdegree nodes, connections are typically formed preferentially. As shown by Barabasi and Albert[1], this results in a *scale-free graph* in which nodes follow a power-law distribution. Another motivation to study scale-free graphs is the observation that many real-world networks are power-law networks, including Internet topologies, the Web, social networks, power grids, and literally hundreds of other domains[2].

It was shown during the last decades, that real scale-free networks exhibit a unique set of 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[3].

Although scale-free networks are omnipresent, surprisingly few rigorous insights are known about the performance of distributed algorithms on them. We believe that distributed algorithms can be specifically designed to exploit these properties with the goal of outperforming more generic approaches for general graphs. Furthermore, the properties of scale-free networks influence the behavior of certain processes on them, for example rumor spreading and influence diffusion. Again, only few rigorous results about their behavior on scale-free networks are known, although these processes take place on networks like social networks and infrastructure networks which are scale-free in real life. The focus of our work is to study the fundamental properties of these distributed algorithms and processes on scale-free networks.

[1] A.-L. Barabási and R. Albert. Emergence of scaling in random networks. Science, 286: 509-512, 1999

[2] M. E. J. Newman. Random Graphs as models of networks. In *Handbooks of Graphs and Networks*, pp. 35-68. Wiley-VCH, 2003

[3] R. van der Hofstad. Random graphs and complex networks. Available at www.win.tue.nl/ rhofstad/NotesRGCN.pdf, 2011

16.21 Ready Fire Aim - An Interactive Fabrication System for Non-expert Users

Thijs Roumen (`thijs.roumen@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Patrick Baudisch

In my research, I am creating interactive fabrication systems. Interactive fabrication systems allow users to work with personal fabrication tools by interacting with a work piece directly, rather than via the indirection of a traditional computer interface. My system I am developing right now is called ready-fire-aim and it allows users to engineer physical objects using a laser cutter. Users of the system use a laser pointer to point at the work piece directly through the laser cutter's safety glass. A camera system observes the laser pointer's bright dot and sends its input over the network to a server. The server runs a custom computer vision program that analyzes what the user is trying to draw. A real-time machine-learning component then classifies the drawn gestures and replaces the user's gesture with the intended shape. The system then sends this shape to the laser cutter, which cuts a shape. The system maintains a library of previously fabricated parts and allows multiple clients to connect to the server in order to make use of this library. The resulting system provides users with a sense of direct manipulation vaguely reminiscent of the affordance of traditional wood working tools.

I am using this basic system to explore how interactive fabrication systems can be adapted to use by inexperienced users, i.e., users without an engineering background. While experts tend to start their work by planning an effective strategy that considers dependencies between parts and resolves alignment and constraints early in the process, we find novices to employ more of a "greed" strategy; in hope of early gratification, they create salient parts firsts, trying to handle alignment and constraints late. On interactive fabrication systems, however, this strategy fails, as the size and shape of the salient parts is not reversible anymore by the time users try to fit it all together.

Based on these findings, I am currently developing a new model for interactive fabrication systems that is compatible with the greedy strategy of casual users and I am implementing these changes into a new version of ready-fire-aim. (1) In order to allow users to perform actions in an arbitrary order, this new version offers specialized alignment functions that users can apply "post-hoc" by matching up parts already created. (2) Post-hoc measurement functions allow matching already created objects with their intended physical environment. (3) The new version allows users to take objects out for testing, then allows them to put them back into the cutter by rescanning the object. (4) The system delays destructive actions as long as possible by causing all tools to initially produce only non-cutting "sketch" lines; only right before testing, the system cuts. My next steps will be to evaluate these new features of my system in another user study.

16.22 Incremental Record Deduplication

Ahmad Samiei (`ahmad.samiei@hpi.uni-postdam.de`)
Supervisor: Prof. Dr. Felix Naumann

Databases play an important role in IT-based companies nowadays, and many industries and organizations rely on accuracy of data in databases to perform their operations. Unfortunately, the data are not always clean. For instance, real-world entities have multiple, different representations, which could be due to erroneous data entry, data evolution, data integration, data transformation, etc. This in turn introduces so-called duplication into the databases. Deduplication intends to detect and eliminate different representations of real-world entities in a database. The focus of this work is on incremental deduplication, a more recent topic in deduplication. Deduplication is a time-expensive process that is executed on a database periodically. The sheer amount of incremental data, generated as a result of wide spreading internet, sensor data, etc., added to an already de-duplicated database makes it unreliable and unusable very fast, therefore imposes extra cost to the industries. Incremental record de-duplication attempts to address this problem and make database with many transactions always up-to-date and clean. That is, deduplication must happen on the fly, as the data arrives and enters the database.

16.23 Encourage Programmers to Build Graphical Tools for Improving Program Exploration and Modification Activities

Marcel Taeumel (`marcel.taeumel@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Robert Hirschfeld

Programmers benefit from graphical tools for programming, which are not just character-based but can exploit screen real estate efficiently with millions of colorful pixels that support comprehension of program-related information. Prominent environments include Eclipse, which integrates tools for source code browsing, writing, executing, and debugging. There, abstract text blocks can be enriched with concrete run-time data and hence plain text editors seem to become full-fledged, interactive visualizations.

Programming environments with graphical and interactive user interfaces represent complex software systems and are hence difficult to comprehend yet extend. Traditionally, there are *tool builders*, who create and maintain such tools, and *tool users*, who create and maintain various applications for their customers. For many programmers, however, it is difficult to take on both roles. When users face domain- or task-specific scenarios that builders failed to anticipate, there will be an obstructively long feedback loop to overcome such a productivity gap. Compared to other domains such as *carpentry*, this is looks unsatisfactory: some wood, a chisel, a hammer, and glue are often sufficient to quickly build self-made tables, props, or measurement aids—directly applicable to a particular bigger project.

Inspired by Unix-like environments where programmers can easily combine filter programs in shell scripts, we investigated a *data-driven* way to create programming tools in graphical environments. As a result, we designed and implemented *VIVIDE*,[1] which supports programmers to directly mold the visual experience of any tool by modifying concise *data transformation and extraction scripts*. This approach promotes low-effort tool construction; it works well for basic programming tools, such as code editors and debuggers, but also for other domains, such as developer chats and bug trackers. A controlled experiment will show that programmers are actually more likely to adapt their tools in use to save time in their daily programming activities.

---

[1] The VIVIDE Programming Environment, http://www.github.com/hpi-swa/vivide

16.24 Omniscient Debugging in Database Applications

Arian Treffer (`arian.treffer@hpi.uni-potsdam.de`)
Supervisor: 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.

16.25 A Deep Semantic Framework for Multimodal Data

Cheng Wang (`cheng.wang@hpi.uni-potsdam.de`)
Supervisor: Prof. Dr. Christoph Meinel

Recently, the problem of joint modeling multi-modal data has gained increasing importance in various real-world multimedia applications. However, most existing approaches focus on inter-modal correlation problem that correlating different modalities through learning a common or intermediate space in a conventional way, eg. Canonical Correlation Analysis (CCA). These works neglected the exploration of high-level representative feature learning and intra-modal feature relationships. With the success of deep networks in multimedia computing, in this paper, a novel unified deep neural framework is proposed for multi-modal data analysis. On one hand, we focus on learning expressive and representative high-level semantic features for image and text representation. Specifically, visual features (deep features) are extracted from deep convolutional neural network and textual features (topical features) are extracted from Latent Dirichlet Allocation (LDA) based approach. In joint model learning, a 5-layer neural network is designed and enforced with a supervised pre-training in first 3 layers for intra-modal regularization. Our framework is able to accomplish three tasks: 1) multi-modal fusion, and 2) multi-modal image retrieval, and 3) cross-modal retrieval. The extensive experiments on benchmark Wikipedia dataset show the effectiveness of proposed framework in learning correlation between different modalities and obtained state-of-the-art results. Our approach achieved 0.6395 mean Average Precision (mAP) in multi-modal image retrieval. Also achieved 0.34 for image query and 0.258 for text query in cross-modal retrieval

These proceedings were typeset by LaTeX using KOMA-Script. We would like to thank Tobias Pape for creating the template.

A.Babari, C.Carapelle